Saginaw County Community Mental Health Authority (SCCMHA)

Network Services Provider Manual

500 Hancock Street
Saginaw, MI 48602
Phone: (989) 797-3400

Fiscal Year 2026

Provider Manual Update - January 2026
Included are the updated policies and procedures since the FY25 October Provider Manual Update

Page	Policy/Procedure Number	Policy/Procedure Name	Updates	Date Revised	Licensed Residential/Crisis Residential	Enhanced Health Services/Autism (speech, behavioral, ot)	Inpatient	Crisis/CAI/MUTT	Primary Providers (Supports Coordination/Case Management/Primary/ACT/Autism/Wraparound/Integrated Care)	Community Living Supports/ CLS Per Diem/Respite Services	Skill Build/Supported Employment/Clubhouse/Drop-In	Fiscal Intermediaries/Pharmacy/LEP
N/A	**Tab 1-Inroduction to SCCMHA-No Updates**											
7	**Tab 2-Eligibility Care Management**											
8	03.01.06	Diagnosis in Medical Record, Billing and Reporting	Overall review, no new changes.	11/1/2025	x	x	x	x	x	x	x	x
12	03.01.07	Cost of Services and Explaination of Benefits	Overall review, no new changes.	11/1/2025	x	x	x	x	x	x	x	x
16	03.01.01.06	Waiting Lists	Overall review, no new changes.	11/1/2025	x	x	x	x	x	x	x	x
N/A	**Tab 3- Services & Protocol-No Updates**											
29	**Tab 4-Service Delivery**											
30	02.03.05	Recovery	Rewritten to conform to current SCCMHA nomenclature and standards. Added current members of armed forces (in addition to veterans). Added reference to SCCMHA policy 03.02.45-Interdisciplinary Treatment Teams.	4/8/2025	x	x	x	x	x	x	x	
41	02.03.08	Welcoming	Rewritten to conform to current SCCMHA nomenclature and standards. Added developmentally appropriate to Standard D. Added case holder to Standard L. Broadend definitions. Changed Exhibit M to reflect updated policy title: Serving LGBTQIA+ Persons	4/8/2025	x	x	x	x	x	x	x	x
48	02.03.09.09	System of Care (SOC)	Language changed from "consumer" to "persons served". Added substance use issues and disorders to Standard E.4. Added evidence based practices and treatments (in additions to services) to Standard 4.8. Added new language to standard 4.9. Added a definition of flex funds.	4/8/2025	x	x	x	x	x	x	x	x
56	02.03.09.44	Art Therapy	New Policy	10/1/2025					x			
61	02.03.12	Alternatives to Gaurdianship	Updated with more inclusive language & to conform to current SCCMHA nomenclature and standards	4/8/2025	x	x	x	x	x	x	x	
83	02.03.25	Wellness	Updated to reflect Current SCCMHA standards and terminology	4/8/2025	x	x	x	x	x	x	x	
88	02.03.41	SOGI Safe	Updated to reflect Current SCCMHA standards and terminology	4/8/2025	x	x	x	x	x	x	x	

96	03.02.31	Services for Members of the Armed Forces, Veterans & Their Families	Updated to reflect Current SCCMHA standards and terminology	4/8/2025	x	x	x	x	x	x	x	
101	03.02.34	Services for American Indians	Updated to reflect Current SCCMHA standards & Nomenclature	4/8/2025	x	x	x	x	x	x	x	
105	03.02.35	Serving LGBTQIA+ Persons	Revised policy title to reflect current terminology. Revised policy to conform to current SCCMHA nomenclature standards and align with CCBHC	4/8/2025	x	x	x	x	x	x	x	
117	03.02.45	Interdiciplinary Treatment Teams	Rewritten to conform to current nomenclature and standards with abbreviations spelled out to ensure understanding. Added "care" to treatment team to make the team more inclusive. Added BHH definition and expanded CCBHC definition. Added references to Michigan CCBHC and BHH published documents. Eliminated Exhibit due to lack of relevance.	4/8/2025	x	x	x	x	x	x	x	x
122	03.02.48	Older Adult Services	No Changes	4/8/2025	x			x	x			
127	03.01.01.07	Behavioral Health Screening and Assesment Standards	New Policy #. Added the Michigan Child and Adolescent Needs and Strengths (MichiCANS). Added the AHC and SDOH screening. Changed "Consumer" to "Person Served". Updated Exhibit A to include additional instruments currently in use by SCCMHA.	4/8/2025				x	x			
137	05.01.01	Management of Medical Products, Supplies, and Devices	No Changes	1/31/2025		x		x	x			
141	05.01.04	Psychiatric Supervision & SCCMHA Medical Director Role	Removed process of taking denials for admissions to the Medical director as it is not required.	8/29/2025	x	x		x	x	x	x	
144	06.03.01	Pest Prevention, Identification and Management	Updated Exhibit A-Pest Response Flow Charts with new floor plans. Added Exhibit D-Terminex Contract Location Grid	10/14/2025	x	x	x	x	x	x	x	x
166	**Tab 5-Regulatory Management & HIPPA Compliance**											
167	05.07.01	Compliance and Ethics Program-Corporate Compliance Plan (CCP)	Added titles to policy sections to summarize contents. Updated application to include employees, board members, contrators and network providers. Added References to Federal and Michigan False Claims Act, Whistleblowers Protection Act, 42 CFR, MSHN Compliance requirements and MDHHS Medicaid contract requirements.	10/14/2025	x	x	x	x	x	x	x	
170	05.07.02	SCCMHA Network HIPAA Compliance	Added Authentication and Access Control Policy Compliance section including requirements of unique usernames and strong passwords that meet SCCMHA complexity standards. Added User Authentication Auditing section to monitro unauthorized access and ensure compliance. Added "employees and network providers" to the application of policy. Defined standards with headers for each section to summarize contents. Changed consumers to "person served". Added Exhibit A-Email and PHI Compliance Tips to protect data and identify what PHI is.	10/14/2025	x	x	x	x	x	x	x	x
176	05.07.05	Reporting of Medicaid Fraud Waste and or Abuse	Defined standards with headers for each section to summarize contents.	10/14/2025	x	x	x	x	x	x	x	x
180	08.04.02.01	Break the Glass	New Policy outlining the policy around the Break the Glass process in Sentri.	11/12/2025	x	x	x	x	x	x	x	x
185	08.05.03.03	HITECH Breach Notification Protected Health Information	Updated language to ensure HIPAA Privacy and Security Rule compliance	11/12/2025	x	x	x	x	x	x	x	

214	08.05.14.01	Employee Ed. Employee Training Regarding the Use and Disclosure of PHI	Added additional reviewers. Mentioned that policy is in accordance with HIPAA Privacy/Security Rule, Michigan Mental Health Code, ect. Added Titles to Policy Sections to summarize contents. Added references for Security Rule, Documentation Standard, Michigan Mental Health Code, and the Privacy Rule to Support Reproductive Health Care Privacy.	10/14/2025	x	x	x	x	x	x	x	x
217	08.05.14.02	Employee Ed. Employee Training on Privacy Awareness	Added additional reviewers. Mentioned that policy is in accordance with HIPAA Privacy/Security Rule, Michigan Mental Health Code, ect. Added Titles to Policy Sections to summarize contents. Added references for Security Rule, Documentation Standard, Michigan Mental Health Code, and the Privacy Rule to Support Reproductive Health Care Privacy. Add definitions to 08.05.00.01 for clarification: PHI, disclosure , use, workforce.	10/14/2025	x	x	x	x	x	x	x	x
221	08.05.15.01	Marketing - Using and Disclosing PHI for Marketing	Added additional reviewers. Mentioned that policy is in accordance with HIPAA Privacy/Security Rule, Michigan Mental Health Code, ect. Added Titles to Policy Sections to summarize contents. Added Standards to retain all authorizations for 6 years and marketing related activities must be pre-approved by CEO and Compliance Officer. Add references to Michigan Mental Health Code, 42 CFR Part 2, SCCMHA POLICY 08.05.01	10/14/2025	x	x	x	x	x	x	x	x
225	08.05.16.01	Recordkeeping-Documentation	Mentioned that policy is in accordance with HIPAA Privacy/Security rule, Michigan Mental Health Code, Etc. Added Titles to Policy sections to summarize contents. Add definitions to 08.05.00.01 for clarification: PHI, documentation, use, disclosure. Added references to HIPAA Privacy & Securitry Rule, Michigan Mental Health Code and 42 CFR Part 2.	10/14/2025	x	x	x	x	x	x	x	
229	08.05.17.03	Individual Rights to PHI - Suspension	Mentioned that policy is in accordance with HIPAA Privacy/Security Rule, Michigan Mental health Code, etc. Added Titles to policy sections to summarize contents. Added definitions to 08.05.00.01 for clarification: PHI, documentation, use, disclosure. Add standard for document retention.	10/14/2025	x	x	x	x	x	x	x	
233	08.06.00.01	Information Technology Definitions	Updated definitions and added ones from new and existing policies.	11/12/2025	x	`x	x	x	x	x	x	x
241	08.06.04	HIPPA Security, Security Sanctions	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance.	11/12/2025	x	x	x	x	x	x	x	x
245	08.06.08.01	HIPPA Security, Security Management Process	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. OCR has increased enforcement around BAAs and vendor due diligence – added language to close compliance gap. Added language for Security Risk Assessment process.	11/12/2025	x	x	x	x	x	x	x	x
252	08.06.08.02	HIPPA Security, Assigned Security Responsibility	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance.	11/12/2025	x	x	x	x	x	x	x	x

256	08.06.08.03	HIPPA Security, Workforce Security	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. BAA Oversight added to comply with OCR increased enforcement for vendor due diligence.	11/12/2025	x	x	x	x	x	x	x	x
263	08.06.08.04	HIPPA Security, Information Access Management	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. OCR has increased enforcement around BAAs and vendor due diligence – added language to close compliance gap. Added language regarding Remote access controls in preparation for VPN setup being completed soon.	11/12/2025	x	x	x	x	x	x	x	x
269	08.06.08.05	HIPPA Security, Security Awareness and Training	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language from updated process for Security training via KnowBe4 that was implemented in March 2025.	11/12/2025	x	x	x	x	x	x	x	x
276	08.06.08.06	HIPPA Security, Security Incident Procedures	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding risk assessments, document retention, and breach procedures.	11/12/2025	x	x	x	x	x	x	x	x
281	08.06.08.07	HIPPA Security, Contingency Plan	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding encryption, backup retention, and care continuity.	11/12/2025	x	x	x	x	x	x	x	x
288	08.06.08.08	HIPPA Security, Evaluation	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding security and risk assessments. Added language regarding BAA responsibilities in areas of audit and compliance.	11/12/2025	x	x	x	x	x	x	x	x
294	08.06.08.09	HIPPA Security, Business Associate Agreements (BBAs) and Other Arrangements	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. OCR has increased enforcement around BAAs and vendor due diligence – added language to close compliance gap.	11/12/2025	x	x	x	x	x	x	x	x
301	08.06.10.1	HIPPA Security, Facility Access Controls	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding environmental monitoring, lost badges, BAA requirements, document retention, and training.	11/12/2025	x	x	x	x	x	x	x	x
308	08.06.10.04	HIPPA Security, Device and Media Controls	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language on how devices should be transported and disposed of including adding Shred Experts as the vendor with a BAA on file with SCCMHA.	11/12/2025	x	x	x	x	x	x	x	x
315	08.06.12.02	HIPPA Security, Audit Controls	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. OCR has increased enforcement around BAAs and vendor due diligence – added language to close compliance gap. Added language for risk assessments, document retention, training and reporting requirements.	11/12/2025	x	x	x	x	x	x	x	x

323	08.06.12.03	HIPPA Security, Integrity	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding unapproved devices when accessing PHI, having public facing workstations, and phishing prevention.	11/12/2025	x	x	x	x	x	x	x	x
329	08.06.12.04	HIPPA Security, Person or Entity Authentication	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding authentication and applicable system. Added language around role-based control, updated process for onboarding and offboarding.	11/12/2025	x	x	x	x	x	x	x	x
336	08.06.12.05	HIPPA Security, Transmission Security	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language around MFA,Encryption standards,documentation retention, datasensitivity and sharing to the cloud. Added language around reinforcement including automatedalerts, training and role based control emphasis	11/12/2025	x	x	x	x	x	x	x	x
342	08.06.12.06	Controlled Access and Least Privilege Access Policy	New Policy outlining extensive controlled access and least privilege for all IT systems.	11/12/2025	x	x	x	x	x	x	x	x
369	08.06.12.07	Guest User Access Policy	New Policy outlining the policy around the Guest User Access Policy for Microsoft Teams.	11/12/2025	x	x	x	x	x	x	x	x
373	08.06.16.01	HIPPA Security, Policies, Procedures and Documentation	Updated language and references to ensure HIPAA Privacy and Security Rule and 42 CFR Part 2 compliance. Added language regarding training, documentation, access controls, backup and recovery.	11/12/2025	x	x	x	x	x	x	x	x
379	08.06.40	HIPPA Security, Data Backup and Storage	Updated language and references to ensure HIPAA Privacy and Security	11/12/2025	x	x	x	x	x	x	x	x
N/A	**Tab 6- Recipient Rights - Customer Service - Appeals & Grievance - No Updates**											
384	**Tab 7-Claims Processing**											
385	05.02.06	Financial Liability for Mental Health Services	Overall review, no new changes required. Reviewer added – Finance Manager	11/1/2025	x	x	x	x	x	x	x	x
389	09.10.01.01	Contracted Network Provider Claims Submission	Reviewed		x	x	x	x	x	x	x	x
393	09.10.01.01.01	Electronic Claims Submission by Provider	Reviewed		x	x	x	x	x	x	x	x
412	09.10.01.01.05	UB 04 (CMS-1450) Uniform Billing Form Instructions	Reviewed				x					
417	09.10.01.01.13	Provider Network Appeal Process for Claim Payment Denial	Reviewed		x	x	x	x	x	x	x	x
420	**Tab 8-Network Services**											
421	09.04.05.08	MDHHS Universal Credentialing for Licensed Clinical Staff	New Procedure	10/1/2025					x			
N/A	**Booklets & Brochures-No Update**											

Tab 2

Eligibility & Care Management

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Diagnosis in Medical Record, Billing, and Reporting</td><td>Chapter: 03 - Continuum of Care</td><td>Subject No. 03.01.06</td></tr>
<tr><td rowspan="2">Effective Date:
September 10, 2019</td><td>Date of Review/Revision:
12/8/2020, 10/11/22, 11/12/24, 08/13/25, 11/01/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Chief Finance Officer and Chief Operations Officer

Authored By:
Linda Tilot

Reviewed By:
Director of Network Services, Public Policy and Continuing Education
Finance Manager</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure the integrity of the diagnosis in the Medical Record and the application of the diagnosis in treatment, billing, reporting and claims payment.

Policy:
SCCMHA shall establish a system of policies and controls to ensure compliance with applicable laws and regulations governing the creation and use of medical diagnosis for treatment, payment and operations.

Application:
All credentialed health professionals in the SCCMHA provider network and associated billing providers.

Standards:

1. Electronic Health Record (EHR): SCCMHA uses a fully electronic health record with no paper records maintained. All patient care documents are either created in the EHR or scanned into the EHR and stored electronically. The EHR shall be the sole source of diagnosis for Treatment, Payment and Operations.

2. Meaningful Use Certified EHR: The SCCMHA electronic medical record shall be a meaningful use certified product based on the current federal and state Health IT Certification Criteria.

3. Electronic Billing and Claims Payment: SCCMHA shall submit claims using ICD10 diagnosis codes which are derived from the electronic health record.

Definitions:
Case Holder: Individual with primary responsibility for the care plan in the electronic health record.

Diagnostic Statistical Manual of Mental Disorders (DSM): This is a publication of the American Psychiatric Association and is a clinician's guide for establishing a diagnosis of mental disorders. The multi-axial construct created by the DSM continues to be used in the Electronic Health Record and among behavioral health practitioners. However, the multi-axial construct is not supported in the ICD-10 the DSM V removed the distinctions of Axis I, II, and III created a single position. SCCMHA uses the current version of the DSM as a guide for clinical assessment

Electronic Health Record (EHR): SCCMHA uses a fully electronic health record with no paper records maintained. All patient care documents are either created in the EHR or scanned into the EHR and stored electronically.

International Classification of Disease: SCCMHA uses the current version of the ICD diagnosis codes and purchases this through the Electronic Health Record.

Meaningful Use: The SCCMHA electronic medical record is a meaningful use certified product based on the 2015 Edition of the Health IT Certification Criteria.

Medical Necessity: Health care services and supplies provided by health care entities in order to prevent, diagnosis or treat and a disease, condition, illness or injury and consistent with the applicable standards of medicine.

Behavioral Health Treatment Episode Data Set BH TEDS: This is a data set established by the Substance Abuse and Mental Health Administration to allow for nationally standardized program evaluation. It's relevance to this policy is that it includes the patient diagnosis for both mental health and substance use disorders.

Mental Health Professional (Adult): [Mental Health Code, Section 330.1100b(15)] - An individual who is trained and experienced in the area of mental illness or developmental disabilities and who is one of the following: a physician, psychologist, registered professional nurse licensed or otherwise authorized to engage in the practice of nursing under part 172 of the public health code (1978 PA 368, MCL 333.17201 to 333.17242), licensed master's social worker licensed or otherwise authorized to engage in the practice of social work at the master's level under part 185 of the public health code (1978 PA 368, MCL 333.18501 to 333.18518), licensed professional counselor licensed or other-

wise authorized to engage in the practice of counseling under part 181 of the public health code (1978 PA 368, MCL 333.18101 to 333.18177), or a marriage and family therapist licensed or otherwise authorized to engage in the practice of marriage and family therapy under part 169 of the public health code (1978 PA 368, MCL 333.16901 to 333.16915). NOTE: The approved licensures for disciplines identified as a Mental Health Professional include the full, limited and temporary limited categories.

Mental Health Professional (Child) (CMHP) - Individual with specialized training and one year of experience in the examination, evaluation, and treatment of minors and their families and who is a physician, psychologist, licensed or limited-licensed master's social worker, licensed or limited-licensed professional counselor, or registered nurse; or an individual with at least a bachelor's degree in a mental health-related field from an accredited school who is trained and has three years supervised experience in the examination, evaluation, and treatment of minors and their families; or an individual with at least a master's degree in a mental health-related field from an accredited school who is trained and has one year of experience in the examination, evaluation and treatment of minors and their families. For the BHT/ABA services individuals must be a BCBA or BCaBA or Psychologist working within their scope of practice with extensive knowledge and training on behavior analysis and BCBA certified by 9/30/2020.

Treatment Payment and Operations (TPO): This is a term established in HIPAA and HiTECH regulation which describes the allowed uses of protected and electronic health information which do not require separate patient permissions.

References:
Michigan Department of Health and Human Services: Michigan PIHP/CMHSP Provider Qualifications, current version

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1) Every consumer served by SCCMHA shall be given a provisional diagnosis in the EHR at the time of record creation.	1) CAI or Crisis Clinician
2) The provisional diagnosis shall be established by a mental health professional as defined by MDHHS (see definition section above).	2) Executive Director of Clinical Services and Programs
3) The provisional diagnosis shall remain in this status until reviewed and verified by the treating psychiatrist.	3) Executive Director of Clinical Services

	and Programs
4) All medical or physical health related diagnosis will be entered only by Physicians, Physician Assistants, or Nurse Practitioners and shall be based on confirmed diagnosis established by primary care or specialists. The role of the Integrated Health or Enhanced Health nurses in the SCCMHA provider network is the primary source of medical or physical health related diagnosis.	4) Executive Director of Clinical Services and Programs and Director of Enhanced Health and Integration
5) The Case Holder shall select the primary diagnosis from the Electronic Health Record for inclusion in the BH TEDS admission and discharge records as well as for billing purposes.	5) All Clinical Staff using EHR
6) Electronic billing shall be based on diagnosis from the electronic health record.	6) Chief Information Officer and Chief Financial Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Cost of Service and Explanation of Benefits</td><td>Chapter: 03 – Continuum of Care</td><td>Subject No: 03.01.07</td></tr>
<tr><td rowspan="2">Effective Date:
10/01/15</td><td>Date of Review/Revision:
3/14/17, 5/8/18, 9/10/19, 1/3/20, 11/12/24, 11/1/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Chief Financial Officer

Authored By:
Linda Tilot

Additional Reviewers:
Operations Committee</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To comply with Mid-State Health Network contractual requirements to perform the delegated function of providing consumers with information about their Estimated Annual Cost of Services and Explanation of Benefits. The purpose of the Cost of Services statement is to assist person(s) served in considering self-determined alternatives. The purpose of the Explanation of Benefits is to engage the person(s) served in monitoring for fraudulent claims paid on their behalf.

Application:
This function will be performed by SCCMHA for all persons served in the SCCMHA network.

Policy:
All persons served with a Person-Centered Plan will be provided an estimate of the annual cost of services which are included in the plan at the time of the plan. A sample of person(s) served will be provided an Explanation of Benefits which informs them of the services that have been paid for on their behalf.

Standards:
- Estimated Cost of Service statements will be provided to the person served with the PCP and at any time of change in the PCP or at the consumer's request.
- The estimated cost of services statement shall include information about self-determination.
- The estimated cost of services statement shall be included in the electronic health record with the PCP and updated in conjunction with changes in the PCP.
- The estimated cost of services statement will be included as a part of the PCP document and signed by the person served.

- The estimated cost of services statement will not include crisis and acute care services.
- The Explanation of Benefits shall be a retrospective statement of services paid for a defined period of time.
- The Explanation of Benefits statement shall include the name of the provider and a service description in terms that can be understood by the person(s) served.
- The Explanation of Benefits will include information for the person(s) served which introduces the document and its purpose.

Definitions:
Cost of Services: This is a prospective cost of services statement based on the authorization associated with the PCP and is based on current provider rates.

Explanation of Benefits: This is a retrospective cost of services statement based on paid claims.

References:
Michigan Department of Health and Human Services Technical Requirement P6.3.2.1.B.i f Estimated Cost of Services

Michigan Department of Health and Human Services Technical Requirement P6.3.e.1.B.ii Explanation of Benefits

Exhibits:
Exhibit A – Understanding Your Explanation of Benefits Statement brochure

Procedure:

ACTION	RESPONSIBILITY
1. The SCCMHA Electronic Health Record will include an Estimated Cost of Services explanation in the Person-Centered Planning document. The EHR will provide a summary of services requested for authorization at the time of the PCP in a sub section of the PCP document. This section will be available for inclusion with the PCP for consumer signature or as a document which can be separately printed for consumers upon their request.	1. Chief Information Officer
2. The Case Manager, Supports Coordinator or primary assigned clinician will explain the purpose of the Estimated Cost of Services document and how it can be used in a Self-Determined service agreement.	2. Primary Case holder

3. The Chief Financial Officer will create a random sample of 5% of consumers served to receive an Explanation of Benefits Statement. The sample shall change annually and participating persons shall be surveyed regarding the thoughts on whether the EOB was easy to understand and useful.	3. Chief Financial Officer
4. The statement will include all claims paid for in the prior quarter and shall be mailed to the person's served address of record.	4. Chief Financial Officer
5. The statement shall include information for the consumer about who to contact if they have questions or if they believe the information in the EOB is false.	5. Chief Financial Officer

The ABC's of an EOB (Explanation of Benefits)

Part of making the most of your mental health coverage is understanding how Saginaw County Community Mental Health Authority (SCCMHA) pays your claims and what your role is in the process. SCCMHA provides you with an important resource called an Explanation of Benefits (EOB) to do this.

Your EOB has a lot of useful information that may help you track your mental health care expenditures and serve as a reminder of the services that you have received from SCCMHA or one of our contracted providers.

When you receive your EOB statement, please check and make sure that the dates and services that you have received are correct. The services listed on the EOB should be consistent with your PCP (Person Centered Plan) in terms of the type and amount, as well as, reflect the services that you have actually received.

If any discrepancies are noticed, or if you have any questions regarding your EOB statement, please call our Member Services Representative at 989-797-3518.

What Information is in My EOB?

Consumer: The name of the person who received the service.

Service Provider: The name of the provider who performed the services for you. This may be the name of SCCMHA or one of our contracted providers.

Service Dates: The date(s) of the mental health related service you received from the Provider.

Service Description: A brief description of the mental health related service you received from the Provider.

Start/End Times: The start and end times of the service provided to you.

Total Charge: The total amount billed by the Provider to SCCMHA.

Total Paid to Provider: Total amount SCCMHA paid to the Provider for the cost of your services after all other insurances were billed and/or paid.

Member Services Information: The contact information (telephone/mailing address) for questions or concerns relating to your EOB.

Medicaid Deductible/ATP: The amount of your monthly Medicaid deductible and/or your monthly ability to pay.

Questions?

If you have a question about what a service is or means, you may refer to the "Service Description Section" in the SCCMHA Consumer Handbook, or you may call our Member Services Representative, Kim Hall, at 989-797-3518. She will be happy to assist you in any questions that you may have about your EOB.

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

500 Hancock Street
Saginaw, MI 48602

Phone: 800-258-8678 or 989-797-3400
TDD/TTY Line: 989-797-3460
Website: www.sccmha.org

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Waiting Lists</td><td>Chapter: 03 - Continuum of Care</td><td>Subject No: 03.01.01.06</td></tr>
<tr><td rowspan="2">Effective Date:
4/1/10</td><td>Date of Review/Revision:
6/11/13, 3/14/17, 3/9/18, 9/10/19, 12/8/20, 7/13/22, 5/20/24, 11/1/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Chief Financial Officer

Authored By:
Linda Tilot, Kim Hall

Additional Reviewers:
Finance Manager</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to ensure SCCMHA compliance with MDHHS contractual requirements and the CCBHC Guidelines regarding the use of waiting lists. The policy establishes protocols for administration of general fund person(s) served waiting list criteria for mental health services and the process for placing individuals on a waiting list when insufficient funding and/or resources exists. Waiting list information is used to assist SCCMHA's planning process to ensure needed services are being provided in a timely manner and waiting list census is reported annually to MDHHS as a part of the Annual Submission and community needs assessment.

Policy:
SCCMHA shall provide an adequate array of Mental Health Code required mental health services to persons most severely affected as well as those with mild to moderate mental health needs, according to the availability of resources. SCCMHA will work to assure that all persons will receive the needed services regardless of their insurance status or ability to pay. When resources are insufficient to address the needs of all individuals desiring to receive services from the public mental health system, SCCMHA will first work to link the person to a community resource that not only meets the individuals needs but is able to provide services in a timely manner. Should community resources not be available, the establishment of waiting list criteria and the process of waiting list maintenance shall be defined and administered according to this policy to ensure systematic access into services and ongoing service delivery.

If it is found that the demand for services consistently exceeds the availability of services within the system, SCCMHA will work to develop a Designed Collaborating Organization (DCO) relationship with a community partner to assure that needed services are available.
Application:

SCCMHA Administration and Provider Network

Standards:

- SCCMHA shall be required to provide services to any individual seeking behavioral health who has Mild, Moderate, Severe and Persistent Mental Illness, Serious Emotional Disturbance and/or Developmental Disability diagnosis, regardless of ability to pay, or access to other third-party payer sources. However, should insufficient mental health General Fund (GF) revenues or lack of resources not allow SCCMHA to address all local mental health needs for the Mental Health Code-defined priority populations, SCCMHA will link the individual with a community resource who is able to meet the individual's needs. SCCMHA shall offer to place these individuals on a waiting list and shall manage the waiting list in accordance with the standards contained in this policy guideline. An individual has a right to decline being placed on a waiting list.
- All Medicaid, Healthy Michigan, and/or MI Child beneficiaries who meet admission criteria shall immediately receive all medically necessary services and shall not be placed on a waiting list.
- Individuals who are in emergent or urgent situations will immediately receive crisis intervention services and will not be placed on a waiting list while in a crisis situation. However, once the individual is stabilized, they may be placed on a waiting list.

Definitions:

Waiting List

A waiting list is:

1. A list of uninsured and indigent only a person(s) served who meets eligibility criteria, but due to insufficient GF (General Fund) and/or services/resources, the service they request or require is not currently available.
2. A list of a person(s) served who are uninsured and indigent and are currently active to SCCMHA, however, due to insufficient funding, services contained in their person-centered plan are reduced or terminated.

References:

1. Michigan Mental Health Code; Act 258 of the Public Acts of 1974 as amended:
   Chapter 1, Sec. 330.1124 (2)
   Chapter 2, Sec. 330.1100c (6)
   Chapter 2, Sec. 330.1206
2. Michigan Department of Health and Human Services Technical Advisory Guidelines for Establishing and Managing General Fund Waiting Lists

3. CARF Standard, Sec. 2.B., Screening and Access to Services

Exhibits:

Exhibit 1: Population Cell Grid
Exhibit 2: Sample Waiting List Notification Letter
Exhibit 3: Sentri Medical Record Waiting List Data Collection Template

Exhibit 4: SCCMHA Outpatient Referrals

Procedure:

ACTION	RESPONSIBILITY
1. In accordance with the MDHHS Specialty Supports and Services Contract, the SCCMHA Board of Directors and Chief Executive Officer shall ensure that the service array provided to the eligible persons is adequate and the available general fund resources are allocated to support services to those most severely affected. When it is determined by the Chief Executive Officer that SCCMHA is unable to financially meet requests for non-emergent public mental health services for non-Medicaid, non-Healthy Michigan or non-MI Child persons deemed eligible for SCCMHA services, those persons shall be placed on a waiting list until funding becomes available.	1. SCCMHA Board of Directors and Chief Executive Officer
2. The Chief Executive Officer will ensure that all SCCMHA policies and procedures related to establishing waiting lists will be available to all individuals seeking services, those currently in services and to the general public.	2. Chief Executive Officer
3. The Executive Director of Clinical Services and Programs shall ensure that screening, access and assessment services are in place which ensure that: a) all non-emergent, non-Medicaid, non-Healthy Michigan, and non-MI Child persons requesting services are apprised of the waiting list criteria, b) that they are provided assistance with accessing alternative services, c) offered a face to face assessment of their eligibility when they are dissatisfied with recommendations following screening or the need for emergent crisis intervention services (d) are offered placement on the waiting list.	3. Executive Director of Clinical Services and Programs
4. For <u>Adults with Mental Illness</u>: SCCMHA may link the individual with a community provider who can meet the individual's needs, if resources are not available within the agency utilizing the "Outpatient Referral" list and complete a warm hand off (coordination of the appointment). If the	4. Central Access and Intake (CAI) Specialist

individual refuses the referral and wishes, SCCMHA may place a G.F. (General Fund) consumer on a waiting list through a telephonic clinical screening by SCCMHA in which the LOCUS (Level of Care Utilization System) assessment conducted by the Central Access and Intake (CAI) unit determines that the G.F. individual does not meet a minimum LOCUS score of 28. Screening results and LOCUS decision will be documented in the Sentri medical record (eligibility screening and LOCUS Assessment sections).	
5. For Persons with Developmental Disabilities: No waiting list will be implemented as of this policy date.	5. Central Access and Intake (CAI) Specialist
6. For Children with Serious Emotional Disturbance: Children between the ages of 7-12 a CAFAS score of 90 or for children between the ages of 13-18 a CAFAS score of 120 or higher will be linked with a community provider who can meet the individual's needs, if resources are not available within the agency utilizing the "Outpatient Referral" list and complete a warm hand off (coordination of the appointment). If the individual refuses the referral and wishes, they will be offered to be placed on the waiting list, with those assessed with a composite CAFAS greater than 90 for children 7-12 or greater than 120 for children 13-18 being offered immediate admission to services.	6. Central Access and Intake (CAI) Specialist
7. SCCMHA link the individual with a community provider who can meet the individual's needs, if resources are not available with in the agency utilizing the "Outpatient Referral" list and complete a warm hand off (coordination of the appointment). If the individual refuses the referral and wishes, SCCMHA will place a person(s) served on a waiting list after a face-to-face intake assessment in which the LOCUS (Level of Care Utilization System) assessment conducted by the Central Access and Intake (CAI) Specialist determines that the G.F. individual does not meet a minimum LOCUS score of 28. Eligibility assessment results and LOCUS decision will be	7. Central Access and Intake (CAI) Specialist

documented in the Sentri medical record (eligibility intake assessment and LOCUS Assessment sections).	
8. SCCMHA may place an active general fund consumer on a waiting list if insufficient funding warrants a reduction or termination of services, as contained in their person-centered plan.	8. Care Management Specialist
9. SCCMHA will inform all eligible general fund front-door applicants and active SCCMHA general fund person(s) served who have had their services denied, reduced, terminated, or suspended due to insufficient general fund resources, of their right to request a review of the waiting list decision within 14 days of the date of written notification. The applicant/active SCCMHA person(s) served shall be informed of this opportunity both verbally and in writing. Written notice will be sent within three (3) business days and include the following: (1) service for which the individual is on a waiting list, (2) instructions on what the individual should do if his/her situation changes, including obtaining Medicaid coverage or obtaining Healthy Michigan coverage. (3) the individual's right to have the decision reviewed if they disagree with the waiting list decision. Copy of letter will be scanned into the Sentri Medical Record.	9. Central Access and Intake (CAI) Specialist
10. In the event consumer requests review of waiting list decision, SCCMHA will ensure the review occurs within five (5) business days from the date of request by the Central Access and Intake (CAI) Supervisor. A person in an urgent situation shall be entitled to an expedited review and shall have their request processed within two (2) business days from the date of request. Decision will be documented in the Sentri Waiting List form and applicant/active SCCMHA person(s) served shall be informed in writing of the review disposition within (3) business days.	10. Supervisor of Care Management
11. SCCMHA will ensure that the order of priority on the waiting list shall be based on the individual's severity and urgency of need (MH Code,	11. Supervisor Care Management

330.1124(2). Prioritization will include the following: (1) front-door applicants waiting for access into SCCMHA, (2) active SCCMHA consumers who have had their services reduced, limited, suspended, or terminated due to insufficient funds.	
12. SCCMHA will designate a MA-level clinician in the Central Access and Intake (CAI) unit to maintain the waiting list including periodic calls to ask consumers if they are still interested in services and to rate the severity of their need.	12. Central Access and Intake (CAI) Specialist
13. Waiting list will be maintained in the Sentri medical record and include name, age, gender, type of service needed, disability designation, diagnostic group, date placed on the list, severity of need and rationale for decision to be placed on the waiting list.	13. Central Access and Intake (CAI) Specialist
14. SCCMHA will ensure that the waiting list is reviewed on a regular basis, but not less than quarterly. Review activities shall be documented and include removal of names of persons offered services, removal of names of persons who request to be removed from the waiting list, re-prioritization of the waiting list according to an individual's changing urgency and severity of needs, and documentation of the reasonable attempts to contact the individuals to determine if they wish to stay on the list or if they have experienced any change in situation.	14. Supervisor Central Access and Intake
15. The Chief Executive Officer shall periodically (no less than annually) report summary information related to the waiting list to its Governing Board via the Ends Committee.	15. Chief Executive Office
16. The Chief of Quality Information and Compliance will annually submit the required waiting list data to MDHHS as required in the MDHHS/CMHSP Contract.	16. Chief of Quality Information and Compliance

Exhibit 1: Population Cell Grid

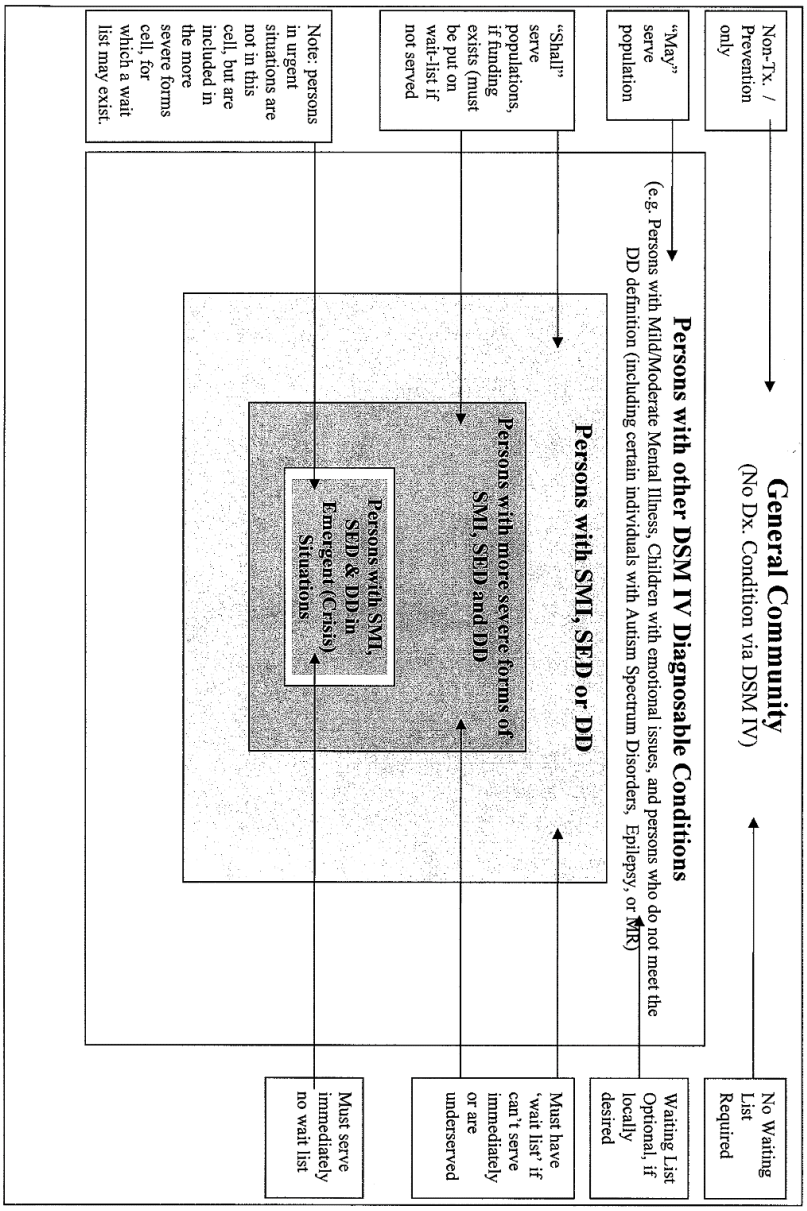


Exhibit 2: Sample Waiting List Notification Letter

DATE

Consumer Name
Address
City, State, Zip

Dear: _____

As a result of your request for mental health services on _____ (date), it has been determined that you meet criteria for the following service: (identify service type). However, due to inadequacy of current funding, you are being placed on a waiting list for service.

You have the right to request a review of this decision. If you would like to request a review of this decision or have questions about this action, please contact us within 14 days from the date of this letter at:

Saginaw County Community Mental Health Authority
Attn: Central Access and Intake Unit
500 Hancock
Saginaw, MI 48601

If your situation changes, if you wish your name removed from the waiting list, or you are experiencing a mental health emergency, please contact the Central Access and Intake Unit at 989-797-3559, 989-792-9732, or toll free at 1-800-233-0022.

Sincerely,

Staff
Title

Exhibit 3: Sentri Medical Record Waiting List Data Collection Template

Adding consumer to waiting list:

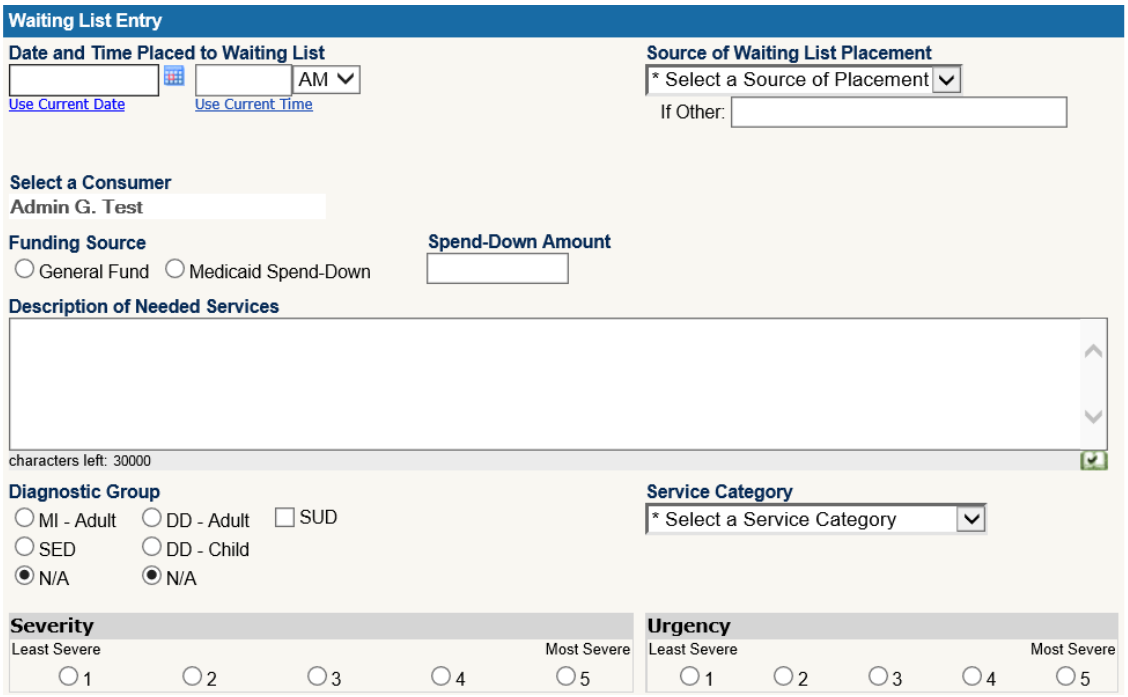


Exhibit 4: SCCMHA Outpatient Referrals

SCCMHA OUTPATIENT REFERRALS

Catholic Family Services 710 N Michigan Ave, Saginaw, MI 48602 (989)753-8446		Children, family, and couple counseling. Open to everyone. Helps with Guardianship. Substance abuse.		All forms of Medicaid, Private insurance: BCBS, Aetna, Cigna, sliding fee scale
Child and Family Services 2838 Automotive Centre Rd, Saginaw, MI 48603 (989) 790-7500		Counseling for children and families, Sexual Assault center.		Medicaid, private insurance: BCBS, Aetna, Cigna, sliding fee scale
David E. Gaffney LMSW 5090 State St., Ste. 103-B Saginaw, MI 48603 (989) 980-1233		Provides counseling for individuals, familes and groups who are verbal and willing to participate, 6+ and older; trauma, chronic pain, sleep		Medicaid; private insurance: BCBS/BCN, Aetna, Cigna Sliding fee scale
Great Lakes Bay Health 3023 Davenport Ave, Saginaw, MI 48602 (989) 907-2761		Adults and children. Therapy and psychiatry. Substance abuse		All forms of Medicaid, Medicare, Private insurances: BCBS/BCN, Aetna, Cigna, Self pay, no insurance
Great Lakes Psychological Services 4901 Towne Centre Rd Ste 205, Saginaw, MI 48604 (989)921-5715		Fully licensed psychologists providing psychotherapy and assessment services for all ages		NO Medicaid. BCBS, Medicare, ASR, Aetna, Cofinity, BCN and several others
Guided Grace Family and Youth services 1232 N Michigan Ave, Saginaw, MI 48602 (989)401-8990 ext. 204 (Dana Simmons)		Services for childen and adults. Family and marital therapy, groups. CBT, DBT		All forms of Medicaid; Private insurances accepted: Aetna, BCBS of MI, BCN, BC complete, Cigna, 1st Health Network; NO LONGER accept HAP, Molina and Priority Health

HealthSource Saginaw Behavioral Medicine Center 3340 Hospital Rd, Saginaw, MI 48603 (989) 790-7700		Children, adolscents, adults, couples/families. Co-occuring, gambling. Psychiatry		Molina, McLaren and Meridian mediciad. Most private insurances: BCBS/BCN, Aetna, Cigna
Healthy Psyche Therapy TELEHEALTH ONLY, All Michigan Residents (989) 220-1204 www.healthypsychetherapy.com		Trauma, PTSD, Couples/marriage counseling, depression, anxiety. Morning, afternoon, and evening sessions		Meridian and McLaren Medicaid; Medicare, Blue Cross Complete
Hope Christian Counseling 1711 Court St, Saginaw, MI 48602 (no phone number listed)		Faith-based counseling for individuals and families. Marriage and family therapy. Substance abuse evaluations		Medicaid, McLaren, Cigna, BCBS, Meridian
Hospital Psychiatry 3085 Hallmark Ct suite 1, Saginaw, MI 48603 (989)790-7742		Psychiatry		Private insurances: BCBS/BCN, Aetna, Cigna
JPS services (Dr. Jafferany) is now CMU Health 3201 Hallmark Ct. Saginaw, MI 48603 (989)790-5990		Adults and children. Psychiatry		Medicare, most Private insurances: BCBS, Aetna, Cigna
List Psychological 5024 North Center Road Saginaw, MI 48604 (989)790-3130		Services for children and adults. Therapy, psychiatry, substance abuse, Seniors, LGBTQ		Meridian, Molina, McLaren medicaid, Medicare, most private insurances. Sliding fee
Maple Leaf Counseling 7950 Gratiot Rd, Saginaw, MI 48609 (989)714-4793		Services for children and adults. Trauma, LGBTQ		Meridian and McLaren Medicaid, BCBS, BCN, ASR, Cigna and several others. Self pay/sliding fee scale
McDowell Healing Arts Center 3253 Congress Ave. Saginaw, MI 48602 (989) 475-4171		Services for children and adults. Couples and family counseling. Nights and weekends. Telehealth		All forms of Medicaid, BCBS, BCN, HAP, Cigna, Priority Health, Aetna, Medicare, ASR and several others

Michigan Comprehensive Counseling 1300 N Michigan Ave, Saginaw, MI 48602 (989)752-1668		Child-centered and family-focused counseling. Anger management, Substance abuse, Domestic violence		All forms of Medicaid, Cigna, Humana, BCBS, and several others
Professional Psychological and Psychiatric Services 1010 Niagara Suite St Suite #1 Saginaw, MI 48602 (989) 401-5562		Anger management, Substance abuse. Psychiatry. Individual, families and groups. Sex Offender Counseling		All forms of medicaid, Cigna, BCN, Omnicare, most other insurances, and offers sliding fee
Renewal Christian Counseling Center 6030 Bay Rd, Saginaw, MI 48604 (989) 244-1888		Counseling for adults and children. Faith based. Psychiatry. Telehealth		Aetna, BCBS, BCN, Cofinity, Beacon Health, Cigna, Hap, McLaren, Medicaid, Medicare, Tricare and sliding fee
Saginaw Psychological 2100 Hemmeter Rd, Saginaw, MI 48603 (989)799-2100		Therapy, psychiatry for children and adults. Play therapy, DBT, Substance Abuse, ADHD testing		All forms of medicaid; Private: BCBS/BCN, Aetna, Cigna, HAP, Medicare, Tri-Care, Humana
Solutions Behavioral Health 1010 N Niagara St #2, Saginaw, MI 48602 (989)401-5562		Therapy for children and adults		All forms of medicaid; Private: Aetna, BCBSM/BCN, HAP, Tri-Care Sliding Fee Scale
State Street Behavioral Services 4713 State Street. Saginaw, MI 48603 (989)270-1749		Services for children and adults. Autism services, Alzheimer's and Dementia. Dr. Tadeo works here		Medicaid, Medicare, BCBS, BCN, Humana, Cigna, HAP, ASR, Tri-Care, Aetna and several others
Talasila Clinic 2578 McLeod Dr N STE 1, Saginaw, MI 48604 (989) 799-5440		Psychiatry		Private insurances: BCBS/BCM, Aetna, Cigna Most commercial insurances
Tri-County Mental Health Therapists 9453 Kochville Rd Suite 1, Freeland, MI 48623 (989)573-8120		Services for children over the age of 11 yrs. and adults. Family/couple therapy. Groups and Telehealth		**NO Medicaid, Medicare, Cigna, Priority Health or Beacon**. Private insurances accepted: BCBS, BCN, Optum, United Health (commercial), McLaren

				Health (commercial), Aetna, HAP, ASR
Westlund Guidiance Clinic 203 M-13, Saginaw, MI 48607 (SVRC Marketplace) (989)793-4790		Children ages 3 and up. Adults. Therapy, psychiatry. Autism, school based therapy. Substance abuse		All forms of Medicaid, Medicare; Private: BCBS, BCN, JAP, Aetna, United Health Care, Priority Health
Peer Warmline 1 (888) 733-7753		The warmline will operate seven days a week from 10:00am to 2:00am and gives the caller a peer to talk to		
National Suicide Prevention Lifeline 24/7 at 1 (800) 273-8255		For individuals in crisis, including those considering suicide		
CRISIS TEXT LINE Text HOME to 741741		Text HOME to 741741 from anywhere in the USA to text with a trained Crisis Counselor		

Tab 4

Service Delivery

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Recovery</td><td>Chapter: 02 - Customer Services and Recipient Rights</td><td>Subject No: 02.03.05</td></tr>
<tr><td rowspan="2">Effective Date:
7/20/06</td><td>Date of Review/Revision:
5/18/09, 6/7/12, 6/3/13, 6/2/14, 4/4/16, 6/13/17, 4/10/18, 3/11/18, 4/9/19, 4/7/20, 4/13/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:
None</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to inculcate an overarching philosophy of recovery, delineate a framework for the provision of strengths-based recovery and resilience focused services and supports, and to provide a structure for the provision of opportunities that support and foster recovery among persons served.

Policy:
All services and supports for persons served and their families shall be provided within the context of a true collaborative partnership which fosters shared decision-making and instills hope and a belief that persons served can recover. SCCMHA shall assist each person served to learn to effectively approach each day's challenges, acquire skills to live independently, and contribute to society in meaningful ways. This includes addressing all of the determinants of health (social and medical) that impact the person served.

Application:
This policy applies to all SCCMHA-funded providers of mental health and substance use disorder prevention, treatment, and recovery services.

Standards:
A. SCCMHA shall adhere to the fundamental components of recovery set forth by the Substance Abuse and Mental Health Services Administration (SAMHSA) in December 2011, which are follows:
   1. Four major dimensions that support a life in recovery:
      a. **Health:** Overcoming or managing one's disease(s) or symptoms – for example, abstaining from use of alcohol, illicit drugs, and non-prescribed medications if one has an addiction problem – and for

everyone in recovery, making informed, healthy choices that support physical and emotional wellbeing.

b. **Home:** A stable and safe place to live.

c. **Purpose:** Meaningful daily activities, such as a job, school, volunteerism, family caretaking, or creative endeavors, and the independence, income and resources to participate in society.

d. **Community:** Relationships and social networks that provide support, friendship, love, and hope.

2. Ten Guiding Principles of Recovery:

a. **Recovery emerges from hope:** The belief that recovery is real provides the essential and motivating message of a better future – that people can and do overcome the internal and external challenges, barriers, and obstacles that confront them. Hope is internalized and can be fostered by peers, families, providers, allies, and others. Hope is the catalyst of the recovery process.

b. **Recovery is person-driven:** Self-determination and self-direction are the foundations for recovery as individuals define their own life goals and design their unique path(s) towards those goals. Individuals optimize their autonomy and independence to the greatest extent possible by leading, controlling, and exercising choice over the services and supports that assist their recovery and resilience. In so doing, they are empowered and provided the resources to make informed decisions, initiate recovery, build on their strengths, and gain or regain control over their lives.

c. **Recovery occurs via many pathways:** Individuals are unique with distinct needs, strengths, preferences, goals, culture, and backgrounds – including trauma experiences – that affect and determine their pathway(s) to recovery. Recovery is built on the multiple capacities, strengths, talents, coping abilities, resources, and inherent value of each individual. Recovery pathways are highly personalized. They may include professional clinical treatment; use of medications; support from families and in schools; faith-based approaches; peer support; and other approaches. Recovery is non-linear, characterized by continual growth and improved functioning that may involve setbacks. Because setbacks are a natural, though not inevitable, part of the recovery process, it is essential to foster resilience for all individuals and families. Abstinence from the use of alcohol, illicit drugs, and non-prescribed medications is the goal for those with addictions. Use of tobacco and non-prescribed or illicit drugs is not safe for anyone. In some cases, recovery pathways can be enabled by creating a supportive environment. This is especially true for children, who may not have the legal or developmental capacity to set their own course.

d. **Recovery is holistic:** Recovery encompasses an individual's whole life, including mind, body, spirit, and community. This includes addressing: self-care practices, family, housing, employment,

education, clinical treatment for mental disorders and substance use disorders, services and supports, primary healthcare, dental care, complementary and alternative services, faith, spirituality, creativity, social networks, transportation, and community participation. The array of services and supports available should be integrated and coordinated.

e. **Recovery is supported by peers and allies:** Mutual support and mutual aid groups, including the sharing of experiential knowledge and skills, as well as social learning, play an invaluable role in recovery. Peers encourage and engage other peers and provide each other with a vital sense of belonging, supportive relationships, valued roles, and community. Through helping others and giving back to the community, one helps one's self. Peer-operated supports and services provide important resources to assist people along their journeys of recovery and wellness. Professionals can also play an important role in the recovery process by providing clinical treatment and other services that support individuals in their chosen recovery paths. While peers and allies play an important role for many in recovery, their role for children and youth may be slightly different. Peer supports for families are very important for children with behavioral health problems and can also play a supportive role for youth in recovery.

f. **Recovery is supported through relationship and social networks:** An important factor in the recovery process is the presence and involvement of people who believe in the person's ability to recover; who offer hope, support, and encouragement; and who also suggest strategies and resources for change. Family members, peers, providers, faith groups, community members, and other allies form vital support networks. Through these relationships, people leave unhealthy and/or unfulfilling life roles behind and engage in new roles (e.g., partner, caregiver, friend, student, employee) that lead to a greater sense of belonging, personhood, empowerment, autonomy, social inclusion, and community participation.

g. **Recovery is culturally-based and influenced:** Culture and cultural background in all of its diverse representations – including values, traditions, and beliefs – are keys in determining a person's journey and unique pathway to recovery. Services should be culturally grounded, attuned, sensitive, and competent, as well as personalized to meet each individual's unique needs.

h. **Recovery is supported by addressing trauma:** The experience of trauma (such as physical or sexual abuse, domestic violence, war, disaster, and others) is often a precursor to or associated with alcohol and drug use, mental health problems, and related issues. Services and supports should be trauma-informed to foster safety (physical and emotional) and trust, as well as promote choice, empowerment, and collaboration.

i. **Recovery involves individual, family, and community strengths and responsibility:** Individuals, families, and communities have strengths and resources that serve as a foundation for recovery. In addition, individuals have a personal responsibility for their own self-care and journeys of recovery. Individuals should be supported in speaking for themselves. Families and significant others have responsibilities to support their loved ones, especially for children and youth in recovery. Communities have responsibilities to provide opportunities and resources to address discrimination and to foster social inclusion and recovery. Individuals in recovery also have a social responsibility and should have the ability to join with peers to speak collectively about their strengths, needs, wants, desires, and aspirations.

j. **Recovery is based on respect:** Community, systems, and societal acceptance and appreciation for people affected by mental health and substance use problems – including protecting their rights and eliminating discrimination – are crucial in achieving recovery. There is a need to acknowledge that taking steps towards recovery may require great courage. Self-acceptance, developing a positive and meaningful sense of identity, and regaining belief in one's self are particularly important.

3. SCCMHA shall include the following additional components of recovery when working with current members of the armed forces and veterans:
   a. Privacy
   b. Security
   c. Honor
   d. Support for VA patient rights
4. SCCMHA shall adhere to the 16 Guiding Principles of a Recovery Oriented System of Care (ROSC) for persons with substance use disorders:
   a. Adequately and flexibly financed
   b. Inclusion of the voices and experiences of recovering individuals, youths, families, and community members
   c. Integrated strength-based services
   d. Services that promote health and wellness will take place within the community
   e. Outcomes driven
   f. Family and significant others involvement
   g. System-wide education and training
   h. Individualized and comprehensive services across all ages
   i. Commitment to peer support and recovery support services
   j. Responsive to cultural factors and personal belief systems
   k. Partnership-consultant relationship
   l. Ongoing monitoring and outreach
   m. Research-based
   n. Continuity of care
   o. Strength-based

p. Promote community health and address environmental determinants to health

5. Service providers will work with persons served to help them develop recovery plans that:
   a. Enable each person served to identify goals for achieving wellness
   b. Specify what each person served can do to reach those goals
   c. Include daily activities as well as longer term goals
   d. Track any changes in a mental health problem experienced by the person served
   e. Identify triggers or other stressful events that can make a person served feel worse, and help them learn how to manage those triggers/stressful events
   f. Foster person served self-care
   g. Are family-driven and youth-guided

B. Support for recovery shall include ensuring that comorbid general health conditions are addressed in a whole-person manner.
   1. Providers shall offer self-management support to activate persons served to self-manage their care, collaborate with providers, and to maintain their health.
   2. Case Holders shall ensure coordination of care among all practitioners and programs, including medical services to address comorbid general health conditions.
      a. Services, supports and coordination shall be provided within the context of an interdisciplinary team approach to care.
      b. Providers shall address the social determinants of health as well as ensure that the medical determinants of health are addressed.

C. Recovery support services shall include peer support as well as assistance with addressing the social determinants of health (see definition below).
   1. SCCMHA providers shall work to remove barriers and address health disparities.

Definitions:

Care Coordination: The Agency for Healthcare Research and Quality (2014) defines care coordination as *involving deliberately organizing care activities and sharing information among all of the participants concerned with a patient's care to achieve safer and more effective care. This means that the [person's] needs and preferences are known ahead of time and communicated at the right time to the right people, and that this information is used to provide safe, appropriate, and effective care to the [person served]*.

Health Coaching: The use of evidence-based skillful conversation, clinical interventions and strategies to actively and safely engage persons served in health behavior change. Health coaches focus on helping persons served who may have chronic conditions or those at moderate to high risk for chronic conditions take charge of their lives.

Michigan's ROSC Definition: Michigan's recovery-oriented system of care supports an individual's journey toward recovery and wellness by creating and sustaining networks of formal and informal services and supports. The opportunities established through collaboration, partnership and a broad array of services promote life enhancing recovery and

wellness for individuals, families and communities. (Adopted by the ROSC Transformation Steering Committee, 2010)

Recovery: A process of change through which individuals improve their health and wellness, live a self-directed life, and strive to reach their full potential. (SAMHSA, 2011) According to the National Consensus Statement on Mental Health Recovery, "*Mental health recovery is a journey of healing and transformation enabling a person with a mental health problem to live a meaningful life in a community of his or her choice while striving to achieve his or her full potential.*"

Recovery Coaching: A peer-based service that is provided by persons who are in recovery and, as a result, have gained knowledge on how to attain and sustain recovery. Also known as peer mentoring, recovery coaching entails the provision of strengths-based support to individuals with addictive disorders and those who are in recovery from alcohol, other drugs, codependency, or other addictive behaviors. It focuses on achieving goals that are of importance to the individual and is a type of partnership in which the person in or seeking recovery self-directs their own recovery while the coach provides expertise in supporting successful change.

Recovery Community: Persons having a history of alcohol and drug problems who are in or seeking recovery, including those currently in treatment; as well as family members, significant others, and other supporters and allies (SAMHSA, 2009).

Recovery Support Services (RSS): These are non-clinical services that assist individuals and families to recover from alcohol or drug problems and include social support, linkages to and coordination among service providers, and a full-range of human services that facilitate recovery and wellness contributing to an improved quality of life. These services can be flexibly staged and may be provided prior to, during, and after treatment. RSS may be provided in conjunction with treatment, or as separate and distinct services, to individuals and families who desire and need them. Professionals, faith-based and community-based groups, and other RSS providers are key components of ROSC (SAMHSA, 2009).

Resilience: An individual's ability to cope with change and adversity. Resilience develops over time and gives an individual the capacity not only to cope with life's challenges but also to be better prepared for the next stressful situation. (SAMHSA 4/4/2022)

Social Determinants of Health (SDOH): Conditions in the places where people live, learn, work, and play that affect a wide range of health and quality-of life-risks and outcomes. (CDC). Social determinants of health as the conditions in which people are born, grow, live, work and age. These circumstances are shaped by the distribution of money, power, and resources at global, national, and local levels. They state social determinants of health are mostly responsible for health inequities – the unfair and avoidable differences in health status seen within and between countries. (WHO)

Five key areas are identified in Healthy People 2030:

1. Healthcare Access and Quality: The connection between people's access to and understanding of health services and their own health. This domain includes key issues such as access to healthcare, access to primary care, health insurance coverage, and health literacy.
2. Education Access and Quality: The connection of education to health and well-being. This domain includes key issues such as graduating from high school, enrollment in higher education, educational attainment in general, language and literacy, and early childhood education and development.

3. Social and Community Context: The connection between characteristics of the contexts within which people live, learn, work, and play, and their health and wellbeing. This includes topics like cohesion within a community, civic participation, discrimination, conditions in the workplace, and incarceration.
4. Economic Stability: The connection between the financial resources people have – income, cost of living, and socioeconomic status – and their health. This area includes key issues such as poverty, employment, food security, and housing stability.
5. Neighborhood and Built Environment: The connection between where a person lives – housing, neighborhood, and environment – and their health and wellbeing. This includes topics like quality of housing, access to transportation, availability of healthy foods, air and water quality, and neighborhood crime and violence.

Whole-Person/Integrated Care: A comprehensive and coordinated person-centered system of care that allows healthcare professionals (i.e., behavioral health, primary care, and specialty providers) to simultaneously consider all of an individual's health conditions, resulting in the systematic coordination of physical and behavioral healthcare. Such integrated healthcare services that are delivered in a whole-person approach produce beneficial outcomes for people with multiple and complex healthcare conditions.

References:

A. Center for Substance Abuse Treatment. (2009). *What Are Peer Recovery Support Services?* SAMHSA. Rockville, MD. [On-line]. Available: http://store.samhsa.gov/shin/content//SMA09-4454/SMA09-4454.pdf.

B. Center for Substance Abuse Treatment. (2010). *Recovery-Oriented Systems of Care (ROSC) Resource Guide.* SAMHSA. Rockville, MD. [On-line]. Available: http://www.samhsa.gov/sites/default/files/rosc_resource_guide_book.pdf.

C. Copeland, M. (Undated). *Action Planning for Prevention and Recovery*. United States Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Mental Health Services. Rockville, Md. [On-line]. Available: http://store.samhsa.gov/shin/content//SMA-3720/SMA-3720.pdf.

D. Copeland, M. (Undated). *Recovering Your Mental Health—A Self-Help Guide.* United States Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Mental Health Services. Rockville, Md. [On-line]. Available: http://store.samhsa.gov/shin/content//SMA-3504/SMA-3504.pdf.

E. del Vecchio, Paolo. (2012). *SAMHSA's Working Definition of Recovery Updated.* United States Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Mental Health Services. [On-line]. Rockville, MD. Available: http://blog.samhsa.gov/2012/03/23/defintion-of-recovery-updated/.

F. Michigan Department of Community Health. (2005). *Transforming Mental Health Care In Michigan: A Plan For Implementing Recommendations Of The Michigan Mental Health Commission.* [On-line]. Available: http://www.michigan.gov/documents/DCH_Implementation_Plan_April_2005_122025_7.pdf.

G. Michigan DCHODCP Treatment Technical Advisory No. 07: *Peer Recovery/Recovery Support Services.* [On-line]. Available: http://www.michigan.gov/documents/mdch/TA-T-07_Peer_Recovery-Recovery_Support_230852_7.pdf.
H. Office of Disease Prevention and Health Promotion. *Healthy People 2030*: https://health.gov/healthypeople
I. SAMHSA's Recovery and Recovery Support Initiative: https://www.samhsa.gov/find-help/recovery
J. SCCMHA Policy 02.03.08 – Welcoming
K. SCCMHA Policy 02.03.09 – Evidence-Based Practices (EPBs)
L. SCCMHA Policy 02.03.09.10 – Substance Use Disorder Services
M. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports
N. SCCMHA Policy 02.03.19 – Peer Support Services
O. SCCMHA Policy 02.03.25 – Wellness
P. SCCMHA Policy 03.02.31 – Services for Members of the Armed Forces Veterans & their Families
Q. SCCMHA Policy 03.02.45 - Interdisciplinary Treatment Teams
R. SCCMHA Policy 03.02.46 – Whole-Person Care
S. United States Public Health Service Office of the Surgeon General. (1999). *Mental Health: A report of the Surgeon General.* Department of Health and Human Services, E.S. Public Health Service. Rockville, MD. [On-Line]. Available: http://www.surgeongeneral.gov/library/mentalhealth/home.html.
T. Veteran's Health Administration. (September 11, 2008, Amended November 16, 2015). *Uniform Mental Health Services in VA Medical Centers and Clinics*. [On-line]. Available: http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1762.

Exhibits:
A. SAMHSA's Four Dimensions of the Recovery Process
B. SAMHSA's 10 Guiding Principles of Recovery
C. Recovery Oriented System of Care (ROSC)

Procedure:
None

Exhibit A

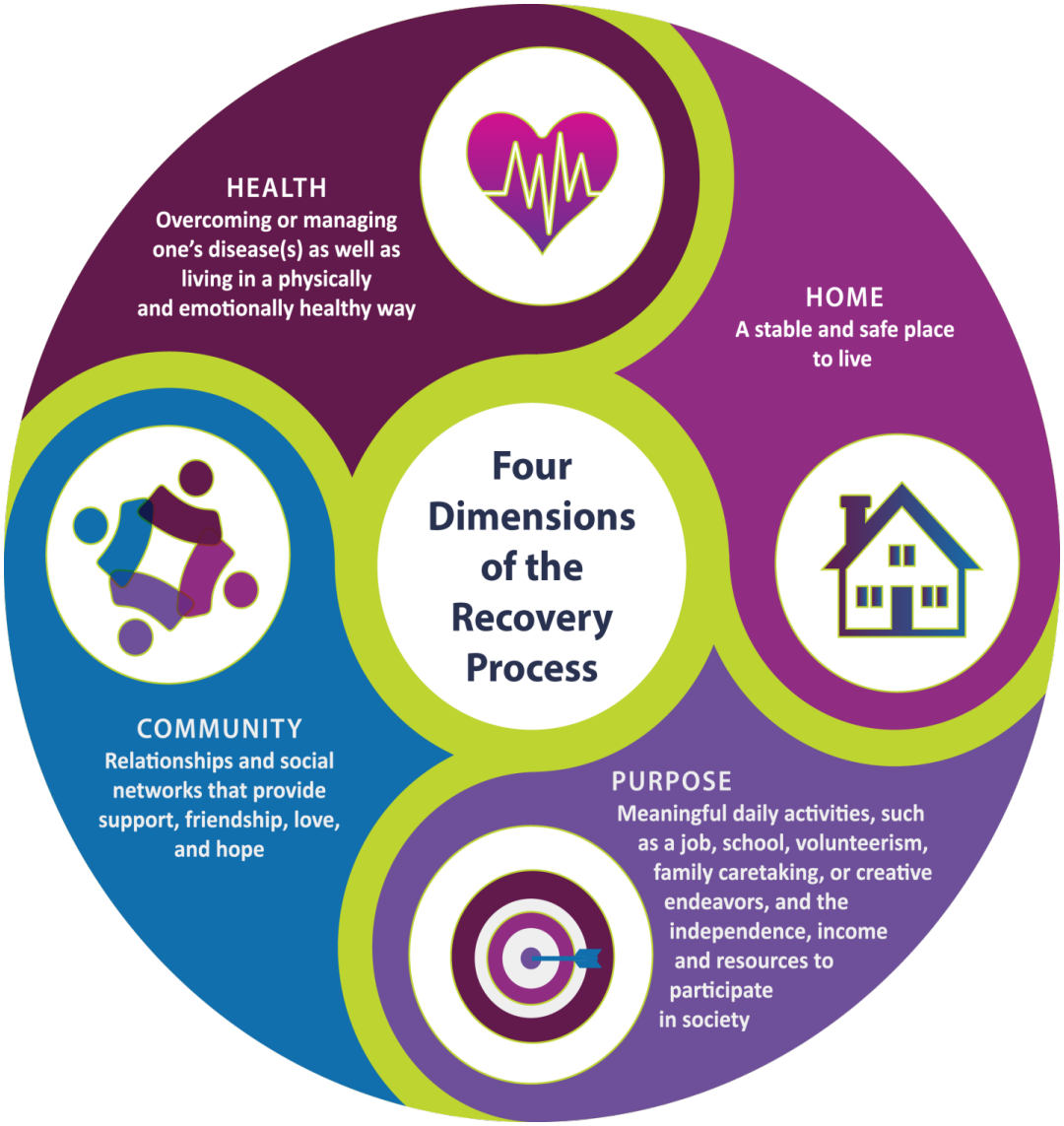

HEALTH
Overcoming or managing one's disease(s) as well as living in a physically and emotionally healthy way
HOME
A stable and safe place to live
Four Dimensions of the Recovery Process
COMMUNITY
Relationships and social networks that provide support, friendship, love, and hope
PURPOSE
Meaningful daily activities, such as a job, school, volunteerism, family caretaking, or creative endeavors, and the independence, income and resources to participate in society

Exhibit B

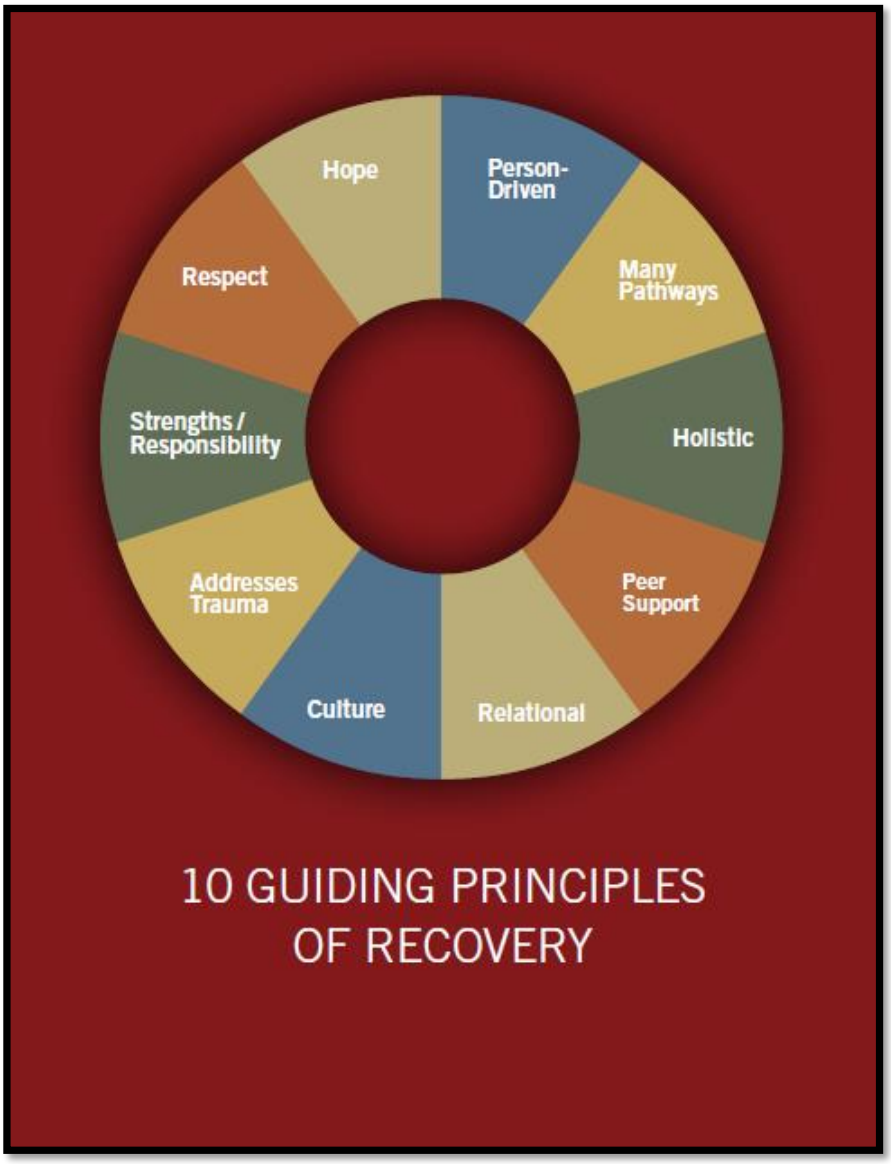
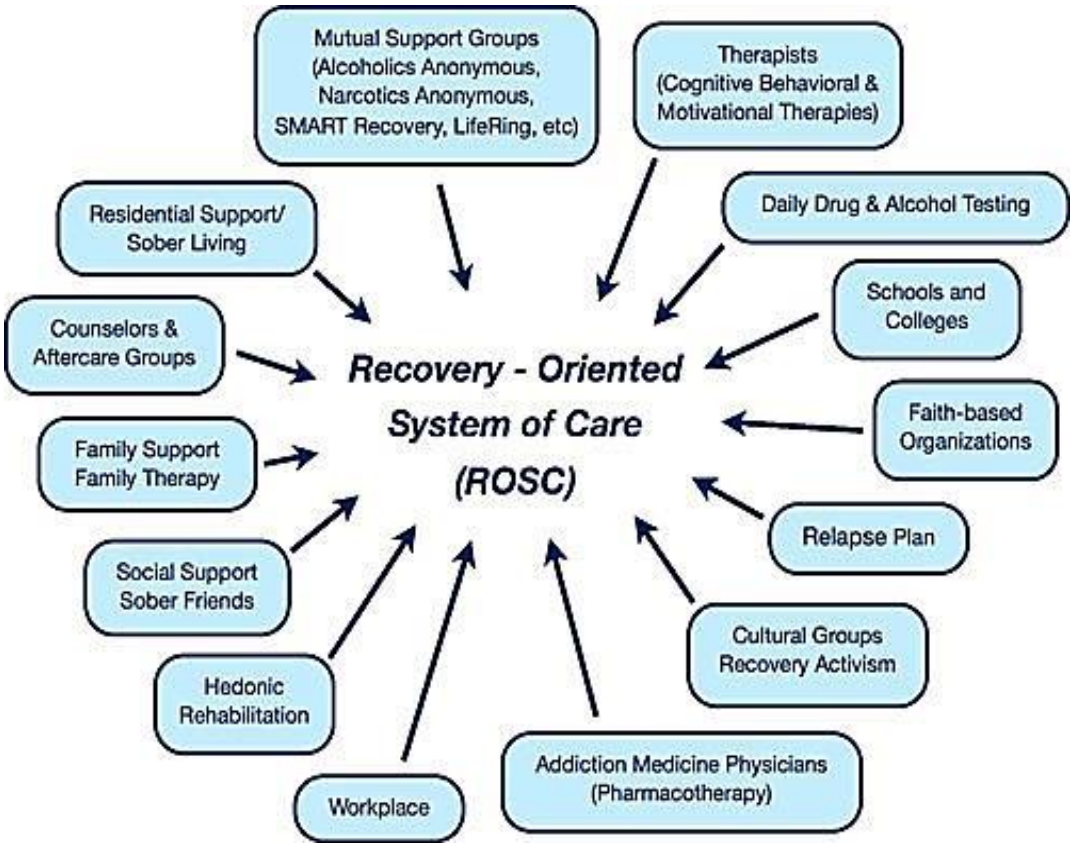

Hope
Person-Driven
Respect
Many Pathways
Strengths / Responsibility
Holistic
Addresses Trauma
Peer Support
Culture
Relational
10 GUIDING PRINCIPLES OF RECOVERY

Exhibit C


Mutual Support Groups (Alcoholics Anonymous, Narcotics Anonymous, SMART Recovery, LifeRing, etc)
Therapists (Cognitive Behavioral & Motivational Therapies)
Residential Support/ Sober Living
Daily Drug & Alcohol Testing
Schools and Colleges
Counselors & Aftercare Groups
Recovery - Oriented System of Care (ROSC)
Faith-based Organizations
Family Support Family Therapy
Relapse Plan
Social Support Sober Friends
Cultural Groups Recovery Activism
Hedonic Rehabilitation
Addiction Medicine Physicians (Pharmacotherapy)
Workplace

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Welcoming</td><td>Chapter: 02 - Customer Services and Recipient Rights</td><td>Subject No: 02.03.08</td></tr>
<tr><td rowspan="2">Effective Date:
7/1/07</td><td>Date of Review/Revision:
5/18/09, 4/2/12, 5/6/14, 4/5/16, 6/13/17, 4/10/18, 4/9/19, 7/29/20, 4/13/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to set forth expectations and standards of a welcoming philosophy wherein individuals and their family members engage in meaningful, non-judgmental interactions with staff within a person-centered, trauma-informed, recovery/resiliency building-oriented system of developmentally appropriate, culturally sensitive services and supports that promote person served/family engagement and shared decision-making.

Policy:
SCCMHA recognizes that a welcoming philosophy is based on the core belief of dignity and respect for all people. Therefore, SCCMHA and its provider network shall create empathic, inclusive and welcoming relationships within all programs and incorporate welcoming into cultural and organizational structures and practices irrespective of service eligibility.

Application:
This policy applies to the entire SCCMHA network of direct operated and contracted service providers.
Welcoming applies to all people including individuals seeking services and their families, the public (who may or may not be seeking services); other providers (including those seeking access for people they serve); agency staff; and the community.

Standards:
A. SCCMHA shall provide safe, functional, clean, and welcoming in-person and virtual environments (telehealth services) for persons served and staff that are conducive to the scope of services provided.
B. All persons seeking or currently receiving services from SCCMHA providers shall experience face-to-face, telephone, and remote (telehealth) assistance provided in a warm, welcoming manner.

C. Irrespective of an individual's presenting problem(s), SCCMHA shall:
   1. Convey the message that it is okay to ask for help.
   2. Indicate that the person has come to the right place.
   3. Let the individual know that if SCCMHA cannot help them, SCCMHA will ensure that the individual is connected to a place(s) that can be of assistance.
   4. Convey understanding of what the person seeking services is experiencing and that assistance is going to be provided.
   5. Convey positive regard and empathy for each individual and their situation.
   6. Indicate that no matter what problem(s) the person is facing, SCCMHA is going to work with the person on them.
   7. Help each individual feel that there is hope.
   8. Convey acceptance that, for individuals with complex problems, non-adherence to one or more treatment recommendations can be typical.
   9. Convey hope through empathizing with the reality of despair, encouragement for asking for help, and acknowledging small step successes.
   10. Enable timely access to treatment/intervention, services, and supports.

D. All contacts shall be welcoming, empathic, hopeful, culturally sensitive, developmentally appropriate, and person-centered in order to engage individuals who may be unwilling to accept or participate in recommended services, or who do not fit into available program models.

E. Welcoming shall be recognized and operationalized as the first step in engagement, by emphasizing welcoming attitudes and messaging during routine and emergency access points. This includes recognizing that addressing co-occurring issues or disorders concurrently results in the most successful and desirable outcomes.
   1. All SCCMHA providers shall include specific welcoming language for people as part of their admissions policies and in recognition of the need to treat co-occurring disorders simultaneously in order to optimize the potential for successful and desirable treatment outcomes.

F. Staff shall demonstrate a belief in the possibility of recovery, a willingness to start where the person served/family is at, and provide services accordingly, including harm reduction approaches.

G. Persons served shall be engaged in a culturally sensitive manner that conveys empathy and hope and that actively reaches out to the person served/family.

H. All individuals and families self-identifying as in need of services shall be welcomed; a "no wrong door" approach to all service requests shall be maintained.
   1. No individual requesting services shall be turned away based on eligibility/exclusion criteria; every door is the right door for screening and gaining access to the most appropriate services irrespective of whether that person/family will be provided with continuing services in a SCCMHA-funded setting.

I. Program materials (e.g., person served and staff orientation information, website, brochures, posters, and newsletters) shall incorporate principles of welcoming including being visibly accessible, culturally and linguistically relevant, and person-friendly.

J. An orientation to welcoming skills shall be provided to all staff.

K. All SCCMHA providers shall have a welcoming policy and procedure that includes how staff are oriented and trained in the warm, welcoming approach and how this shall be utilized for performance improvement.

L. All SCCMHA providers shall include clinician/case holder competencies as a written part of human resource policies that require welcoming attitudes, accepting values, and skills in conveying empathy and hope to persons served, and that these competencies need to be demonstrated in practice and by formal assessment.

Definitions:

Co-occurring Disorders include coexisting mental health, general health conditions, intellectual/developmental disabilities, and substance use disorders in any combination.

Welcoming is an accepting attitude and understanding of how people present for treatment that also reflects a capacity on the part of the provider to address the person's needs in a manner that accepts and fosters a service and treatment relationship. Welcoming is considered a best practice for programs, particularly those that serve persons with co-occurring mental health, general health, and substance use disorders. Welcoming consists of the following:

Reception areas:

- Places of welcome that give newcomers first impressions of the whole organization
- Greeting in a manner that conveys the person matters to the people who are in charge of the facility/program
- Communicating that people are properly cared about and confidentiality is respected
- A culturally competent invitation to receive services, including assistance for individuals whose first language is not English.
- A clean and cared for environment
- Up-to-date and commonly read materials (e.g., magazines and newspapers) in waiting areas, as well as information on various mental health disorders and recovery-oriented treatments
- Group meetings clearly posted
- Tasteful décor
- Posters and artwork promote hope and recovery
- Receptionists greet all with warmth, respect, and dignity
- A welcome sign
- Waiting areas include consideration for family members or others accompanying the individual seeking services

Facilities:

- Clean and cared for
- Furniture that is clean, of good quality, comfortable, and ergonomically correct
- Treatment areas that afford privacy and confidentiality
- Barrier-free accommodations
- Smoking areas designated away from the entrance

Staff members:

- Listen to persons served

- Offer persons served helpful suggestions
- Help persons served with decision-making in an empowering manner
- Offer explanations
- Provide assistance
- Function as advocates for persons served regardless of whether they are in agreement with the perspectives of the person served
- Support hope and belief in the unlimited potential of persons served
- Provide prompt and on-time services
- Offer choices to persons served

Programs/Agencies:

- Hours of operation meet the needs of the population(s) being served
- The service location is considered with regard to public transportation and accessibility, including access to telehealth

References:

A. Michigan Department of Community Health, Office of Drug Control Policy Treatment Technical Advisory # 05 (October 1, 2016) – Welcoming: https://www.michigan.gov/documents/mdch/TA_Treatment_05_Welcoming_175207_7.pdf
B. SCCMHA Policy 02.03.03 – Person-Centered Planning
C. SCCMHA Policy 02.03.09 – Evidence-Based Practices (EPBs)
D. SCCMHA Policy 02.03.09.01 – Dual Diagnosis Treatment Capacity
E. SCCMHA Policy 02.03.05 – Recovery
F. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports
G. SCCMHA Policy 02.01.10 – Therapeutic Environment
H. SCCMHA Policy 02.01.01.02 – Cultural Competence
I. SCCMHA Policy 02.01.05 – Consumer Orientation
J. SCCMHA Policy 02.01.02 – Customer Service
K. SCCMHA Policy 03.02.31 – Services for Members of the Armed Forces, Veterans & their Families
L. SCCMHA Policy 03.02.34 – Services for American Indians
M. SCCMHA Policy 03.02.35 – Serving LGBTQIA+ Persons
N. SCCMHA Policy 03.02.46 – Whole Person Care

Exhibits:

A. Person-Centered, Trauma-Informed, Welcoming Tips and Reminders (Dawn Heje, 9.29.16)

Exhibit A

Person-Centered, Trauma-Informed, Welcoming Tips and Reminders

It is the policy and the expectation that anyone seeking or receiving services from SCCMHA or its network will experience face-to-face, telephone, video (telehealth) assistance that is provided in a warm, welcoming, non-judgmental, person-centered, trauma-informed, recovery/resiliency building manner. We will always keep in mind that the person we are talking to is someone's cherished husband or wife, brother or sister, mother or father, child or best friend. It is our job to give the person and their loved ones hope for recovery.

Do	Don't
• During face-to-face contacts sit beside or at a right angle to the person whenever possible.	• Sit across from the person with a desk or table between you.
• Ask the person if it would be okay to take notes while you talk. Take notes in a way that the person can see what you are writing. Transfer the notes into the EMR after the face-to-face contact. • If you must enter directly into the EHR when you are with the person, acknowledge the limited eye contact and let them know what you typing as you type.	• Type into a computer as you talk with the person. If you are entering information into the EMR you are not fully engaged with the person. • Sit or stand with your back to the person at any time.
• Use non-verbal and para-verbal communication to let the person know you are listening and that you care. The way you listen, look, move and react is going to tell the person how well you are listening. Examples include eye contact as appropriate for the person's culture; nodding; "um-hmm", leaning in toward the person, facial expression.	• Look at your watch or phone, enter information into the EMR while the person is talking, fidget, stare out the window, doodle or use facial expressions that convey anything but care, concern or respect. • Use sarcasm or an angry tone of voice.
• Truly listen. If you are planning what you're going to say next, daydreaming, or thinking about something else, you are probably going to miss nonverbal cues and other subtleties in the conversation. Stay focused on the person and the conversation in order to fully understand what's going on.	• Interrupt, daydream, plan your response, focus on your notes, check your phone, or show signs of impatience or disinterest. • Finish the person's sentence.
• Convey verbally and non-verbally that no matter what the person is facing, there is hope and acknowledge the big step the person took by asking for help. • Each contact should offer explanations and clarifications, and resources and support, especially if the outcome is not quite what was requested.	• Turn away a person based on eligibility or exclusion criteria. Remember that every door is the right door for screening and gaining access to the most appropriate services.

• Make the person the most important part of the interview. Gathering information is more than getting answers to all of the questions on the intake screen.	• Make the questionnaire or medical record the focus of the interview.
• Make the person feel safe and in control by offering the choice of where they would like to sit, offer water, having a box of tissues close by, showing where restrooms are in a gender-neutral way, letting the person know they can take a break at any time, and letting the person know they have the right to not respond to any question.	• Ignore the person's basic needs. • Force them to ask where restrooms are located. • Insist the person answer questions.
• Listen without judgement, artfully ask questions for clarification, provide accurate information, offer assistance, and support the person in their recovery journey by starting in the place they are at to ensure that the person will come back for services.	• Offer advice, assume you know what is best for the person, or judge the person's decisions or situation.
• Remember that asking people to reveal personal information can be re-traumatizing, embarrassing, or frightening. Fully explain about confidentiality before starting every contact. • Acknowledge that some questions can be difficult to answer and that the person is doing a great job with a difficult task.	• Hand the person confidentiality material to read and expect them to fully understand the concept of confidentiality. • Neglect the person's signs of discomfort or embarrassment.
• Keep in mind that if a person becomes upset during the interview, it is not recommended to probe for more information. The clinician should stop, take care of the person's needs and help the person regain a sense of safety.	• Ignore signs of distress. • Continue with the interview while the person is crying or showing other signs of emotional distress. • Neglect to offer follow-up services before the person leaves.
• Be extra sensitive to questions about gender identity, sexual orientation, sexual activity, military experience, homelessness or near homelessness, family situation, abuse and trauma, and suicidality.	• While any question could trigger re-traumatization, don't forget that some questions are more likely to bring to mind painful memories, shame or guilt.
• Look for signs of distress or agitation at the end of the session and help the person regain control over their feelings. Once the clinician is sure the person is okay, end with a warm sendoff or warm handoff. • Each contact should summarize key information and confirm next steps or follow up plans if applicable.	• End the interview or session with the person distressed or disassociated. • Neglect to spend a few minutes engaging with the person before gently handing them off to another person or walking them to the front door.

	• Neglect to let the person know what a genuine pleasure it was to meet with them.

For more information:
SAMHSA LGBT Training Curricula for Behavioral Health and Primary Care Practitioners: http://www.samhsa.gov/behavioral-health-equity/lgbt/curricula
National Sexual Violence Resource Center: http://www.nsvrc.org
VA Mental Health: https://www.mentalhealth.va.gov/msthome/index.asp
Zero Suicide: http://zerosuicide.sprc.org/

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: System of Care (SOC)</td><td>Chapter: 02 - Customer Services and Recipient Rights</td><td>Subject No: 02.03.09.09</td></tr>
<tr><td rowspan="2">Effective Date:
5/1/08</td><td>Date of Review/Revision:
6/10/09, 6/10/10, 4/4/12, 5/6/14, 4/19/16, 6/13/17, 4/10/18, 4/9/19, 7/29/20, 4/13/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:
None</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

A. The purpose of this policy is to delineate a framework for fostering the development and maintenance of a System of Care (SOC) for children and families with serious emotional/behavioral disturbances who require services and supports from multiple child-serving organizations and public sector service delivery systems, and that enables children to be cared for in their homes, schools, and communities. SOC goals include:

1. Helping children and families develop the skills needed to manage their lives in their homes and communities.
2. Promoting parent–professional–community partnerships in the design, implementation and evaluation of the system of care.
3. Ensuring cultural competence in the delivery of services.
4. Expanding the amount and quality of services and supports available from all child-serving agencies and matching them to each individual child.
5. Providing ongoing training/education for families, advocates, and professionals.
6. Using quality improvement activities to help make decisions.
7. Expanding community-based systems of services and supports.
8. Providing state-of-the-art, effective clinical services and supports.

Policy:

Children with serious emotional disturbances and their families often need a range of comprehensive, individualized, coordinated services and supports. All key partners must come together to plan for and deliver these services, with families as full partners in the process. To this end, SCCMHA shall promote and help maintain a child-focused and family-

centered system of community-based, trauma-informed, resiliency-focused, developmentally appropriate care for children with serious emotional disturbances and their families.

Application:
This policy applies to all providers of mental health treatment and related supports to children, adolescents, and families operating under the auspices of the Saginaw County Community Mental Health Authority.

Standards:

A. Children with serious emotional disturbances often experience a variety of problems that require solutions from an array of professionals and services.

B. Serving children who have serious emotional disturbances and multiple service system needs requires substantial assistance from the community.

C. The following core values of a system of care shall be adhered to:
   1. Child and family-centered. The needs of the child and family shall dictate the types and mix of services and supports provided; services are adapted to the child and family rather than expecting the child and family to conform to preexisting service and support configurations.
   2. Individualized. A unique service plan shall be developed for each child and family which assesses their strengths and needs, prioritizes their needs in each life domain, and is responsive to the family's cultural, racial, and ethnic identity.
   3. Community-based. Services shall be provided within or close to the child's home community in the least restrictive setting feasible and coordinated and delivered via connections between providers.
   4. Oversight by a multi-agency advisory team. A multi-agency advisory team shall provide oversight for a system of care. The team shall be comprised of representatives from families and partner agencies who engage in planning and decision-making. The team will monitor the development and maintenance of interagency collaborations, seek to improve the overall effectiveness of the partnerships and help to maintain open communication and decision-making across all stakeholders.

D. The following guiding principles of a system of care shall be adhered to:
   1. Service coordination or case management
      a. Coordination between primary health care and specialty mental health services.
   2. Prevention, early identification and intervention
      a. Incorporating mental health promotion, prevention, screening, early identification, and early intervention services.
   3. Smooth transitions among agencies, providers, and to the adult service system (where indicated)
   4. Human rights protection and advocacy
   5. Nondiscrimination in access to services
   6. A comprehensive array of services
   7. Individualized service planning
   8. Services in the least restrictive environment
   9. Family participation in all aspects of planning, service delivery, and evaluation

10. Integrated services with coordinated planning across child-serving systems
11. Promotion of the use of best practices across all systems; evidence-based clinical interventions are integral to an effective system of care.
12. An explicit focus on achieving equity in mental health care for young people and their families in an effort to mitigate structural and systemic racism, implicit bias, and historical trauma that impact the social determinants of health, such as economic stability, education, housing, health care, nutrition, and safety.

E. The following core services of a system of care shall be made available to eligible children, youth and families as needed and resources permit:

1. Mobile Crisis Response and Stabilization Services (MRSS) shall be provided to children and youth who are experiencing mental health emergencies and their families in order to defuse and stabilize crises, maintain children and youth in their current living arrangements, prevent hospitalization, prevent disruption of child welfare placements, and improve functioning.
2. Intensive care coordination using Wraparound as an approach to providing individualized care for children, youth, and young adults with complex mental health needs and their families.
3. Intensive in-home mental health treatment services provided to improve child, youth, and family functioning and to prevent the need for out-of-home placement, inpatient hospitalization, or residential treatment that includes individual and family therapy, skills training, behavioral interventions, crisis response, and care coordination.
4. Parent and youth peer support provided by individuals who have personal "lived" experience with mental health conditions (including substance use issues and disorders) and navigating service systems, either as a person served or as a family member or caregiver.
5. Respite care to provide parents and other primary caregivers with planned or emergency short-term care for their child, enabling children and youth with mental health needs to remain in a safe and supportive environment, usually in their own homes.
6. Flex funds using financing mechanisms covered by Medicaid and other sources.
7. Trauma-specific treatments and trauma-informed systems to address traumatic experiences with particular attention to the impact of adverse childhood experiences on later mental health needs.
8. The provision of evidence-based practices, services and treatment as well as specific evidence-informed and promising practices to ensure treatment effectiveness.
9. Telehealth services including videoconferencing, internet access, store-and-forward imaging, streaming media, and terrestrial and wireless communication, as resources permit, particularly to provide care to underserved populations and thus increase access to behavioral health care services.

Definitions:

Blended Funds: Funds that come from various sources that are merged and used interchangeably.

Braided Funding: Funding that uses monies from different sources but accounts for the different sources separately.

Cultural Competence: Help that is sensitive and responsive to cultural differences. Caregivers are aware of the impact of culture and possess skills to help provide services that respond appropriately to a person's unique cultural differences, including race and ethnicity, national origin, religion, age, gender, sexual orientation, or physical disability. They also adapt their skills to fit a family's values and customs.

Flexible Funds (Flex Funds): Funds for services and/or supports families are unable to afford and for which there is no other method of payment. Flex funds can fill gaps in the system of care by facilitating the purchase of goods or services that would otherwise not be available to a family. Typically, funds are not used for ongoing expenses but are more often one-time or occasional costs that connect to the needs identified by the youth with input from the team and family. Flex funds are often used as a last resort when other sources cannot meet the identified need. Within a Wraparound team approach, flex funds are used strategically to put services and supports into place while the team continues to work on the plan to sustain the service/support beyond the availability of flex funds.

System of Care (SOC): A comprehensive spectrum of effective services and supports for children, youth, and young adults with or at risk for mental health or other challenges and their families that is organized into a coordinated network of care, builds meaningful partnerships with families and youth, and is culturally and linguistically responsive in order to help them to thrive at home, in school, in the community, and throughout life. A system of care incorporates mental health promotion, prevention, early identification, and early intervention in addition to treatment to address the needs of all children, youth, and young adults. (Stroul, Blau, Larson 2021) [MDHHS]

References:

A. Glassheim, B. (2006). *A Guide to Evidence-Based Practices for Children, Adolescents and their Families*. SCCMHA: https://www.sccmha.org/userfiles/filemanager/287/

B. Hernandez, M., Worthington, J., Davis, C.S. (2005). *Measuring the Fidelity of Service Planning and Delivery to System of Care Principles: The System of Care Practice Review (SOCPR).* (Making children's mental health services successful series, 223-1). University of South Florida, The Louis de la Parte Florida Mental Health Institute. Tampa FL. http://cfs.fmhi.usf.edu/tread/PDFs/SOCPR_Monograph%20FINAL-3-5-05.pdf.

C. MDHHS – Mental Health Partnerships (SOC): https://www.michigan.gov/mdhhs/keep-mi-healthy/mentalhealth/mentalhealth/childrenandfamilies/mh-partnerships

D. SCCMHA Policy 02.03.09 – Evidence-Based Practices (EPBs)

E. SCCMHA Policy 02.03.09.09 – Wraparound

F. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports

G. SCCMHA Policy 03.02.46 – Whole Person Care
H. Stroul, B. (2002). A Framework For System Reform In Children's Mental Health. *Issue Brief*. National Technical Assistance Center For Children's Mental Health, Georgetown University, Child Development Center. Washington, DC. http://guc-chd.georgetown.edu/files/products_publications/SOCbrief.pdf
I. Stroul, B., Blau, G., Friedman, R. (2010). Updating the system of care concept and philosophy. Georgetown University Center for Child and Human Development, National Technical Assistance Center for Children's Mental Health. Washington, DC. https://www.isbe.net/Documents/soc-brief-2010.pdf
J. Stroul, B., Blau, G., Larson, J. (2021). The Evolution of the System of Care Approach. Baltimore: The Institute for Innovation and Implementation, School of Social Work, University of Maryland. https://www.cmhnetwork.org/wp-content/uploads/2021/05/The-Evolution-of-the-SOC-Approach-FINAL-5-27-20211.pdf
K. Stroul, B., Friedman, R. (1986). *A System of Care for Children and Youth with Severe Emotional Disturbances*. Georgetown University Child Development Center, National Technical Assistance Center for Children's Mental Health. Washington, DC.
L. Worthington, J., Davis, C., Hernandez, M., Pinto, A., Vergon, K. (2005). *System of Care Practice Review: Review Team Member Training Manual* (rev. ed.) University of South Florida, The Louis de la Parte Florida Mental Health Institute. Tampa, FL.
http://cfs.fmhi.usf.edu/tread/PDFs/SOCPR%20Training%20Manual.pdf.

Exhibits:
A. System of Care Framework
B. System of Care Practice Review (SOCPR) domains and subdomains

Procedure:
None

Exhibit A

System of Care Framework

The range of services that may be included in a system of care:

- Case management (service coordination)
- Community-based in-patient psychiatric care
- Counseling (individual, group, and youth)
- Crisis residential care
- Crisis outreach teams
- Day treatment
- Education/special education services
- Family support
- Health services
- Independent living supports
- Intensive family-based counseling (in the home)
- Legal services
- Protection and advocacy
- Psychiatric consultation
- Recreation therapy
- Residential treatment
- Respite care
- Self-help or support groups
- Small therapeutic group care
- Therapeutic foster care
- Transportation
- Tutoring
- Vocational counseling

Exhibit B

SYSTEM OF CARE PRACTICE REVIEW (SOCPR)

DOMAIN 1	Child-Centered and Family-Focused: The needs of the child and family dictate the types and mix of services provided.

SUBDOMAINS

INDIVIDUALIZATION	Individualization refers to the development of a unique service plan for each child and family in which their needs are assessed and prioritized in each life domain. Strengths are also identified and included as part of the plan.
FULL PARTICIPATION	Developing an individualized service plan is possible with full participation of the child, family, providers, and significant others. Additionally, the child and family participate in setting their own treatment goals, and plan for the evaluation of interventions to reach those goals.
CASE MANAGEMENT	Case management is intended to ensure the child and family receive the services they need in a coordinated manner, that the type and intensity of services are appropriate, and that services are driven by the family's changing needs over time.

DOMAIN 2	Community-Based: Services are provided within or close to the child's home community, in the least restrictive setting possible, and are coordinated and delivered through linkages between public and private providers.

SUBDOMAINS

EARLY INTERVENTION	Early identification and intervention for the child with emotional disturbances enhance the likelihood of positive outcomes by reversing maladaptive behaviors and preventing problems from reaching serious proportions. This refers to both providing services before problems escalate, in the case of the older child, and designing services for the younger child.
ACCESS TO SERVICES	Each child and family has access to comprehensive services across physical, emotional, social, and educational domains. These services are flexible enough to allow the child and family to integrate them into their daily routines.
MINIMAL RESTRICTIVENESS	Systems serve the child in as normal an environment as possible. Interventions provide the needed services in the least intrusive manner to allow the family to continue day-to-day routines as much as possible.
INTEGRATION AND COORDINATION	Coordination among providers, continuity of services, and movement within the components of the system are of central importance for each child and family with multiple needs.

DOMAIN 3	Culturally Competent: Services are attuned to the cultural, racial, and ethnic background and identity of the child and family.

SUBDOMAINS

AWARENESS	Culturally competent service systems and providers are aware of the impact of their own culture and the culture of each family being served. They accept cultural differences and understand

	the dynamics at play when persons from different cultural backgrounds come into contact with each other. They recognize how cultural context uniquely relates to service delivery for each child and family.
AGENCY CULTURE	The child and family are assisted in understanding the agency's culture, in terms of how the system operates, its rules and regulations, and what is expected of them.
SENSITIVITY AND RESPONSIVENESS	Cultural Competence includes the ability to adapt services to the cultural context of each child and family.
INFORMAL SUPPORTS	Cultural Competence is reflected in the inclusion of the family's informal or natural sources of support in formal service planning and delivery. Each service provider becomes knowledgeable about the natural resources that may be used on behalf of the child and family and are able to access them.

DOMAIN 4 — Impact: The SOC philosophy implies that the implementation of SOC principles at the practice level produce positive outcomes for child and family receiving services.

SUBDOMAINS

IMPROVEMENT	Services that have had a positive impact on the child and family have enabled the child and family to improve their situation.
APPROPRIATENESS OF SERVICES	Services that have had a positive impact on the child and family have provided appropriate services that have met the needs of the child and family.

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Art Therapy</td><td>Chapter: 02 – Customer Services & Recipient Rights</td><td>Subject No: 02.03.09.44</td></tr>
<tr><td rowspan="2">Effective Date:
10/01/2025</td><td>Date of Review/Revision:</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Director of Network Services, Public Policy, Continuing Education, OBRA/PASARR and Enhanced Health Services

Authored By:
Mary Baukus

Additional Reviewers:
Joey Bourdow, EBP Leadership Team</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to delineate a framework for the provision of Art Therapy as an evidence-based practice.

Policy:

A. Art Therapy shall be provided by a licensed and qualified master's- level or higher mental health professionals credentialed in Art Therapy.
B. Art Therapy shall be delivered in accordance with trauma-informed care principles.
C. Art Therapy promotes healing and emotional well-being for individuals of all ages, including children who are experiencing behavioral challenges or those with autism spectrum disorder.
D. Art therapy can be a treatment for people and caregivers in health crises; victims of violence or other trauma; older adults with dementia; and any person served who needs help coping with life's challenges.
E. SCCMHA-funded practitioners of Art Therapy shall adhere to the tenets of Art Therapy when providing this therapeutic intervention.
F. Art Therapy can be delivered face-to-face, in-person, or via telehealth technology.
G. SCCMHA shall, resources permitting, offer Art Therapy as an intervention choice for outpatient psychotherapy.

Application:
This policy applies to all mental health professionals involved in the delivery, supervision, and support of Art Therapy services within the SCCMHA-funded provider network.

Standards:

A. Art Therapists must hold appropriate credentials (at least ATR-Provisional from the Art Therapy Credentials Board, Inc.) and licensure for their specific profession (LMSW, LLMSW, LMFT, LLC, LPC, etc.).
    1. Sessions must be documented in accordance with agency standards.
    2. All artwork created by persons served during Art Therapy sessions shall be treated as part of the medical record and stored securely in accordance with agency policies on confidentiality and protected health information. The disposition of artwork (e.g., return to person served, destruction, or retention) shall be discussed with the person served as part of the therapeutic process, and documented in record. Any removal or disposal of artwork must comply with applicable legal, ethical, and agency guidelines regarding client property and privacy.
    3. Supervision must be provided regularly to ensure fidelity to the model and adherence to trauma-informed principles. Supervision shall be conducted by a board-certified art therapist (ATR-BC) or a licensed mental health professional with experience in art therapy and trauma-informed care.
    4. All staff must complete required training and credentialing prior to delivering Art Therapy services.

B. Training Guidelines:
    1. All staff implementing Art Therapy must complete the minimum education and training requirements of the Art Therapy Credentials Board.
    2. Training must include modules on recognizing trauma responses, creating safe environments, and ethical considerations.
    3. Six hours of specific or related continuing education must be completed annually to maintain SCCMHA privileging.
    4. Any external training records must be shared with the continuing education department.

C. SCCMHA's quality improvement activities shall include fidelity monitoring to ensure adherence to the evidence-based practice model using the GOI (Global Organization Index) as a guide.
    a. The Evidence-Based Practice and Trauma-Informed Care Coordinator and/or the Director of Network Services, Public Policy, & Continuing Education will facilitate quarterly meetings for Supervisors of EBP Teams, including Art Therapy when appropriate, to discuss fidelity monitoring.
    b. When Art Therapy is actively being offered, the Adult Strengths and Needs Assessment (ANSA) will be used as a tool to examine outcomes with reports reviewed at least annually (or as is appropriate for how frequently Art Therapy is occurring) for Art Therapy participants.

Definitions:
Art Therapy: Art therapy is a therapeutic practice that enriches the lives of individuals, families, and communities through active artmaking, creative process, applied psychological theory, and human experience within a psychotherapeutic relationship.

Trauma-Informed Care: An approach that recognizes the impact of trauma and prioritizes safety, trustworthiness, and empowerment.

References:
A. American Art Therapy Association (AATA) Home - New - American Art Therapy Association
B. Art Therapy Credentials Board, Inc. (ATCB) Art Therapy Credentials Board, Inc. | Credential Conversations
C. Art Therapy Resources Art Therapy Resources
D. National Child Traumatic Stress Network (NCTSN)
E. SCCMHA Policy 02.03.09 – Evidence-Based Practices (EPBs)
F. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports
G. SCCMHA Procedure 08.04.01 – Person served Records
H. Substance Abuse and Mental Health Services Administration (SAMHSA)

Exhibits:
A. Sample Art Therapy Session Plan
B. Becoming an Art Therapist graphic

Procedure:

ACTION	RESPONSIBILITY
Conduct initial assessment and determine appropriateness for Art Therapy	Registered Art Therapist
Develop individualized Art Therapy treatment plan goals	Registered Art Therapist
Deliver Art Therapy sessions with fidelity	Registered Art Therapist
Document session outcomes and progress of the person served	Registered Art Therapist
Provide supervision and review documentation	Clinical Supervisor
Ensure staff training compliance and maintain records	Responsible Director, Continuing Education Department, Evidence Based Practice and Trauma Informed Care Coordinator

Exhibit A

Sample Art Therapy Session Plan

1. Client Update / Initial History / Biopsychosocial Assessment
   Gather current concerns, background information, or updates on client status.

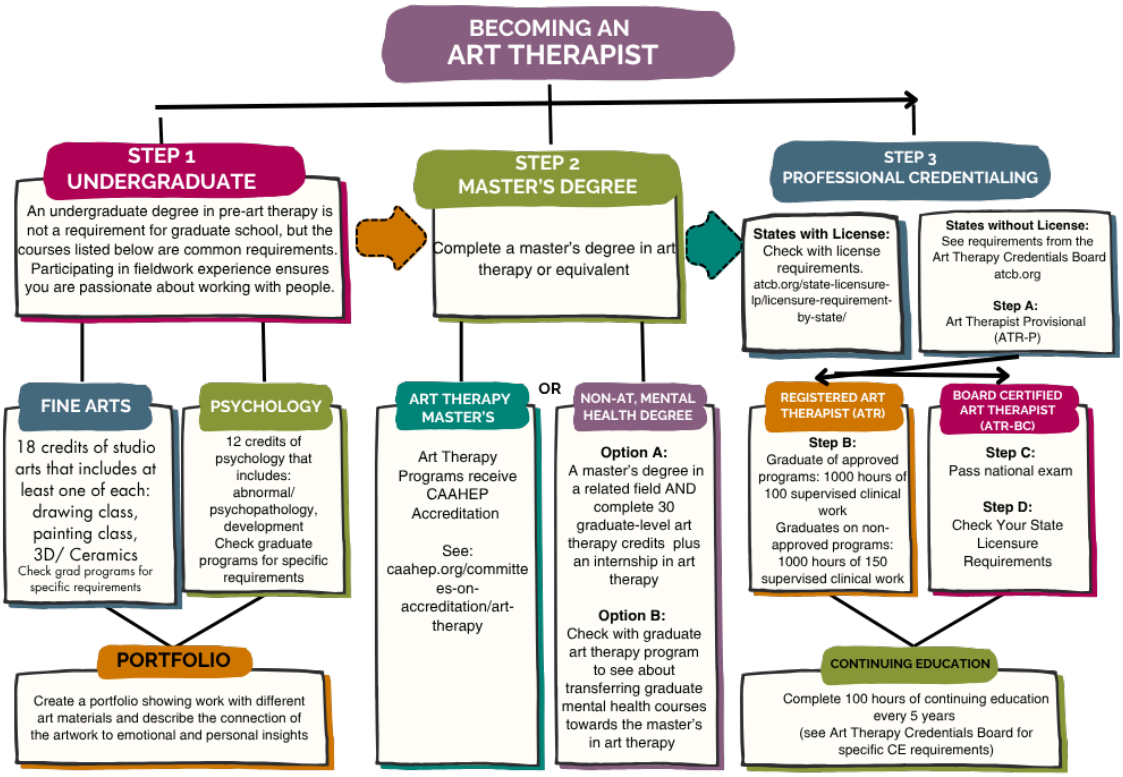
2. Art Therapy Assessment (if applicable)
   Use structured or observational tools to assess emotional, cognitive, or behavioral patterns through art.

3. Art Directive
   Provide a specific prompt or activity tailored to therapeutic goals.

4. Artmaking and Processing
   Engage in art creation followed by discussion to explore themes, insights, and emotional content.

5. Next Steps / Homework
   Identify goals, coping strategies, or art-based activities to continue outside of session.

Exhibit B



Created by Meera Rastogi, PhD, ATR-BC, LPAT, Reviewed by AATA Undergraduate Education Committee

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Alternatives to Guardianship</td><td>Chapter: 02 - Customer Services & Recipient Rights</td><td>Subject No: 02.03.12</td></tr>
<tr><td rowspan="2">Effective Date:
5/1/08</td><td>Date of Review/Revision:
6/10/09, 6/10/10, 4/4/12, 5/8/14, 8/6/14, 10/29/14, 5/4/15, 6/13/17, 4/10/18, 12/11/18, 4/9/19, 8/14/20, 4/13/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

This document sets forth SCCMHA's policy regarding alternative methods to handle decision-making that assist adults with a serious mental illness, substance use disorder, intellectual/developmental disability, and their advocates. It is designed to provide guidance, encourage best practice, and promote the rights of persons served by SCCMHA as well as ensure that individuals have access to alternatives to guardianship including, but not limited to those delineated below in Standard F.

Policy:

Independence, respect, and equality are values important to all people and, as such, help define the concepts of autonomy (i.e., independence and freedom) and self-determination (i.e., a person's right to make decisions for him or herself).

SCCMHA believes that adults should be empowered to make their own decisions but recognizes that persons served may require support that can include restrictions on autonomous decision-making in instances of clearly demonstrable risks to health and safety. SCCMHA shall always seek to balance the preservation of safety with the dignity of risk approval.

The least restrictive alternative should always be considered before taking away a person's civil and legal rights to make decisions for him or herself. The least restrictive alternative is an option that allows a person to maintain as much autonomy and self-determination as possible while providing only the level of protection and supervision necessary.

Persons served for whom decision-making autonomy has been restricted shall be provided with opportunities to acquire the skills and abilities needed for autonomous decision-making as well as those deemed essential to maintaining health and safety.

Application:

This policy applies to all SCCMHA-funded providers of services and supports to adults with mental illness, substance use disorder, co-occurring condition(s), and/or an intellectual/developmental disability.

Standards:

A. All SCCMHA-funded providers shall endeavor to preserve the basic human, civil rights and freedom of all persons served.

B. Alternatives to guardianship shall always be pursued prior to considering guardianship for persons served.
   1. These options shall be reviewed with persons served and their supporters.

C. The alternative to guardianship identified for each individual shall be deemed as the most effective relative to the person's situation in terms of empowerment and legal enforceability.
   1. Alternatives to full guardianship that offer the greatest autonomy and are the least intrusive/restrictive shall be given priority consideration.
   2. Any restrictions placed upon the right of the person served to autonomous decision-making shall be as narrow as feasible and shall be based on demonstrable health and safety issues.
      a). Said restrictions shall be reviewed on a regular basis to ensure that they continue to be necessary and are effective.
         1). Reviews and continued justification of any restrictions placed upon the autonomy of the person served shall be documented in their PCP (person-centered plan).
      b). A person served whose decision-making autonomy has been reduced or eliminated shall be offered interventions that are designed to help them gain the necessary skills and abilities to eliminate or decrease the restrictions placed upon them for their health and safety.

D. Guardianship issues and alternatives to guardianship shall, as indicated and warranted, be incorporated into the person-centered planning process and documented in the person-centered plan of service of the person served and shall include:
   1. The identification of a specific and individualized assessed need.
   2. Documentation of positive interventions and supports used prior to any revisions to the person-centered service plan that will result in a curtailment of the decision-making autonomy of the person served.
   3. Documentation of less intrusive methods of addressing the identified need that have been tried but found to be ineffective.
   4. A clear description of the condition that is directly proportionate to the specific assessed need.
   5. Systematic collection and review of data on an ongoing basis to measure the effectiveness of the modification.
   6. Established time limits for periodic reviews to determine if the modification is still necessary or can be terminated.
   7. The informed consent of the individual.
   8. An assurance that interventions and supports will not cause harm to the person served.

E. The clinical record of the person served shall clearly indicate any surrogate decision-maker and the extent of that surrogate's authority.
   1. This will be recorded in the applicable Demographic section of the electronic record (Sentri).
   2. A legible and legal document providing proof, such as the court guardianship papers, power of attorney, etc. must be scanned into the electronic record (Sentri).

F. SCCMHA providers need to be familiar with alternatives to guardianship and actively advocate for alternatives including the following options:
   1. A natural support system consisting of a network of committed family members, friends, and circles of support that are fully aware of a person's strengths, wishes, and character traits can assure that decisions are not made in a void or by paid service providers. In addition, a support system can distribute tasks and supports in a shared fashion so that no single person bears full responsibility. Consideration should be given for a release of information to allow family and other supporters access to medical records and receive routine invitations to participate in person-centered planning meetings.
   2. The provision of community assistance for support and observation including, but not limited to:
      a. Postal service checks for piled up mail
      b. Unpaid utility bills and meter reader observation
      c. Telephone reassurance programs
      d. Home visitors and pets on wheels
      e. Meals on wheels
      f. Food and prescription medication delivery
      g. Home sharing/roommate
      h. Personal assistance/home health care
      i. Service animals
   3. The provision of assistance with finances for people who have difficulty managing their funds. Including the following options:
      a. A representative payee designated by the Social Security Administration, the Veteran's Administration, and other government agencies to receive monthly benefit checks on behalf of a beneficiary when the beneficiary is determined incapable of managing the funds themselves.
      b. A bill payer who assists an individual in organizing monthly income and expenditures, writes checks for the person's signature, and assists the client with paperwork related to bill paying. **Bill** payer programs serve individuals with limited incomes who are still in charge of their own financial affairs but need some help organizing their bills and checkbook.
      c. Banking arrangements and dual signature accounts can be used as alternatives to conservatorships. A person can often retain control of their own affairs with the help of automatic deposits and withdrawals for bills or banking by mail or phone. Another method often used

is the establishment of a joint bank account in which a trusted friend or family member's name is added to an account. Caution is recommended because both persons on the account have ownership of the account. A limited bank account that requires a co-signor to access funds, write checks, or transact business is another banking option.

d. A joint property arrangement in which two or more people share ownership of real estate or bank accounts is a common form of property management. Joint property arrangements, particularly joint bank accounts, generally are easy and inexpensive to establish and no court supervision is necessary. On the other hand, joint property arrangements are inherently risky because of the control they allow the co-owner over money or property and these arrangements may be less flexible once control over the property is given to the co-owner.

4. Families can set up Special Needs Trusts (SNTs) that adhere to Social Security, SSI (Supplemental Security Income), and Medicaid rules to ensure their family member with a disability has available resources after parents or other caretakers are no longer available. Funds in Special Needs Trusts are not counted as part of an individual's income (unlike funds in traditional savings accounts) and thus provide a safeguard for benefits such as Medicaid and Social Security. People with disabilities can also set up trusts on their own behalf.

   a. An OBRA 93 trust is used to shelter the assets of a person with a mental illness or intellectual/developmental disability while protecting their eligibility for Medicaid. Such assets are typically in the form of accounts created for the person prior to reaching the age of majority or unexpected distributions such as inheritances, gifts from relatives, or personal injury settlements. OBRA 93 trust provisions must require that the income and principal be unavailable to provide support to the beneficiary. These trusts must also specifically authorize that the state of Michigan will receive all amounts remaining in the trust upon the death of recipient up to an amount equal to the total medical expenditures paid on their behalf, including benefits received prior to the creation of the trust. An exception allows for the assets retained by the trust subsequent to the death of the beneficiary by a trustee that is a nonprofit organization which may then use retained assets for the benefits of others with disabilities.

   b. An amenities trust is designed to supplement means-tested entitlement benefits[1] (e.g., SSI, SSDI, and Medicaid) that are essential to securing personal assistance and medical treatment. Amenities trusts provide a resource for purchasing amenities to enhance the person's quality of life without hindering their access to essential public

[1] Any outright inheritance or distribution received by an individual with an intellectual/developmental disability or mental illness can interfere with the flow of their mean-tested benefits such as SSI or Medicaid.

benefits. They can also be used to purchase a residence[2] for the beneficiary and ensure the beneficiary's needs are monitored subsequent to parents' deaths. An Amenities trust is typically a subtrust to a family or credit shelter trust funded upon the death of the grantor and grantor's spouse. A fiduciary is required to manage the assets throughout the beneficiary's lifetime. The grantors (typically parents) determine the disposition of any remaining trust assets subsequent to the death of the beneficiary.

c. A "solely for the benefit of" trust is created solely for the benefit of a person who is disabled under federal law and is in the amenities trust format. The transfer of assets to the trust (typically by a parent) is used to qualify the parent for Medicaid without disqualifying the person with an intellectual/developmental disability or mental illness from also receiving Medicaid. Thus, the assets are transferred to the trust and removed from the parent's countable assets which are not a divestment subject to the look-back period with respect to the parent's Medicaid application. A parent who is moving toward long-term care and may need to qualify for Medicaid can create a trust that is solely for the benefit of their child with an intellectual/development disability or mental illness and can fund the trust during the parent's lifetime. The parent thus becomes immediately eligible for medical assistance and the beneficiary of the trust does not have to count the trust assets or income generated by the trust. This type of trust can be effective in estate planning when the parent's estate is at risk for depletion due to their medical and long-term care needs.

5. **ABLE (Achieving a Better Life Experience) accounts** are tax-advantaged savings accounts that enable eligible individuals with disabilities to save money in a tax-exempt account that may be used for qualified disability expenses while still maintaining their eligibility for federal public benefits. Contributions to ABLE accounts are made on an after-tax basis and earnings grow tax-deferred and are tax-free if used for qualified disability expenses. Contributions may be made by any person (the account beneficiary, an employer, family and friends) and may or may not be tax deductible depending on the specifics of the state ABLE law. Funds in the account may be used for many different types of expenses (e.g., education, housing, transportation, employment training and support, assistive technology, personal support services, health care expenses, financial management and administrative services, daily living expenses and other expenses to enhance the beneficiary's quality of life). The beneficiary is the owner of the account, but legal guardianship and powers of attorney will permit others to control

[2] If the beneficiary pays rent to the trust and the rent payment constitutes a reasonable share of the expenses for maintaining the home, the provision that the trust cannot be used for shelter is satisfied. The amenities trust can purchase the home in the beneficiary's name if their income is sufficient to pay for basic utilities and property taxes. If the beneficiary opts to include roommates, they can share the expenses associated with home maintenance.

ABLE funds in the event that the beneficiary is unwilling or unable to manage the account.

6. **Power of Attorney** allows an individual to designate a person to discuss and make decisions regarding medical decisions, living situations, confidentiality issues and other areas. The power of attorney allows the individual to give that power and they can take it away if they become dissatisfied with the decisions being made. There are general powers of attorney that convey a broad range of authority and limited powers of attorney that convey power over specific activities.
   a. A General Power of Attorney authorizes the attorney-in-fact to act on the person's behalf in all personal affairs and financial transactions. The authorization ceases upon death. Unless the document is a durable power of attorney, it terminates upon disability or incapacity.
   b. A Limited Power of Attorney authorizes the attorney-in-fact to act on the person's behalf only in matters specifically designated in the written document. The authorization ceases upon death. Unless the document is a durable power of attorney, it terminates upon disability or incapacity.
   c. Durable and Standby Powers of Attorney continue to be effective even in the event of disability or incapacity. Furthermore, a durable power of attorney can be made effective upon occurrence of a certain date or event such as a diagnosis by a physician of disability or incapacity. Because the effective date is delayed, this type of durable power of attorney is referred to as a standby power of attorney. Financial and medical Powers of Attorney can be made durable.
   d. A Medical (Durable) Power of Attorney or Durable Power of Attorney for Health Care appoints an agent to provide informed consent to surgery, medical treatment, personal care, and other medical or health related matters. A Medical Durable Power of Attorney covers a broader spectrum of medical procedures than a Living Will can. This type of power of attorney allows an individual to choose someone as their agent (i.e., someone who acts on their behalf) to make health care decisions whenever the individual cannot, due to unconsciousness or loss of ability to think and reason. This agent is required to make health care decisions according to directions provided by the principal. If the principal's wishes are not clearly understood and defined, then the agent must make decisions based on what he or she believes to be in the principal's best interests. The durable power of attorney for health care only comes into play when the principal's doctor has determined that the principal is unable to make health care decisions for him or herself, even when the situation is temporary.
      1) A Protective Medical Decisions Document (PMDD) is a durable power of attorney for health care that gives a person named (the agent) to make health care decisions the

authority to act on another person's behalf. The PMDD does not give the agent authority to approve the direct and intentional ending of life; it specifically prohibits euthanasia and assisted suicide.

e. A Financial (Durable) Power of Attorney appoints an agent to make financial decisions and/or handle financial transactions for an individual.

7. A conservator is appropriated by the court and is responsible for making decisions about the financial affairs of the ward. The ward's financial affairs include assets (e.g., stocks, bonds, bank accounts, cash and real estate) for which the conservator has assumed responsibility. Generally, the conservator controls all of the ward's income and property, takes care of paying bills, and handles other financial matters. The conservator's duties are to first take possession of all the real and personal property of the ward. The conservator should immediately establish a bank account on which the conservator has signature authority. All of the ward's income, including Social Security, investment income and other sources should go into this account so the conservator can control it and render appropriate accounting when it is required. It is also the conservator's duty to preserve and protect the ward's property. At all times the conservator should exercise the same diligence that he/she would practice handling their own financial affairs. The conservator should invest prudently, keep records, and return the assets at the termination of the conservatorship. The conservator must be careful not to mix their property with the ward's property.

   A conservator's powers are divided into two distinct categories: those powers that can be exercised without prior court approval, and those powers that can be exercised only with the court's prior approval. Powers that the conservator can exercise without prior court approval include: collecting principal and income from any source; suing or defending claims in favor of, or against, the ward; selling or transferring perishable personal property; voting for the ward at corporate meetings; and receiving additional property from any source. The powers that the conservator can exercise only with the court's prior approval include: making payments to or for the benefit of the ward, including payments for nursing homes, medical expenses; investing the ward's funds; executing leases on behalf of the ward; applying any part of the ward's income or property for the support of anyone else; settling a legal claim; selling any property of the ward's; canceling contracts entered into by the ward that are no longer beneficial to the ward; and making gifts.

   a. A limited conservatorship gives only those specific powers that are set out in the court order; the ward can still make decisions in all other matters. By law, the court must attempt to give the conservator the fewest powers necessary to meet the needs of the ward. In contrast, a general or full conservatorship gives the conservator the authority to make all but a few decisions on behalf of the ward.

   b. A standby conservatorship can be appropriate for a person who may currently be able to handle their affairs but anticipates a time when

they may not be able to do so. A person of sound mind can establish a standby conservatorship to plan for any infirmities without giving up present control over the property. A verified petition must be executed for the voluntary appointment of a conservator to establish a standby conservatorship. The petition must contain the express condition that the petition be acted upon by the court only upon the occurrence of a specified event, or the existence of a described condition of mental or physical health of the petitioner. The occurrence of the event, or the existence of such condition, must be established in the manner directed by the petition. The petitioner can revoke the petition before the appointment if the petitioner is of sound mind.

8. An Advance Directive names a proxy and provides guidance about a person's wishes and is essentially a combination of a health care power of attorney (or health care proxy) and a living will. Advance directives are oral or written instructions an adult gives to health care providers, family and loved ones while being able to communicate. The reason for giving advance directives is to ensure a person's wishes regarding their health care are followed in case the person is no longer able to communicate with providers. Advance directives should be executed while the principal (person entering into an advance directive) is competent. The principal must be able to understand who he or she is appointing to make health care decisions and should choose an agent who is trusted. There are two types of advance directives: the durable power of attorney for health care and the living will.
9. A living will, also called a directive or declaration, is a document signed while an individual is competent, that instructs doctors to withdraw or withhold artificial life support if the individual becomes medically terminal. Living wills only apply to artificial life sustaining procedures. It should be noted that because the attending physician may be a total stranger who is completely unfamiliar with the values and wishes of the person served, terms in the document may be interpreted by the physician in a manner that was not intended by the signer. In addition, family members and others who are familiar with the signer's values and wishes have no legal standing to interpret the meaning of the directive.

Definitions:

ABLE Act: The Stephen Beck Jr. Achieving a Better Life Experience (ABLE) Act (PL 113-295) added Section 529A to the federal tax code to enable eligible individuals with disabilities to save money in a tax-exempt account that may be used for qualified disability expenses while still keeping their eligibility for federal public benefits.

ABLE Account: A tax-advantaged savings account that qualified individuals with disabilities may open as a result of the passage of the ABLE Act of 2014 and subsequent enactment of state ABLE laws. Individuals with disabilities can only have $2,000 in assets at any given time in order to remain eligible for many federal means-tested benefits programs which provide much-needed supports, such as Supplemental Security Income (SSI). Under ABLE, eligible individuals and families may establish ABLE savings accounts that will not affect their eligibility for SSI (up to $100,000), Medicaid and other public benefits. ABLE accounts provide a mechanism to essentially increase this $2,000 asset limitation so

that individuals with disabilities and their families can save money for their future and to improve their quality of life.

An individual must meet two requirements to be eligible for an ABLE account: an age requirement and a severity of disability determination. The onset of symptoms of the person's disability must have occurred before age 26. Additionally, the disabled individual must have "marked and severe functional limitations" (essentially, a Social Security definition of disability). An individual whose disability occurred prior to age 26 and is already receiving SSI and/or SSDI is automatically eligible to establish an ABLE account. Those who are not recipients of SSI and/or SSDI but still meet the age of onset disability requirement will be eligible to open an ABLE account upon obtaining a disability certification from their physician.

The total annual contributions by all participating individuals, including the beneficiary, family and friends, is $14,000 (the federal gift tax exclusion). The total limit of contributions that could be made to an ABLE account over time is tied to the individual state's maximum amount for regular 529 accounts (typically around $350,000). The first $100,000 in ABLE accounts will be exempted from the SSI $2,000 individual resource limit. After $100,000, the beneficiary's SSI will be suspended (but not terminated), though Medicaid benefits will continue regardless of ABLE funds.

Amenity: An amenity is anything that is not food or shelter and does not involve a direct distribution of cash to a Medicaid recipient. For purposes of SSI, amenities trusts cannot pay for basic support including rent, utilities (gas, water, sewer, electricity, and garbage removal), mortgage payments, property taxes, and property insurance.

Allowable amenities include:

- acupuncture/acupressure
- advocacy
- appliances (TV, VCR, stereo, microwave, stove, refrigerator, washer/dryer)
- bottled water
- bus pass/public transportation fees
- clothing
- clubs and club dues (record clubs, book clubs, health clubs, service clubs)
- computer (hardware, software, programs, Internet service)
- courses or classes (academic or recreational)
- curtains, blinds, drapes
- dry cleaning and laundry services
- elective surgery
- fitness equipment
- furniture, home furnishings
- gasoline for automobile
- haircuts/salon services
- house cleaning/maid services
- insurance (automobile and/or possessions)
- linens and towels
- massage
- musical instruments (including lessons)
- nonfood grocery items (laundry soap, bleach, fabric softener, deodorant, dish soap, hand and body soap, personal hygiene products, paper towels, napkins, Kleenex, toilet paper, any household cleaning products)
- over-the-counter medications (including vitamins or herbs)
- personal assistance
- pet, pet supplies
- physician specialists
- private counseling
- repair services (appliance, automobile, bicycle, household)
- retail store charge accounts (gift stores, craft stores, hardware stores, pet stores)
- sporting goods/equipment
- taxi cab scrip

- telephone, internet, cable or satellite television
- tickets to concerts or events (for beneficiary and accompanying companion)
- transportation (automobile, motorcycle, bicycle, moped)
- vacation (including paying for a companion to accompany the beneficiary)

Guardian: A person who is responsible for someone legally unable to care for him/herself and manage their affairs and has been given decision making authority pursuant to testamentary or court appointment. A guardian is appointed by the court to make decisions about the ward's needs or affairs other than financial matters. These may include decisions regarding medical treatment, where the ward lives, and arrangements for services such as meals, personal care, training, and education. A guardian's duties and powers are divided into two distinct categories: those powers and duties that can be exercised without prior court approval, and those powers and duties that can be exercised only with the court's prior approval. Powers that a guardian can exercise without prior court approval include: providing for the care, comfort and maintenance of the ward, including appropriate training and education intended to maximize the ward's potential; taking reasonable care of the ward's clothing, furniture, vehicle and other personal effects; assisting the ward in developing maximum self-reliance and independence; ensuring that the ward receives necessary emergency medical services and routine medical care; ensuring that the ward receives professional care, counseling, treatment and services as needed; plus any other powers and duties that the court may specify. The powers the guardian can exercise only with the court's prior approval include: changing the ward's permanent residence if the proposed residence is more restrictive than the current residence; arranging the provision of major elective surgery or any non-emergency major medical procedure; and consenting to the withholding or withdrawal of life-sustaining procedures.

A **general guardian** is someone charged with the care of both the ward and his property. This includes room and board, personal maintenance, financial needs, medical care, and other legal responsibilities pertaining to handling the ward's estate, property, and assets responsibly. A **personal guardian** or **guardian of the person** has the power only to make all personal decisions, including where the ward will live.

A **full (plenary) guardian** possesses all the legal duties and powers enumerated in law. A person with a full guardian has some or all of their rights taken away and given to another person including the right to choose their own clothes, leisure activities, friends, and food.

A **limited guardian** possesses fewer than all other legal duties and powers of a full guardian and whose rights, powers, and duties have been specifically enumerated by the court. A limited guardianship gives the guardian only those specific powers that are set out in the court order; in all other matters the ward can still make decisions for him or herself. The court must, by law, only give the guardian the powers necessary for the guardian to meet the needs of the ward. By contrast, a general or full guardianship gives the guardian the authority to make all decisions on behalf of the ward, except those that require prior court approval.

A person may currently be able to handle their affairs but anticipates a time when he/she may not be able to do so. To pre-determine who will serve as guardian, if in the future a guardianship becomes necessary, a person of sound mind can establish a **standby guardianship**. The standby guardianship takes effect only upon the occurrence of an event specified in the document (petition). With a standby guardianship, a person can retain control over their personal affairs until the event specified occurs. To establish a standby

guardianship, a verified petition must be executed for the voluntary appointment of a guardian. The petition must contain the express condition that the petition be acted upon by the court only upon the occurrence of an event specified or the existence of a described condition of mental or physical health of the petitioner. The occurrence of the event or the existence of such conditions shall be established in the manner directed by the petition. The petitioner can revoke the petition before the need for appointment if the petitioner is of sound mind.

A guardian is usually selected in accordance with the following prioritized list:

1. A member of the individual's natural support system (e.g., spouse, adult child, parent, sibling relative or friend)
2. A representative of a recognized advocacy organization (e.g., United Cerebral Palsy Association of Michigan, National Association for the Mentally Ill Michigan Chapter, the ARC, Disability Rights Michigan).

It should be noted that Michigan law provides that guardianship over individuals with intellectual/developmental disabilities be considered as a last resort (MCL 330.1602). In addition, guardianship does not confer power of compulsion, only of persuasion. Guardianship is not appropriate in order simply to require a person to take medication nor does it authorize a person to be treated without their consent. Moreover, unless a guardian is with the person 24/7, guardianship cannot prevent abuse or exploitation; guardianship cannot prevent bad things from happening.

Health Care Proxy: An agent who makes health care decisions for a person lacking the capacity to make such decisions for him/herself.

Incapacitated Person: Any person who is impaired by reason of mental illness, mental deficiency, physical illness or disability, chronic use of drugs, chronic intoxication or other cause (except minority) to the extent that s/he lacks sufficient understanding or capacity to make or communicate responsible decisions concerning their person or which cause has so impaired the person's judgment that they are incapable of realizing and making a rational decision with respect to their need for treatment.

Living Will: A legal document directing the principal's doctor to withhold or withdraw certain treatments (life-sustaining procedures) that could prolong the dying process. It is used to express wishes for medical decisions about withholding or withdrawing of life-sustaining treatment wherein the person lacks capacity to make decision. This advance directive becomes effective only at the point when, in the written opinion of the doctor (and confirmed by one other doctor), the principal is expected to die soon and is unable to make health decisions for him or herself (because he/she is unconscious or unable to think and reason) or because of permanent unconsciousness (irreversible coma or persistent vegetative state). A living will is often used in conjunction with health care proxy.

Power of Attorney: A written document by which one person (the principal) gives to another person (attorney-in-fact) the authority to act on the first person's behalf in one or more matters. The person giving legal authority must be competent to grant a power of attorney and only a trusted individual should be chosen to act as the attorney-in-fact. A power of attorney for financial matters grants authority to the attorney-in-fact to transact business on the person's behalf. The power of attorney can grant the attorney-in-fact one or all of the following:

- Open, maintain or close bank accounts or brokerage accounts
- Purchase insurance for the principal's benefit

- Access to safe deposit boxes and their contents
- Make financial investments
- Borrow money, mortgage property, or renew or extend debts
- Prepare and file federal and state income tax returns
- Vote at corporate meetings
- Sell, convey, lease or maintain real estate
- Initiate, defend, prosecute, or settle any lawsuit
- Start or carry on business
- Employ professional and business assistances of all kinds, including lawyers, accountants, real estate agents, etc.
- Apply for benefits and participate in governmental programs
- Transfer to a trustee any and all property
- Disclaim part or all of an inheritance

Representative Payee: A person appointed to take care of another person's money. Government benefits may be paid to a representative payee. The person appointed as the Representative Payee will pay for the other person's living expenses. The Social Security Administration and the Veterans Administration (if applicable) must be contacted to have a representative payee appointed for someone.

Trust: A legal relationship in which one person (a trustee) holds real or personal property (e.g., money, real estate, stocks, bonds, collections, business interests, personal possessions, and other tangible assets) for the benefit of another person (the beneficiary). Trusts that can be changed or terminated at any time by the grantor are **revocable**. Trusts that cannot be changed or terminated before the time specified in the trust itself are **irrevocable**. The trustee holds legal title to the property transferred to the trust and has a legal duty to use the property as provided in the trust agreement as permitted by law. The beneficiary retains equitable title (i.e., the right to benefit from the property as specified in the trust). Trusts can be useful planning tools for incapacity because they can be established and controlled by a competent person and later continue in operation under a successor trustee if the person establishing the trust becomes unable to manage their affairs. One person often establishes a trust for the benefit of another. This type of trust involves at least three people: the grantor/trustor (the person who creates the trust); the trustee (the person or financial institution who holds and manages the property for the benefit of the grantor and others); and the beneficiary or beneficiaries (the person(s) who receives the benefits from the trust).

References:

A. Centers for Medicare & Medicaid Services (CMS) Home and Community Based Services (HCBS) Final Rule (CMS 2249-F/2296-F): https://www.michigan.gov/documents/mdch/Final_Rule_474879_7.pdf

B. MDHHS BHDDA HCBS Guardianship FAQs: https://www.michigan.gov/documents/mdhhs/MDHHS_BHDDA_HCBS_GUARDIANSHIP_FAQ_6.25.18_634277_7.pdf

C. Medcaid.gov Home & Community Based Services Final Regulation: https://www.medicaid.gov/medicaid/hcbs/guidance/hcbs-final-regulation/index.html

D. Michigan Medicaid Provider Manual: Home and Community Based Services Chapter

E. Michigan Mental Health Code, Chapter 6 (*Guardianship for the Developmentally Disabled)*: https://www.legislature.mi.gov/(S(es1wxoil2rubqjnavtoe3pjd))/documents/mcl/pdf/mcl-258-1974-6.pdf
F. SCCMHA Policy 02.03.03 – Person-Centered Planning
G. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports

Exhibits:
A. Guardianship Referral Form
B. Authorization for Payment to Guardianship Services
C. Guardianship Questionnaire Electronic Form

Procedure:

ACTION	RESPONSIBILITY
1. Incorporates discussion of guardianship issues and alternatives into the person-centered planning process, as indicated/needed, and documents that process in the person-centered plan of service and ongoing reviews in accordance with Standards C and D of this policy.	1. Case Holder
2. Establishes a guardianship request review committee to review requests for guardianships	2. Executive Director of Clinical Services
3. Submits the guardianship referral form to the Administrative Coordinator for the Customer Service/Recipient Rights Office	3. Case Holder
4. Adds the form to the guardianship review committee's monthly meeting agenda.	4. Administrative Coordinator for the Customer Service/Recipient Rights Office
5. Meets with the Case Holder, reviews relevant information, and decides whether or not SCCMHA agrees that the Case Holder should pursue a guardianship and whether or not to request authorization for a court-required psychological evaluation.	5. SCCMHA Guardianship Committee
6. If approved, completes the Guardianship Questionnaire form and sends to	6. Case Holder

Braun Kendrick Law Offices for pursuit of guardianship	
7. Sends a copy of the signed Guardianship Referral form to Medical Records for scanning into the Clinical Record.	7. Administrative Coordinator for Customer Service/Recipient Rights
8. Approves guardianship for a period of one year only.	8. Guardianship Committee
9. Completes and submits a new referral to the Guardianship Committee if the guardianship is not completed within one year.	9. Case Holder
10. Works with family/advocate/supporter to establish an alternative to guardianship if the committee determines the Case Holder should not pursue guardianship.	10. SCCMHA Guardianship Committee and Case Holder
11. Completes the Authorization for Payment form and sends it to Guardianship Services when there is a vacancy in the list kept by Guardianship Services.	11. Director of Recipient Rights, Customer Service, & Security

Exhibit A

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Guardianship Referral Form

Please review Alternatives to Guardianship Policy # 02.03.12 before making the referral to the Guardianship Committee

Case Manager/Support Coordinator to complete form and send to the Customer Service/Recipient Rights Administrative Coordinator for inclusion on the next scheduled Guardianship Committee Meeting.

Date of Referral:	
Consumer Name:	Consumer Case #:
Case Holder:	
Provider/Team:	
Reason for Referral:	
Referral Approved by Supervisor:	Name/Signature / Date

****

Information Below to be completed by Guardianship Committee

Date of Guardianship Committee Meeting:	
Request for SCCMHA Support of Guardianship Accepted:	☐
Request for SCCMHA Support of Guardianship Declined:	☐
Reason for Decision OR other Recommendations:	
SCCMHA Guardianship Chair – Kristie Wolbert	**Date**

Scan: Legal

4/22/20 tn

Exhibit B

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Authorization for Payment to Guardianship Services

Guardianship Committee to complete this form for every person approved for Guardianship or Payee Services through contract with SCCMHA.

Consumer Name: _____ **Consumer Case #:** _____

Case Holder: _____

Provider/Team: _____

Reason for Authorization: _____

_____

Service to be Provided: ☐ **Guardianship** ☐ **Payee**

Date of Guardianship/Payee Authorization: _____

_____ _____

SCCMHA Guardianship Chair – Kristie Wolbert **Date**

Exhibit C

GUARDIANSHIP QUESTIONNAIRE

Kosta D. Povich, Esq.
Braun Kendrick Finkbeiner P.L.C.
4301 Fashion Square Blvd.
Saginaw, Michigan 48603
Phone: (989) 399-0620
Fax: (989) 799-4666
E-mail Address: kospov@braunkendrick.com

If you are asking the Court to appoint a guardian, then you are the *petitioner*. The person who requires a guardian is the *proposed ward*. The person/entity that you want to have the Court appoint as guardian is the *proposed guardian*. The information contained in this Questionnaire will be used to draft a Petition seeking the appointment of the *proposed guardian*.

NOTE: A Report must accompany the Petition that is submitted to the Court for the appointment of a guardian. The Report is to be completed by a licensed medical professional and cannot be more than a year old. Please also note that we will be required to submit information regarding the medications that the proposed ward is receiving. The type of Petition and Report that is submitted to the Court will depend on what type of guardianship is sought. The Court has standard forms that are used for the Petition and the Report.

*After you have completed this Questionnaire, please ***fax*** it to my attention at the number above. Please do not hesitate to call me at the number above regarding any questions or concerns. I look forward to working with you on this matter. Thank you.

****

GUARDIANSHIP COMMITTEE ONLY

A guardian is needed to assist the proposed ward with the following responsibilities and duties:

Proposed ward's name: _____

☐ medical treatment ☐ living arrangements
☐ program and placement decisions ☐ financial matters
☐ other: _____

Guardianship Committee is Requesting:
☐ plenary (full) guardian of the ☐ individual ☐ estate

☐ partial guardian of the ☐ individual
☐ estate with the following powers: _____

****

****

PETITIONER INFORMATION:

Name of the petitioner: _____

Petitioner's interest/relationship to the proposed ward: _____

☐ Address: _____

City: _____ State: _____Zip Code: _____

Telephone number: _____ Cell phone number:_____

Email: _____ Fax: _____

****

PROPOSED GUARDIAN INFORMATION IF NOT GUARDIANSHIP SERVICES OF SAGINAW COUNTY, INC.:

Full name of proposed guardian: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____ Cell phone number:_____

Email: _____

****

PROPOSED WARD INFORMATION:

Proposed ward's name: _____

Address where proposed ward is currently living: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____ Cell phone number:_____

County proposed ward is a resident of: _____

Date of birth: _____

Social security number: _____ Race: _____

☐ Male ☐ Female

If applicable, citizen of foreign country: _____

Does the proposed ward have:

A guardian: ☐ Yes ☐ No

A Conservator: ☐ Yes ☐ No

A General Durable Power of Attorney: ☐ Yes ☐ No

A Durable Medical Power of Attorney: ☐ Yes ☐ No

A representative payee for social security benefits: ☐ Yes ☐ No

*If you answered "Yes" to any of the above, please provide additional information/ documentation of same.

****

The proposed ward has a severe, chronic condition that meets the following:

☐ self-care ☐ receptive and expressive language ☐ learning ☐ mobility

☐ self-direction ☐ capacity for independent living ☐ economic self-sufficiency

****

Specific nature and extent of proposed ward's disability is:

_____

****

The proposed ward lacks sufficient understanding or capacity to make or communicate informed decisions due to: (mark all that apply)

☐ mental illness ☐ mental deficiency ☐ physical illness/disability
☐ chronic intoxication ☐ chronic drug use

Facts about the proposed ward's recent condition or conduct that is believed to warrant the need for a guardian and/or conservator:

_____

Estimated value of proposed ward's estate and income:

Real Estate: $ _____ Yearly Income: $ _____

Personal Property: $ _____ Source of Yearly Income: _____

Does the proposed ward receive, or is he/she entitled to receive any income, financial assistance or other payment of money? If so, provide yearly amount.

Social Security: Yes _____ No _____ Unknown _____

SSI: Yes _____ No _____ Unknown _____

MDHS: Yes _____ No _____ Unknown _____

Pension: Yes _____ No _____ Unknown _____

Veterans benefits: Yes _____ No _____ Unknown _____

If yes, provide claimant number: _____

Annuity Payments: Yes _____ No _____ Unknown _____

Dividends: Yes _____ No _____ Unknown _____

****

If an action within the jurisdiction of the family division of circuit court involving the family or family members of the proposed ward has been previously filed provide the following:

County: _____ Judge: _____

Case Number: _____ ☐ remains ☐ is no longer pending.

****

Name of proposed ward's spouse: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

****

All children of the proposed ward: (attach extra sheet if necessary)

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

****

Name of proposed ward's father, if living: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

Name of proposed ward's mother, if living: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

****

Please provide information regarding any other relatives of the proposed ward: (attach extra sheet if necessary)

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

****

Who currently has the care and custody of the proposed ward?

Name: _____ DOB: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Telephone number: _____

****

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Wellness</td><td>Chapter: 02.03. – Philosophy of Care</td><td>Subject No: 02.03.25</td></tr>
<tr><td rowspan="2">Effective Date:
6/13/17</td><td>Date of Review/Revision:
4/10/18, 4/9/19,7/29/20, 4/13/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

The purpose of this policy is to delineate a framework for the adoption and support of a culture of well-being for persons served and staff so that services and supports are provided in a person/family-centered, trauma-informed, recovery/resiliency-oriented, developmentally and phase-of-life appropriate, culturally and linguistically sensitive manner that promotes engagement and shared decision-making with the person served and employs evidence-based practices and treatments to maximize the potential for beneficial outcomes.

Policy:

A. SCCMHA recognizes that individuals with a mental illness experience a life span that is 25 years shorter than members of the general population (with an average age of death of 53 years). Moreover, those who have a co-occurring substance use disorder are at even greater risk for premature death (with an average age of death of 45 years). This disparity in life expectancy has been found to be primarily due to increased morbidity and mortality from treatable medical conditions that are caused by modifiable risk factors including smoking, obesity, and substance abuse, as well as preventable medical conditions such as diabetes and cardiovascular, respiratory, or infectious diseases (including HIV). In addition, people with mental health problems often live in poverty and experience social isolation, stigma, and trauma, which can lead to higher levels of stress and/or reduce access to quality primary care services that can help prevent and manage health conditions.

B. SCCMHA recognizes that persons with substance use disorders (SUDs) also often experience comorbid mental health conditions including anxiety disorders, post-traumatic stress disorder (PTSD), attention-deficit hyperactivity disorder (ADHD), as well as physical health conditions, including chronic pain, https://www.drugabuse.gov/publications/research-reports/common-comorbidities-substance-use-disorders/references cancer, and heart disease. In addition, suicide is the leading cause of death among people with SUDs and co-occurring mental illness and SUDs increases the risk even further. (SAMHSA)

C. SCCMHA also recognizes the growing disparity in health status and life expectancy between individuals with intellectual/developmental disabilities (I/DD) and the general population. Individuals with I/DD have been found to be in poorer overall health and have a higher incidence of obesity (as well as the secondary conditions that often accompany obesity including hypertension, hypercholesterolemia, and diabetes), coronary heart disease, and pulmonary problems.

D. SCCMHA further recognizes that chronic diseases (e.g., depression and hypertension) can lead to a decline in the overall health of employees and that a healthy lifestyle can lead to a significant reduction in the risk of developing chronic diseases and premature disability and death.

E. SCCMHA-funded providers shall support physical health prevention, wellness checks, routine tests or screenings recommended by physicians, and other health and wellness promotion activities for persons served and staff members.

F. SCCMHA shall adopt the Wellness Initiative developed by the Substance Abuse and Mental Health Service (SAMHSA) which encourages the incorporation of the Eight Dimensions of Wellness into the lives of persons served as well as staff:
    1. **Emotional:** Coping effectively with life and creating satisfying relationships
    2. **Environmental:** Good health by occupying pleasant, stimulating environments that support well-being
    3. **Financial:** Satisfaction with current and future financial situations
    4. **Intellectual:** Recognizing creative abilities and finding ways to expand knowledge and skills
    5. **Occupational:** Personal satisfaction and enrichment from one's work
    6. **Physical:** Recognizing the need for physical activity, healthy foods and sleep
    7. **Social:** Developing a sense of connection, belonging, and a well-developed support system
    8. **Spiritual:** Expanding our sense of purpose and meaning in life

Application:
This policy applies to all SCCMHA employees, persons served, visitors, volunteers, and contractors.

Standards:
A. SCCMHA shall support the well-being of persons served and staff through a whole-person approach that encompasses the integration of mental health and physical health which allows for holistic approaches to disease prevention and health promotion.

B. SCCMHA shall promote a culture of well-being among persons served as well as staff and support the adoption of a healthy lifestyle.
    1. SCCMHA shall use its Better Together We Can campaign to promote health and well-being among persons served, providers and staff through SCCMHA-sponsored events, activities, classes and presentations.
        a. To encourage participation in SCCMHA's culture of well-being and adopt a healthy lifestyle, full and part-time SCCMHA employees

shall earn Better Together (BT) hours based on employment status in accordance with SCCMHA human resource policy.

C. SCCMHA shall promote mental health recovery by supporting improved general health and vice versa.

D. Persons served shall be encouraged to stop or reduce high-risk behaviors as well as engage in healthy activities, including, but not limited to:
   1. Eating a healthy diet
   2. Getting physical exercise
   3. Effective stress management, including, but not limited to:
      a. Gaining an understanding of triggers and how to mitigate or avoid them
      b. Learning to use mindfulness as a technique to manage stress
   4. Recommended health screenings (e.g., A1c level, blood pressure, body mass index, cholesterol levels)
   5. Maintaining oral health and accessing preventive oral health services
   6. Screening for depression and suicidality
   7. Participating in programs that target tobacco cessation
   8. Avoiding substance misuse and abuse
   9. Developing a natural support system
   10. Engaging in meaningful activities

Definitions:

Health: A resource that allows people to realize their aspirations, satisfy their needs and to cope with the environment in order to live a long, productive, and fruitful life. Health is more than the absence of disease. (Centers for Disease Control and Prevention [CDC])

Well-being: While there is a lack of consensus around a single definition of well-being, it is generally agreed that, at minimum, well-being includes the presence of positive emotions and moods (e.g., contentment, happiness), the absence of negative emotions (e.g., depression, anxiety), satisfaction with life, fulfillment and positive functioning. Aspects of well-being include: physical well-being; economic well-being, social well-being; development and activity; emotional well-being; psychological well-being; life satisfaction; domain specific satisfaction; engaging activities and work.

Wellness: A conscious, deliberate process that requires an individual to become aware of and make choices for a more satisfying lifestyle. It is the process of creating and adapting patterns of behavior that lead to improved health in the wellness dimensions (physical, spiritual, social, intellectual, emotional/mental, occupational, environmental, and financial).

Wellness is self-defined because each person has individual needs and preferences, and the balance of activity, social contact, and sleep varies from person to person.

Wellness Lifestyle: A self-defined balance of health habits such as adequate sleep and rest, productivity, exercise, participation in meaningful activity, nutrition, productivity, social contact, and supportive relationships.

Whole-Person/Integrated Care: A comprehensive and coordinated person-centered system of care that allows healthcare professionals (i.e., behavioral health, primary care, and specialty providers) to simultaneously consider all of health conditions of persons served, resulting in the systematic coordination of physical and behavioral healthcare. Such

integrated healthcare services that are delivered in a whole-person approach produce beneficial outcomes for people with multiple and complex healthcare conditions.

References:

A. Glassheim, B. (March 2022). *A Guide to Evidence-Based Wellness Practices.* SCCMHA: https://www.sccmha.org/userfiles/filemanager/1058/
B. SCCMHA Consumer Health Education Council Workgroup Charter
C. SCCMHA Employee Handbook Policy Number 528 – Better Together Bank
D. SCCMHA Employee Wellness Committee Workgroup Charter
E. SCCMHA Policy 02.03.09 – Evidence-Based Practices (EPBs)
F. SCCMHA Policy 03.02.46 – Whole-Person Care
G. SCCMHA Wellness Incentive Program

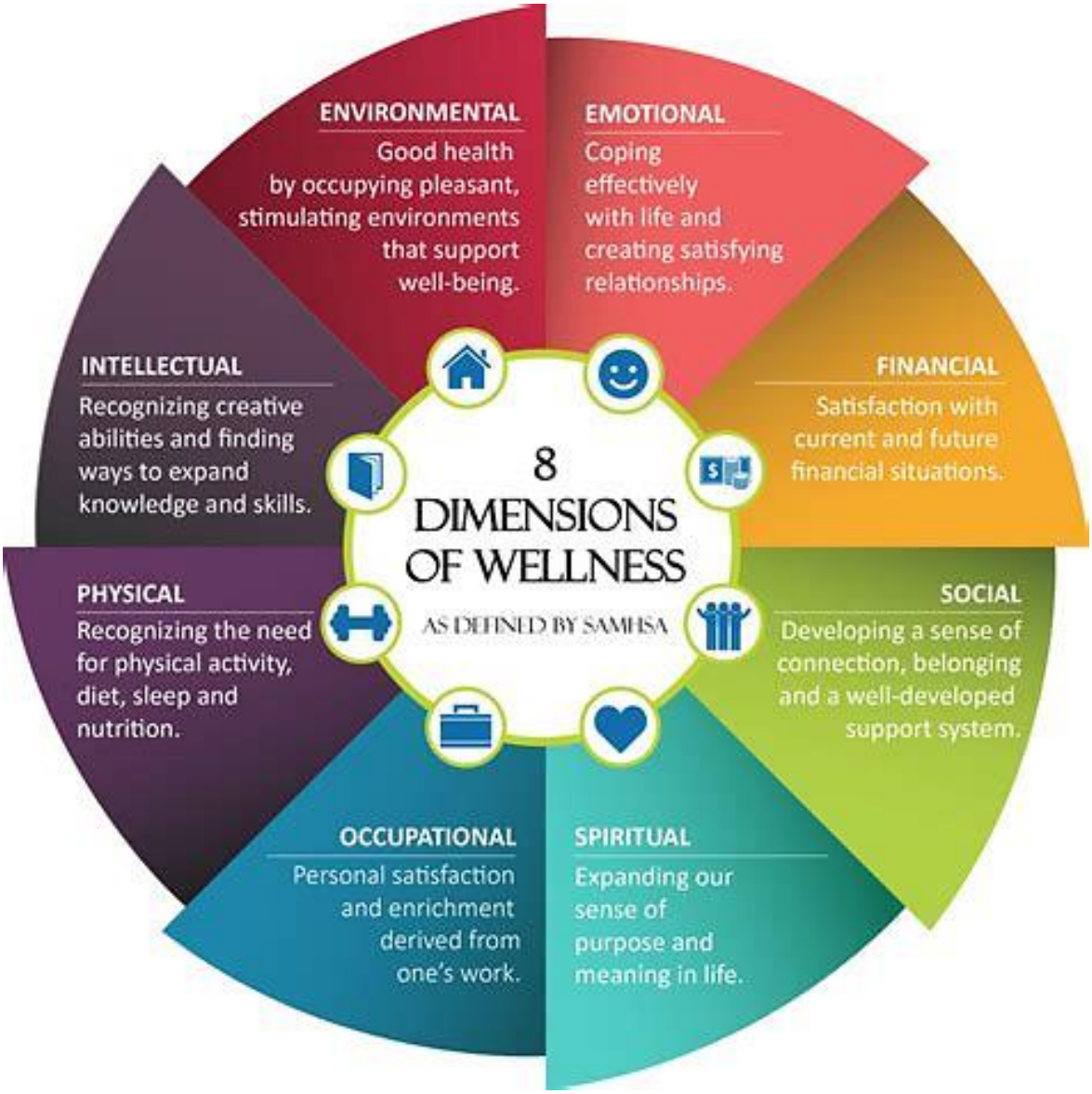
Exhibits:

A. SAMHSA Wellness Wheel

Procedure:

None

Exhibit A: SAMHSA Wellness Wheel



<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: SOGI Safe</td><td>Chapter: 02 - Customer Services and Recipient Rights</td><td>Subject No: 02.03.41</td></tr>
<tr><td rowspan="2">Effective Date:
4/10/18</td><td>Date of Review/Revision:
4/9/19, 8/21/20, 5/10/21, 4/12/22, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim, Heidi Wale Knizacky

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to apply specific staff development training that is designed to promote a safe, supportive and welcoming environment for LGBTQAI+ persons as well as to enhance the competency and effectiveness of providers who serve LGBTQAI+ persons and their families.

Application:
This policy applies to SCCMHA-funded providers.

Policy:

SCCMHA recognizes that LGBTQAI+ people face many health disparities and experience stigma and discrimination in health care settings as well as discrimination in employment, housing, and public accommodations. SCCMHA also recognizes that LGBTQAI+ persons served have higher rates of histories of trauma (including abuse and neglect), depressive symptomatology, PTSD (posttraumatic stress disorder), suicidality, and SUDs (substance use disorders) than their counterparts in the general population.

In addition, SCCMHA recognizes that LGBTQAI+ youth are more likely than their counterparts in the general population to experience family rejection, victimization (including bullying, teasing, harassment, and physical assault), employment and housing instability, and have higher rates of juvenile justice involvement.

In an effort to maximize the potential for recovery and resiliency through the provision of affirming services and supports to LGBTQAI+ persons served, SCCMHA shall, resources permitting, offer a Sexual Orientation and Gender Identity (SOGI) Safe Study group to providers.

Standards:

A. SCCMHA shall endeavor to increase its provider network's understanding of the unique needs of LGBTQAI+ individuals in order to be able to effectively assess

and provide and/or coordinate appropriate, supportive services within a safe environment for LGBTQAI+ persons served and their family members by providing relevant training, including a SOGI Safe Study Group.

B. The SCCMHA SOGI Safe Study Group shall endeavor to inculcate the following principles and standards in order to increase the number of providers that can effectively and skillfully offer an authentically safe, non-judgmental and affirmative space for LGBTQAI+ persons served and their families:

1. Use gender neutral language (e.g., significant other) until informed by the person served of another preference.
2. Understand and appreciate the fact that people may use a range of pronouns, including "she/her/hers", "he/him/his", and "they/them/their".
3. Avoid disrespectful language, including terminology that is considered outdated (e.g., homosexual, transvestite, etc.).
4. Ask, rather than assume terms, labels, and experiences.
5. Avoid assuming gender or sexual orientation; a person's gender or sexual orientation cannot be assumed based on how they look or sound.
6. Understand and appreciate the fact that gender identity and sexual orientation labels are personally relevant, and that these labels may change, especially for individuals who are gender fluid, working through the Coming Out process, or Questioning.
7. Appreciate and understand the ways the sexual orientation and gender identity of the person served can be relevant to the provision of mental health services and supports.
8. Understand and appreciate the challenges families can face in accepting a child who identifies as LGBTQA+.
9. Demonstrate cultural awareness of multiple social identities and the intersectionality of race, ethnicity, religion and other cultural factors (e.g., socioeconomic status).
10. Understand how past and present trauma may impact the lives of LGBTQ+ people and ways to avoid re-traumatization as well as mitigate the adverse effects of trauma.
11. Differentiate between effective, appropriate evidence-based treatments and those that are ineffective and/or harmful to LGBTQ+ persons served.

Definitions:

Coming Out: The process that LGBTQAI+ people go through as they work to accept their sexual orientation or gender identity and share that identity openly with other people. Coming out is a process of understanding, accepting, and valuing one's sexual orientation/identity that typically occurs in stages and may not be linear. Moreover, a person may come out multiple times to different people and groups throughout a lifetime. Every time an LGBTQ+ person meets someone new (e.g., friends, co-workers, healthcare and other professionals, etc.), they have to decide if, when, and how to come out. Finally, it should be noted that coming out can have benefits and risks and is not always by choice; some people are outed by others.

LGBTQAI+: An acronym for lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and other sexual and gender minorities. It refers to a population of people united by having gender identities or sexual orientations that differ from the heterosexual

and cisgender (i.e., individuals whose gender identity matches the sex that they were assigned at birth or those who perform a gender role society considers appropriate for one's sex) majority. It is used as a catchall term to represent the entire spectrum of diversity in sexual orientation and gender identity.

Questioning: The process of exploring, learning, or experimenting with one's gender, sexual orientation, romantic orientation, or another part of one's identity. Questioning can happen at any age and can take anywhere from days to years. Questioning is normal for anyone, irrespective of whether the person turns out to actually be of a gender or sexual minority or not. Questioning can describe the process of exploring one's identity as well as an individual who is in the process of questioning.

SOGI: Sexual Orientation and Gender Identity is an all-inclusive term; sexual orientation describes people that an individual is sexually or romantically attracted to as compared to their own gender; gender identity is any individual's own internal awareness of their gender (often "male" or "female," but gender is not solely a binary construct). Sexual orientation and/or gender identity may change during an individual's lifetime.

SOGI Safe: The provision of a safe and welcoming space and the creation of a supportive and inclusive climate that encourages the success of all individuals irrespective of sex, gender identity, or sexual orientation.

References:

A. It's Pronounced Metrosexual: http://itspronouncedmetrosexual.com/
B. National LGBT Health Education Center: https://www.lgbthealtheducation.org/
C. SCCMHA LGBTQAI+ & SOGI (Sexual Orientation Gender Identity: https://www.sccmha.org/about/diversity-equity-and-inclusion-initiative/lgbtqia-and-and-sogi.html
D. SCCMHA Policy 02.01.01.02 – Cultural Competence
E. SCCMHA Policy 02.03.08 – Welcoming
F. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports
G. SCCMHA Policy 03.02.35 – Serving LGBTQAI+ Persons

Exhibits:

A. SCCMHA SOGI Safe Study Group Pre-Test
B. The Genderbread Person v3.3
C. What Does it Mean to be SOGI Safe?

Procedure:

ACTION	RESPONSIBILITY
Arrange accommodations for the SCCMHA SOGI Safe Study Group in conjunctions with the facilitator(s)	SCCMHA CE Unit
Promote the group to recruit participants	SCCMHA CE Unit/Agency Leaders
Complete the SCCMHA SOGI Safe Study Group Pre-Test	SOGI Safe Study Group Participants
Convene the SCCMHA SOGI Safe Study Group	SOGI Safe Study Group Facilitator(s)
Complete the SCCMHA SOGI Safe Study Group Post-Test	SOGI Safe Study Group Participants

Evaluate the effectiveness of the SOGI Safe Study Group	SOGI Safe Study Group Facilitator(s)

Exhibit A

SCCMHA SOGI Safe Study Group

Pre-Test

*Name: Job Title:

**This questionnaire is being used to establish a baseline from which the outcomes of this study group will be measured. Your name is requested so individual changes can be measured by differences in Post-Test scores at the end of this program. All reporting will only show aggregate results and absolutely no individual responses will be shared with anyone outside of the APPRECOTS team.*

Lesbian, Gay, and Bisexual Affirmative Counseling Self-Efficacy Inventory

Frank R. Dillon and Roger L. Worthington

Instructions: Below is a list of activities regarding counseling/psychotherapy. Indicate your confidence in your current ability to perform each activity by marking the appropriate answer below each question ranging from Not at all Confident to Extremely Confident. Please answer each item based on how you feel now, not on your anticipated (or previous) ability. I am interested in your actual judgments, so please be honest in your responses.

	How confident am I in my ability to … ?	Not at all Confident					Extremely Confident
1	Directly apply sexual orientation/identity development theory in my clinical interventions with lesbian, gay, and bisexual (LGB) clients.	1	2	3	4	5	6
2	Directly apply my knowledge of the coming out process with LGB clients.	1	2	3	4	5	6
3	Identify specific mental health issues associated with the coming out process.	1	2	3	4	5	6
4	Understand the socially constructed nature of categories and identities such as lesbian, bisexual, gay, and heterosexual.	1	2	3	4	5	6
5	Explain the impact of gender role socialization on a client's sexual orientation/identity development.	1	2	3	4	5	6
6	Apply existing American Psychological Association guidelines regarding LGB-affirmative counseling practices.	1	2	3	4	5	6
7	Use current research findings about LGB clients' critical issues in the counseling process.	1	2	3	4	5	6
8	Assist LGB clients to develop effective strategies to deal with heterosexism and homophobia.	1	2	3	4	5	6

9	Evaluate counseling theories for appropriateness in working with an LGB client's presenting concerns.	1	2	3	4	5	6
10	Help a client identify sources of internalized homophobia and/or biphobia.	1	2	3	4	5	6
11	Select affirmative counseling techniques and interventions when working with LGB clients.	1	2	3	4	5	6
12	Assist the development of coping strategies to help same-sex couples who experience different stages in their individual coming out processes.	1	2	3	4	5	6
13	Facilitate an LGB-affirmative counseling/support group.	1	2	3	4	5	6
14	Recognize when my own potential heterosexist biases may suggest the need to refer an LGB client to an LGB-affirmative counselor.	1	2	3	4	5	6
15	Examine my own sexual orientation/identity development process.	1	2	3	4	5	6
16	Identify the specific areas in which I may need continuing education and supervision regarding LGB issues.	1	2	3	4	5	6
17	Identify my own feelings about my own sexual orientation and how it may influence a client.	1	2	3	4	5	6
18	Recognize my real feelings versus idealized feelings in an effort to be more genuine and empathic with LGB clients.	1	2	3	4	5	6
19	Provide a list of LGB-affirmative community resources, support groups, and social networks to a client.	1	2	3	4	5	6
20	Refer an LGB client to affirmative social services in cases of estrangement from their families of origin.	1	2	3	4	5	6
21	Refer LGB clients to LGB-affirmative legal and social supports.	1	2	3	4	5	6
22	Provide a client with city, state, federal, and institutional ordinances and laws concerning civil rights of LGB individuals.	1	2	3	4	5	6
23	Help a same-sex couple access local LGB-affirmative resources and support.	1	2	3	4	5	6
24	Refer an elderly LGB client to LGB-affirmative living accommodations and other social services.	1	2	3	4	5	6
25	Refer an LGB client with religious concerns to an LGB-affirmative clergy member.	1	2	3	4	5	6
26	Integrate clinical data (e.g., mental status exam, intake assessments, presenting concern) of an LGB client.	1	2	3	4	5	6

27	Complete an assessment for a potentially abusive same-sex relationship in an LGB-affirmative manner.	1	2	3	4	5	6
28	Assess for post-traumatic stress felt by LGB victims of hate crimes based on their sexual orientations/identities.	1	2	3	4	5	6
29	Assess the role of alcohol and drugs on LGB clients' social, interpersonal, and intrapersonal functioning.	1	2	3	4	5	6
30	Establish an atmosphere of mutual trust and affirmation when working with LGB clients.	1	2	3	4	5	6
31	Normalize an LGB client's feelings during different points of the coming out process.	1	2	3	4	5	6
32	Establish a safe space for LGB couples to explore parenting.	1	2	3	4	5	6

Additional Items:

Support parents/family members as they come to terms with their LGBTQ+ youth's identity.	1	2	3	4	5	6
Have the same (or higher) level of confidence in working with Transgender youth as I do with working with LGB youth.	1	2	3	4	5	6
Refer a transgender client for appropriate and affirmative medical consultation and care.	1	2	3	4	5	6

What is your own individual growth objective for participating in the SCCMHA SOGI Safe Study Group?

How will you know you have achieved this objective?

What support do you hope to receive from the group leaders and other group members to help you achieve your objective?

Exhibit B

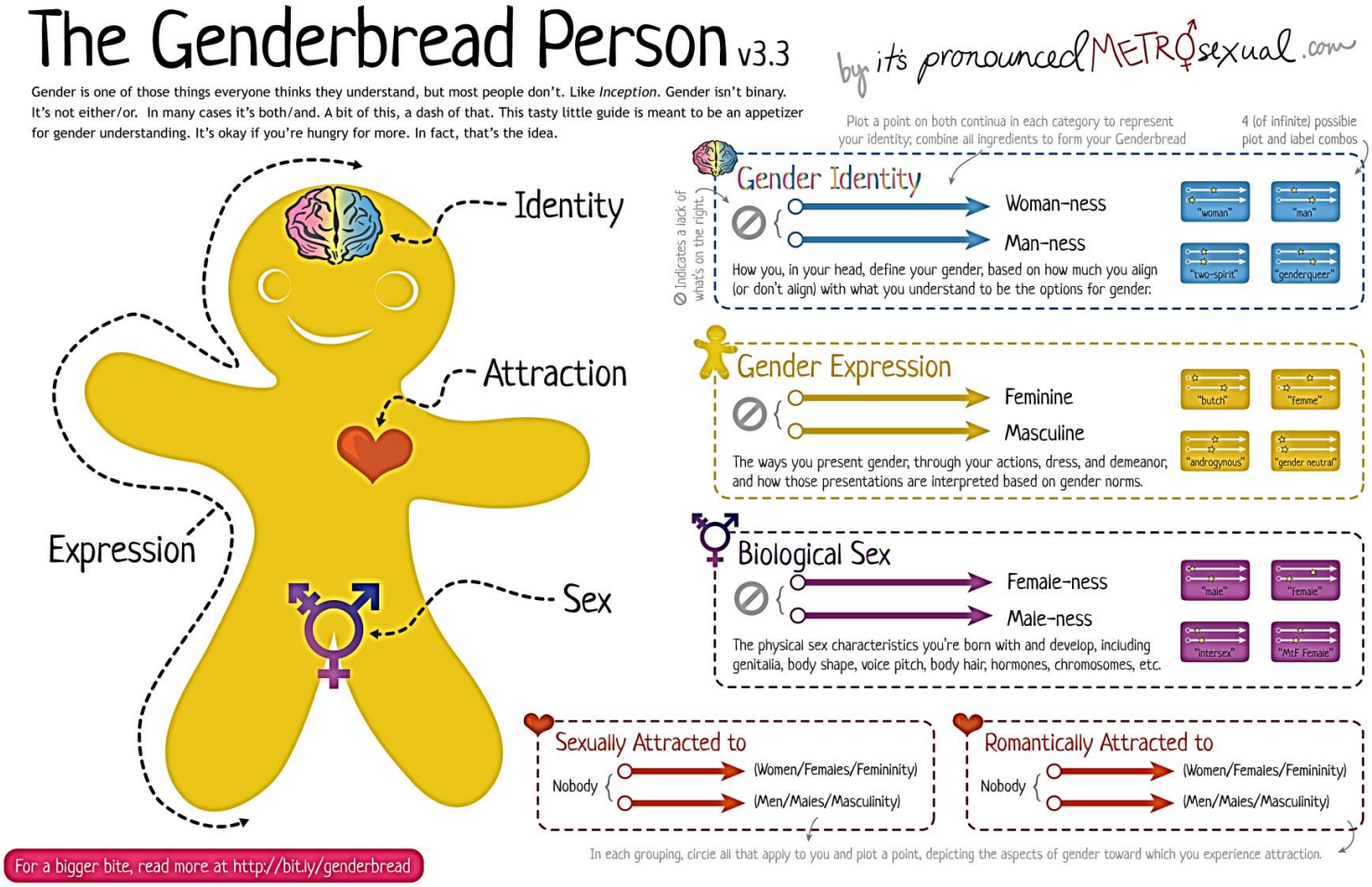

The Genderbread Person v3.3
by it's pronouncedMETROsexual.com
Gender is one of those things everyone thinks they understand, but most people don't. Like *Inception*. Gender isn't binary. It's not either/or. In many cases it's both/and. A bit of this, a dash of that. This tasty little guide is meant to be an appetizer for gender understanding. It's okay if you're hungry for more. In fact, that's the idea.
Plot a point on both continua in each category to represent your identity; combine all ingredients to form your Genderbread
4 (of infinite) possible plot and label combos
Identity
Attraction
Expression
Sex
Gender Identity
Indicates a lack of what's on the right.
Woman-ness
Man-ness
How you, in your head, define your gender, based on how much you align (or don't align) with what you understand to be the options for gender.
"woman"
"man"
"two-spirit"
"genderqueer"
Gender Expression
Feminine
Masculine
The ways you present gender, through your actions, dress, and demeanor, and how those presentations are interpreted based on gender norms.
"butch"
"femme"
"androgynous"
"gender neutral"
Biological Sex
Female-ness
Male-ness
The physical sex characteristics you're born with and develop, including genitalia, body shape, voice pitch, body hair, hormones, chromosomes, etc.
"male"
"female"
"intersex"
"MtF Female"
Sexually Attracted to
Nobody
(Women/Females/Femininity)
(Men/Males/Masculinity)
Romantically Attracted to
Nobody
(Women/Females/Femininity)
(Men/Males/Masculinity)
In each grouping, circle all that apply to you and plot a point, depicting the aspects of gender toward which you experience attraction.
For a bigger bite, read more at http://bit.ly/genderbread

Exhibit C

What Does it Mean to be SOGI Safe?

You can tell that a professional is SOGI Safe if they:

Don't:

- Assume clients are straight and/or cisgender.
- Gender stereotype clients or clients' interests.
- Assume that being LGBTQ+ is caused by trauma.
- Assume that knowing a client's sexual orientation and gender identity isn't relevant to providing treatment.
- Assume that a client's sexual orientation and gender identity is ALWAYS relevant to their treatment.
- Impose judgment on families who are struggling to accept their LGBTQ+ loved one.
- Ignore clients' intersectionality of race, religion, or other cultural backdrops.
- Assume LGBTQ+ clients will volunteer the fact that they're LGBTQ+ if no one asks.

Do:

- Use gender-neutral language, such as "significant other," until told otherwise.
- Demonstrate a working knowledge of the Coming Out process and the decisions each individual faces related to personal congruence and choosing to share or not share information with others.
- Recognize forms of trauma and microaggressions that are unique to LGBTQ+ individuals.
- Understand that when youth are raised in affirming environments, risk of trauma can be mitigated.
- Cite APA guidelines and research on the inefficacy of anti-gay conversion therapy.
- Ask (rather than assume) terms, labels, and experiences.
- Understand that gender identity and sexual orientation labels are personally relevant, and that individuals, especially those who are gender fluid, working through the Coming Out process, or Questioning, may change their labels.
- Offer an authentically safe, non-judgmental space for clients and clients' families.

Perhaps most of all, SOGI Safe professionals will continue to bring their intense awareness and willingness to learn into their work with LGBTQ+ clients, and will actively pursue further professional competency as more knowledge becomes available.

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Services for Members of the Armed Forces, Veterans and their Families</td><td>Chapter: 03 – Continuum of Care</td><td>Subject No: 03.02.31</td></tr>
<tr><td rowspan="2">Effective Date: 5/5/16</td><td>Date of Review/Revision: 9/7/16, 6/13/17, 4/10/18, 4/9/19, 7/29/20, 4/13/21, 5/10/22, 4/11/23, 4/4/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to specify services and supports that may be provided to members of the armed forces, veterans and their families who meet SCCMHA's eligibility criteria.

Policy:

Mental health problems are common among veterans, particularly those who have been exposed to combat. Exposure to combat has been found to be a risk factor for post-traumatic stress disorder (PTSD) and depression. Service members have been identified as an "at risk" population. As such, they face increased risk for substance use disorders; suicide; diminished physical health and increased mortality; diminished employment and productivity; homelessness; and family problems including marital distress, parenting issues and adverse child outcomes.

Adjustment to civilian life following military service includes coping with the loss of the support and regimentation of military life, challenges with reestablishing relationships with family and friends, accessing needed services and benefits and finding, and maintaining gainful employment. Historically, the United States military has not provided adequate transition training and supports for military members and veterans who are returning home. While the military and Department of Veterans Affairs have begun to address the challenges of transitioning military members, the need to provide supports and resources for returning service members continues at the federal, state, and local levels.

In recognition of these challenges and the unmet mental health needs of many veterans, SCCMHA shall provide mental health and substance use disorder treatment services to eligible members of the armed forces, veterans, and their families in accordance with standards set forth by SAMHSA for Certified Community Behavioral Health Clinics

(CCBHCs). Such services shall include: crisis services; screening, assessment and diagnosis; person-centered treatment planning; outpatient behavioral health services; outpatient primary care screening and monitoring; targeted case management; psychiatric rehabilitation; peer and family supports; and intensive community-based outpatient behavioral health care.

Application:
This policy applies to all SCCMHA-funded services for veterans with mental illnesses, substance use disorders and co-occurring disorders.

Standards:
A. SCCMHA-funded providers shall, as resources permit, receive cultural competency training that includes understanding military culture.
B. All persons seeking services shall be screened for military service (or family member's service in case of children).
C. The military status of the person served shall be documented in the clinical record.
D. SCCMHA shall, resources permitting, provide an on-site Veteran and Military Family Program Navigator as a component of the continuum of care for veteran and military members served by SCCMHA.
E. SCCMHA providers shall coordinate care for members of the armed forces and veterans with Department of Veterans Affairs' facilities and providers as appropriate.
F. Persons served currently serving in the military (i.e., active military personnel) shall be offered assistance in accordance with the following standards:
    1. Active-Duty Service Members (ADSMs) must use their servicing Military Treatment Facility (MTF).
        a. SCCMHA providers shall contact the MTF Primary Care Manager (PCM) of the person served regarding referrals outside the MTF[1].
G. SCCMHA shall serve veterans who decline or are ineligible for Veterans Health Administration (VHA) services in accordance with the minimum clinical mental health guidelines promulgated by the VHA and who meet SCCMHA eligibility criteria.
H. Services for persons served/veterans with co-occurring disorders (e.g., substance use and psychiatric disorders or more than one psychiatric disorder) and/or comorbid medical conditions shall be provided in an integrated manner in accordance with SCCMHA policy.
I. Every person served who is a veteran shall be assigned a principal behavioral health provider, typically a case manager or therapist who shall be identified in the record and to the person served.

[1] ADSMs and activated Reserve Component (Guard/Reserve) members who reside more than 50 miles (or one hour's drive time) from a military hospital or military clinic enroll in TRICARE PRIME Remote and use the network PCM or select any other authorized TRICARE provider as the PCM. In addition, PCMs make referrals to specialists for care they cannot provide and work with the VHA's regional managed care support contractor for referrals/authorizations. Members of the Selected Reserves, not on Active Duty (AD) orders, are eligible for TRICARE Reserve Select and can schedule an appointment with any TRICARE-authorized provider, network or non-network. Veterans: Persons affirming former military service (veterans) are offered assistance to enroll in VHA for the delivery of health and behavioral health services.

1. The principal behavioral health provider shall ensure that services are coordinated and contact with maintained with persons served/veterans receiving services from more than one behavioral health provider and who are involved in more than one program.
    a. The principal (or primary) provider shall ensure that a psychiatrist or other qualified independent prescriber reviews and reconciles the psychiatric medications of the veteran/person served on a regular basis.

J. The treatment plan of the veteran/person served shall incorporate input from the person served/veteran and, when appropriate, the family with the consent of the veteran/person served when the person served/veteran has adequate decision-making capacity or with their surrogate decision-maker's (e.g., legal guardian's) consent when the person served/veteran lacks such capacity.
    1. Implementation of the treatment plan, including progress and care delivered, outcomes achieved, and goals attained shall be monitored and documented in the clinical record.
    2. The treatment plan shall be periodically reviewed with the person served/veteran and revised when indicated.

K. The primary therapist or behavioral health provider shall communicate with the person served/veteran (and their natural support system when appropriate and with the consent of the person served/veteran) about the treatment plan and any problems or concerns expressed by the person served/veteran regarding their care.

L. All veterans/persons served shall be offered crisis planning services and the opportunity to designate a surrogate decision-maker in the event of incapacity.
    1. Persons served/veterans shall be offered the opportunity to prepare Advance Directives in accordance with SCCMHA policy and VHA Handbook 1004.1.

M. The treatment plan shall be person-centered and reflect the goals and preferences for care of the person served/veteran.

N. The person served/veteran shall verbally consent to their treatment plan and sign it in accordance with SCCMHA policy and VHA Handbook 1004.1.
    1. Persons served/veterans whose capacity for decision-making is of concern shall be referred for a formal assessment and the results of that evaluation shall be documented in the record.
        a. An authorized surrogate decision-maker shall be identified for a veteran/person served who is deemed to lack such capacity and the authorized surrogate's consent to treatment on behalf of the person served/veteran is documented per VHA Handbook 1004.1.

O. Veterans shall be offered evidence-based practices that are available to persons served by SCCMHA with psychiatric and substance use disorders (e.g., Seeking Safety, Motivational Interviewing, Family Psychoeducation, Supported Employment, smoking cessation, CBT for relapse prevention, CBT for depression and

anxiety disorders, and pharmacotherapies[2] including Medication Assisted Treatment [MAT], etc.).

1. SCCMHA shall make every effort to refer veterans in need of specialized approaches (e.g., gender-specific treatment for MST/Military Sexual Trauma) to providers with relevant training and expertise.

P. Services and supports for veterans shall be recovery-oriented, person-centered, trauma-informed evidence-based and provided in a manner consistent with relevant SCCMHA policies and the VHA Handbook 1160.01.

Q. SCCMHA shall establish and maintain a Memorandum of Understanding (MOU) with the Aleda A. Lutz VA Medical Center.

R. SCCMHA shall work with assigned liaison(s) from the local VA to coordinate services for veterans including participating in community events designated for veterans and their families (e.g., Stand Downs for veterans who are homeless and Community Homeless Assessment Local Education and Networking Groups [CHALENG] meetings).

Definitions:

Mental Health Treatment Coordinator (MHTC): A veteran's primary contact for all specialty mental health services. MHTCs coordinate mental health treatment plans for veterans.

TRICARE: The Department of Defense's (DoD) health care benefits program which serves all of members of the uniformed services and their families.

Veteran: Any person who served for any length of time in any **military service branch**.

References:

A. Substance Abuse and Mental Health Services Administration. (Undated). Criteria for the Demonstration Program to Improve Community Mental Health Centers and to Establish Certified Community Behavioral Health Clinics: http://www.samhsa.gov/sites/default/files/programs_campaigns/ccbhc-criteria.pdf

B. Substance Abuse and Mental Health Services Administration. (2012). Behavioral Health Issues Among Afghanistan and Iraq U.S. War Veterans. *In Brief*, Volume 7, Issue 1: https://store.samhsa.gov/sites/default/files/d7/priv/sma12-4670.pdf

C. SCCMHA Policy 03.02.14 – Advance Directives

D. SCCMHA Policy 02.01.01.02 – Cultural Competence

E. SCCMHA Policy 10.01.02 – Health Home Services

F. SCCMHA Policy 02.03.03 – Person-Centered Planning

G. SCCMHA Policy 02.03.05 – Recovery

H. SCCMHA Policy 02.03.09.01 – Dual Diagnosis Treatment Capacity

I. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports

J. SCCMHA Policy 02.03.08 – Welcoming

K. Department of Veterans Affairs. (August 14, 2009, Amended September 17, 2021). *1nformed Consent for Clinical Treatments and Procedures. VHA Handbook 1004*

[2] Veterans diagnosed with schizophrenia or schizoaffective disorders with severe residual suffering, symptoms, or impairments must be offered clozapine following two unsuccessful trials of other antipsychotic medications.

L. Department of Veterans Affairs. (September 11, 2008, revised November 16, 2015). *Uniform Mental Health Services in VA Medical Centers And Clinics. VHA Handbook 1160.01*

Exhibits:
None

Procedure:
None

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Services for American Indians</td><td>Chapter: 03 – Continuum of Care</td><td>Subject No: 03.02.34</td></tr>
<tr><td rowspan="2">Effective Date:
5/5/16</td><td>Date of Review/Revision:
6/13/17, 4/10/18, 4/9/19, 7/29/20, 5/10/22, 4/11/23, 4/5/24, 4/8/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Executive Director of Clinical Services

Authored By:
Barbara Glassheim

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to ensure the provision of and/or coordination of services to American Indians is person/family-centered, trauma-informed, recovery-oriented, developmentally and phase-of-life appropriate, culturally and linguistically sensitive and promotes engagement and shared decision-making with the person served using evidence-based practices and treatments to maximize the potential for beneficial outcomes.

Policy:
SCCMHA shall provide holistic, person/family-centered, trauma-informed, developmentally and phase of life appropriate care which recognizes the particular cultural and linguistic needs of the person served and addresses health disparities.

Services for American Indians may be provided either directly or via agreement with tribal providers. In some instances, services may be provided conjointly by SCCMHA and tribal providers.

Application:
This policy applies to the delivery of all services and supports funded by SCCMHA for persons with a mental illness, substance use disorder, intellectual/developmental disability as well as children and youth with a serious emotional disturbance.

Standards:
A. SCCMHA shall address the five nationally accepted core elements of cultural competence in serving members of any distinct cultural group, including American Indians:
   1. Awareness, acceptance and valuing of cultural differences
   2. Awareness of one's own culture and values
   3. Understanding the range of dynamics that result from the interaction between people of different cultures

4. Developing cultural knowledge of the particular community served or to access cultural brokers who may have that knowledge
5. Ability to adapt individual interventions, programs, and policies to fit the cultural context of the individual, family, or community

B. SCCMHA shall, resources permitting, offer cultural competency training to providers in order to help them understand and appreciate American Indian culture.

C. SCCMHA shall offer choice of providers to eligible members of the Saginaw Chippewa Indian Tribe residing in Saginaw County who request mental health services.
   1. SCCMHA shall serve American Indians who request and meet criteria for services.
      a. SCCMHA shall engage and coordinate care with the Saginaw Chippewa Indian Tribe Behavioral Health Program when serving members of the tribe.

D. SCCMHA shall work with the Saginaw Chippewa Indian Tribe Behavioral Health Program to assist in the provision of services to tribal members who are served by SCCMHA and to help inform the provision of culturally appropriate services to those persons including traditional approaches to care.
   a. Every effort shall be made to ensure services and supports are compatible with the Tribe's traditional healing practices and commitment to restoring the balance of the mind, body, and spirit and address mental health issues specific to Tribes including, but not limited to, historical trauma, relocation, grief and loss, foster placement, physical, sexual, emotional, spiritual abuse, reactive attachment disorder, and trauma.

E. SCCMHA shall develop and implement an agreement to coordinate care and/or fund services on an out-of-network basis for persons deemed eligible for SCCMHA services who are tribal members and seek services at the Saginaw Chippewa Indian Tribe Behavioral Health Program.
   1. SCCMHA shall authorize medically necessary services provided to eligible Medicaid and Healthy Michigan Plan beneficiaries who are eligible to receive services from the Saginaw Chippewa Indian Tribe Behavioral Health Program in accordance with established medical necessity criteria.
   2. SCCMHA shall provide crisis screening and intervention, including authorization for inpatient psychiatric hospitalization services, for tribal members when needed.
   3. SCCMHA case holders shall coordinate care for persons who are serviced by both SCCMHA and the Saginaw Chippewa Indian Tribe Behavioral Health Program.
   4. Reimbursement rates to the Chippewa Indian Tribe Behavioral Health Program shall be in alignment with SCCMHA network rates for like services.

Definitions:

Culture: The beliefs, customs, social norms, and material traits of a racial, religious, or social group. It affects the group members' viewpoints: how they act; how they think; and how they see themselves in relation to the rest of the world. Culture is also defined as a particular society that has its own beliefs, ways of life, art, etc. or a way of thinking, behaving, or working that exists in a place or organization (such as a business).

Culture is transmitted through language, symbols, and rituals. Cultural differences can be manifested in help-seeking behaviors, language and communication styles, symptom patterns and expressions, nontraditional healing practices, and the role and desirability of an intervention or treatment.

Cultural Customs: A particular group or individual's preferred way of meeting their basic human needs and conducting daily activities as passed on through generations. Customs are influenced by: ethnicity, origin, language, religious/spiritual beliefs, socioeconomic status, gender, sexual orientation, age, marital status, ancestry, history, gender identity, geography, etc. American Indian cultural customs are expressed via material culture such as food, dress, dance, ceremony, drumming, song, stories, symbols, and other visible manifestations.

Cultural Competence: Recognition of the importance of the cultures, skills, knowledge, and policies needed to deliver effective treatments. Cultural competence is demonstrated through respecting and valuing differences among persons served, assuming responsibility to address these differences, and an appraising the effectiveness of an organization's ability to address cultural differences.

Cultural Identity: The character or feeling of belonging to a group that is part of a person's self-conception and self-perception and is related to nationality, ethnicity, religion, social class, generation, locality or any kind of social group that has its own distinct culture. An individual's own personal and family history determines their cultural identity and practices, which may change throughout the lifespan as they are exposed to different experiences.

Diversity: Differences in geographic location (rural, urban), sexual orientation, age, religion or spiritual practice, socioeconomic status, and physical and mental capacity.

Ethnicity: A population or group having a common cultural heritage that is distinguished by customs, characteristics, language, and common history.

References:

A. Cross, T., Bazron, B., Dennis, K., and Isaacs, M. (1989). *Towards A Culturally Competent System of Care Volume I.* Georgetown University Child Development Center, CASSP Technical Assistance Center. Washington, D.C. [On-line]. Available: https://spu.edu/~/media/academics/school-of-education/Cultural%20Diversity/Towards%20a%20Culturally%20Competent%20System%20of%20Care%20Abridged.ashx

B. National Association of State Mental Health Program Directors (NASMHPD). (2004). *Cultural Diversity Series: Meeting the Mental Health Needs of American Indians and Alaska Natives.* National Association of State Mental Health Program Directors. Alexandra, VA. NTAC. [On-line]. Available: http://www.azdhs.gov/bhs/pdf/culturalComp/ccna.pdf.

C. Saginaw Chippewa Indian Tribe Behavioral Health Programs: http://www.sagchip.org/behavioralhealth/#.VzXvivkrKpA.

D. SCCMHA Policy 02.01.01.02 – Cultural Competence

E. SCCMHA Policy 02.03.05 – Recovery

F. SCCMHA Policy 02.03.08 – Welcoming

G. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports

H. SCCMHA Policy 03.02.46 – Whole-Person Care

I. Substance Abuse and Mental Health Services Administration (SAMHSA). (September 2010). *American Indian and Alaska Native Culture Card: A Guide to Build Cultural Awareness.* SAMHSA. Rockville, MD. [On-line]. Available: https://store.samhsa.gov/sites/default/files/d7/priv/sma08-4354.pdf.

Exhibits:
None

Procedure:
None

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Serving LGBTQIA+ Persons	**Chapter**: 03 – Continuum of Care	**Subject No**: 03.02.35
Effective Date: 5/5/16	**Date of Review/Revision**: 6/13/17, 4/10/18, 4/9/19, 8/21/20, 4/8/21, 5/10/22, 4/11/23, 4/5/24, 4/8/25	**Approved By**: Sandra M. Lindsey, CEO
	Supersedes:	**Responsible Director:** Executive Director of Clinical Services
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Authored By:** Barbara Glassheim, Heidi Wale Knizacky
		Additional Reviewers:

Purpose:

The purpose of this policy is to provide basic information regarding LGBTQIA+ culture and terminology as well as to ensure that persons with a mental illness, substance use disorder, serious emotional disturbance, and/or intellectual/development disability who are lesbian, gay, bisexual, transgender, questioning, intersex, pansexual, two-spirit, and other types of sexual orientation or gender identity minority (LGBTQIA+) are provided with high quality, person/family-centered, trauma-informed, culturally and linguistically sensitive, developmentally appropriate, recovery oriented services and supports in a manner that promotes shared decision-making and employs evidence-based practices.

Policy:

SCCMHA recognizes that health disparities among LGBTQIA+ individuals, including higher rates of sexually transmitted infections (STIs), HIV, depression, anxiety, suicidality, tobacco use, and substance use disorders, result from bias present at individual, interpersonal, social, and structural levels. SCCMHA also recognizes that it is especially important to build rapport as a way to counteract the exclusion, discrimination, and stigma that many LGBTQIA+ people have historically experienced in health care settings. SCCMHA further recognizes that providers need to be aware of their own implicit biases that may affect the way they interact with LGBTQIA+ people they serve.

SCCMHA shall provide gender/identity affirming, person/family-centered, trauma-informed, developmentally and phase of life appropriate, recovery-oriented, and culturally and linguistically sensitive services to persons served who identify as LGBTQIA+ in a manner that promotes the engagement of the person served and shared decision-making in accordance with the purpose of this policy as explicated above.

Application:

This policy applies to all SCCMHA-funded services and supports provided to persons with a mental illness, substance use disorder, intellectual/developmental disability and children with a serious emotional disturbances.

Standards:

A. SCCMHA values diversity and inclusiveness including, but not limited, to race, ethnicity, age, religion, gender, sexual orientation, and disability, among others, and shall provide services and supports in a manner that is sensitive to the concerns of all persons served including those who are LGBTQIA+.
   1. SCCMHA shall create a safe and welcoming atmosphere safe for LGBTQIA+ people.
   2. SCCMHA-funded providers shall display the appropriate cultural awareness, knowledge and skill to create a welcoming environment for persons served of every sexual orientation, gender identity and gender expression.

B. SCCMHA shall use inclusive language in policies and practice including:
   1. Using gender-neutral terms such as partner, spouse, loved one, child, and caregiver to avoid heteronormative and gender binary language, which can be discriminatory.
   2. Avoiding the use of words such as lifestyle, sex-change, and homosexual, as these may be offensive and inappropriate.
   3. Asking individuals to identify their own pronouns, preferred name, and preferred identity terms and adhering to these terms when talking to and about the individual and adding documentation to their medical record.

C. SCCMHA shall provide culturally competent, trauma-informed, integrated treatment and recovery support services that are grounded in a strengths-based, shared decision-making approach to LGBTQIA+ people.

D. SCCMHA shall deliver services and supports that are LGBTQIA+-welcoming and respectful by:
   1. Not assuming anyone is straight or cisgender.
   2. Not assuming an individual will disclose their sexual orientation or gender identity if not asked.
   3. Not viewing an individual's sexual orientation or gender identity as a behavioral target or symptom in need of treatment intervention.
   4. Avoiding influencing or implying a pre-determined outcome when working with individuals who are questioning their sexual orientation or gender identity.
   5. Recognizing that, while being LGBTQIA+ does not imply need for treatment, individuals who are LGBTQIA+ are at increased risk for experiences of trauma and minority stress and a thorough assessment should be completed to identify all needs.
   6. Recognizing and supporting the function of self-actualizing behaviors of LGBTQIA+ individuals and avoiding labels and diagnoses – such as Oppositional Defiant Disorder – that place the burden of change on the individual when the conflict is, in fact, due to inappropriate family or societal response.

E. LGBTQIA+-affirmative values shall be reflected in employee training, supervision, and evaluation.

F. SCCMHA shall include topics regarding LGBTQIA+ cultures and communities during cultural awareness and competency trainings.
   1. SCCMHA shall provide staff education regarding the LGBTQIA+ population.
   2. Training will encourage culturally affirmative environments of care for LGBTQIA+ persons served and family members.

G. SCCMHA shall promote LGBTQIA+ tolerance in the community and speak out against discrimination and intolerance.
   1. SCCMHA shall forge relationships with LGBTQIA+ groups and resources by attending their events, meeting to discuss common interests, supporting their efforts, and sharing resources.
   2. SCCMHA shall endeavor to help address stigma and microaggressions, including those associated with LGBTQIA+ people, and to foster a deeper sense of heritage and community.

H. SCCMHA recognizes the dangers of conversion or "reparative" therapy for LGBTQIA+ people and does not provide or support it; SCCMHA supports only those therapies that affirm the identities of LGBTQIA+ people and respect their right to self-determination.

I. SCCMHA policies, regulations, training materials and contracts shall reflect protection from discrimination based on sexual orientation, gender identity and gender expression.

J. Persons served, families, providers and staff shall be encouraged to report violations of SCCMHA's policies of non-discrimination and anti-conversion therapy.

K. SCCMHA shall ensure that all practices consider LGBTQIA+ needs.
   1. SCCMHA shall ensure that all family services are available for domestic partners and significant others of LGBTQIA+ persons served.

L. SCCMHA providers shall avoid inadvertently outing LGBTQIA+ persons served to others, including to the families of youth being served.

Definitions:

Note: *Discussion of topics that have a history of oppression (such as LGBTQIA+ experiences) creates localized and covert communication. As conversations become increasingly open and inclusive, more accurate terms are identified and disseminated. Checking updated sources and – especially – asking preferences of individuals whose language will be used with and about is advised.*

Agender: A person who does not identify with a specific gender or who does not experience gender as a primary identity component.

Ally: A person who identifies as heterosexual and cisgender but is connected to or a part of the LGBTQIA+ community and is an advocate of rights for LGBTQIA+ people.

Androgyne/Androgynous: A person who presents themselves in a gender-neutral manner or who combines outward characteristics that are typically thought of as masculine or feminine. Androgynous people may identify as male, female, a third gender, or no gender.

Aromantic: A person who experiences little or no romantic attraction to others, and/or lacks interest in forming romantic relationships. Aromantic people may still have intimate relationships.

Asexual: An individual who does not identify with any sexual orientation because they do not experience sexual attraction; a person who experiences little or no sexual attraction to others. Asexual people may still engage in sexual activity.
Assigned Female at Birth/Assigned Male at Birth: The sex that is assigned to an infant, most often based on the infant's anatomical and other biological characteristics. Commonly abbreviated as AFAB (assigned female at birth) or AMAB (assigned male at birth).
Bigender: A person who has two genders; exhibiting cultural and/or physical characteristics of male and female roles.
Binding: The process of tightly wrapping one's chest in order to minimize the appearance of having breasts. This is achieved through use of constrictive materials such as cloth strips, bandages, or specially designed undergarments, called binders.
Biphobia: Discrimination towards, fear, marginalization, and hatred of bisexual people, or those who are perceived as bisexual. Individuals, communities, policies, and institutions can be biphobic.
Bisexual: An individual who is attracted to people of both genders or either gender. This term may be used to describe self-identity, behavior, or both. It may be used to describe a person's past, present, or potential range of romantic and/or sexual attraction. Bisexual people may be monogamous, non-monogamous, or celibate, and may never have had sexual relations with men, with women, or with anyone at all.

Some bisexually identified people indicate that gender is irrelevant to their attraction or choice of romantic partners while others indicate that gender is quite salient, and they are attracted to men and to women for different reasons or at different times. (Bisexual does not mean that the person is necessarily involved with both men and women at the same time.)
Bisexuality: The capacity to be romantically and/or sexually attracted to individuals of more than one sex.
Bottom: A slang term for genitals and buttocks. Also used to refer to the receptive partner in anal sex.
Bottom Surgery: Slang term for gender-affirming genital surgery.
Chosen Name/Name Used: The name a person goes by and wants others to use in personal communication, even if it is different from the name on that person's insurance or identification documents (e.g., birth certificate, driver's license, and passport). Use of the term 'chosen name' is recommended over 'preferred name.' The terms Chosen Name or Name used can be put on patient health care forms alongside Name on one's insurance (if different) and Name on your legal identification documents (if different). In conversation with patients, health care staff can ask, "What name do you want us to use when speaking with you?", or "What is your chosen name?"
Cisgender: An individual who identifies with the gender assigned to them at birth; someone who is not transgender. The term cisgender comes from the Latin prefix cis, meaning "on the same side of."
Closeted (or "being in the closet"): Lack of disclosure – or actively hiding or disguising – one's sexual orientation or gender identity. Like "coming out," it may be situational and/or change over time; a given person may be "closeted" at work, but quite "out" socially.
Coming Out (or "coming out of the closet" or being "out"): The individual process by which a person recognizes, accepts, and shares with others one's sexual and/or gender

identity. This is a non-linear process; an individual may be "out" in some situations or to certain people but not to others. The process of coming out to oneself and to others is unique for every individual.

Conversion Therapy or Reparative Therapy: Clinical treatment with the purpose of changing a person's sexual orientation. This type of treatment assumes that any sexual or affectional preferences other than heterosexual are pathological.

Cross Dresser: A person of any gender and any sexual orientation who wears clothing that is not usually associated with his/her socially assigned gender roles.

Culture: The beliefs, customs, social norms, and material traits of a racial, religious, or social group. Culture affects the group members' viewpoints: how they act; how they think; and how they see themselves in relation to the rest of the world. Culture is also defined as a particular society that has its own beliefs, ways of life, art, etc. or a way of thinking, behaving, or working that exists in a place or organization (such as a business). Culture is transmitted through language, symbols, and rituals. Cultural differences can be manifested in help-seeking behaviors, language and communication styles, symptom patterns and expressions, nontraditional healing practices, and the role and desirability of an intervention or treatment.

Drag: The theatrical performance of a gender or multiple genders that are not your own. Performers are called Drag Kings and Drag Queens. Most drag performers are cisgender. The terms Drag King and Drag Queen can also be used as an insult.

Ethnicity: A population or group having a common cultural heritage that is distinguished by customs, characteristics, language, and common history.

Diversity: Differences in geographic location (rural, urban), sexual orientation, age, religion or spiritual practice, socioeconomic status, and physical and mental capacity.

Enby/N.B.: Non-binary. Refers to individuals and social systems that do not limit their experience and understanding of gender as being restricted to only male and/or female.

F to M: A female to male transgender or transsexual person (i.e., a person who transitioned or is transitioning from living as a girl/woman to living as a man).

Family of Choice: Supportive friendship networks that function as family, often due to rejection or lack of disclosure to the biological family. Persons an individual sees as significant in their life. It may include none, all, or some members of their family of origin as well as include individuals such as significant others or partners, friends, coworkers, etc.

Family of Origin: Birth or biological family or any family system instrumental or significant in an individual's early development.

Gay: A person who is attracted to people of the same gender. It is primarily used in reference to men (gay men) but may also be used as an inclusive term to encompass both men and women. Gay may also be used as an adjective to denote same-sex sexual orientation. Someone who identifies as gay may have sexual relations with someone of the same sex, the opposite sex, or may not have sexual relations.

Gender: A person's biological, personal, social and/or legal status as male or female. However, the term "sex" may be defined as the biological, and "gender" as the personal, social, or legal. Thus, a person could have male (biological) sex but live full time as and think of herself as a woman.

Gender Affirmation: The process of making social, legal, and/or medical changes to recognize, accept, and express one's gender identity. Social changes can include changing one's pronouns, name, clothing, and hairstyle. Legal changes can include changing one's

name, sex designation, and gender markers on legal documents. Medical changes can include receiving gender-affirming hormones and/or surgeries. Although this process is sometimes referred to as transition, the term gender affirmation is recommended.

Gender-Affirming Chest Surgery: Surgeries to remove and/or construct a person's chest to be more aligned with that person's gender identity. Also referred to as top surgery. Types of chest surgeries include feminizing breast surgery (breast augmentation, chest construction, or breast mammoplasty) and masculinizing chest surgery (mastectomy and chest contouring).

Gender-Affirming Genital Surgeries: Surgeries that help align a person's genitals and/or internal reproductive organs with that person's gender identity, including: clitoroplasty (creation of a clitoris); hysterectomy (removal of the uterus; may also include removal of the cervix, ovaries, and fallopian tubes); labiaplasty (creation of inner and outer labia); metoidioplasty (creation of a masculine phallus using testosterone-enlarged clitoral tissue); oophorectomy (removal of ovaries); orchiectomy (removal of testicles); penectomy (removal of the penis); phalloplasty (creation of a masculine phallus); scrotoplasty (creation of a scrotum and often paired with testicular implants); urethral lengthening (to allow voiding while standing); vaginectomy (removal of the vagina); vaginoplasty (creation of a neovagina); and vulvoplasty (creation of a vulva).

Gender-Affirming Hormone Therapy: Feminizing and masculinizing hormone treatment to align secondary sex characteristics with gender identity.

Gender-Affirming Surgery (GAS): Surgeries to modify a person's body to be more aligned with that person's gender identity. Types of GAS include chest and genital surgeries, facial feminization, body sculpting, and hair removal.

Gender Binary: The assertion that there are only two genders, male and female, and that a person can only be either exclusively male or female.

Gender Diverse: The community of people who fall outside of the gender binary structure (e.g., non-binary, genderqueer, gender fluid people).

Gender Dysphoria: Distress experienced by some people whose gender identity does not correspond with their sex assigned at birth.

Gender Expression: Characteristics in appearance, personality, and behavior, culturally defined as masculine or feminine – i.e., the manner in which an individual outwardly expresses their gender identity.

Gender Fluid (or Genderfluid): An individual who does not identify as having a fixed gender. A person who is gender fluid may always feel like a mix of more than one gender but may feel more aligned with a certain gender some of the time, another gender at other times, both genders sometimes, and sometimes no gender at all.

Gender Identity: An individual's inner sense of self as male, female, somewhere in between, or something else altogether. Most people develop a gender identity that corresponds to their biological sex, but some do not. Gender identity may or may not be consistent with biological, social or legal gender. For example, a person may be born with a penis – and therefore assigned as male at birth – but have a female gender identity.

Genderism: The belief that there are, and should be, only two genders, and that one's gender, or most aspects of it, are inevitably tied to one's sex assigned at birth.

Gender Neutral: Facilities that any individual can use regardless of gender (e.g., gender-neutral bathrooms); can also be used as a synonym for androgynous, or someone who does not identify with a particular gender.

Gender Non-Conforming (GNC): A person who does not subscribe to gender expression or roles imposed by society.
Genderqueer or Gender Queer : A person who identifies as living outside the traditional gender construct of male body and gender, and female body and gender; someone who resists male or female labels.
Gender Roles: Female or male roles created by society and culture that often proscribe narrow sets of behavior for both men and women (and disregard transgender people).
Gender Variant: Individuals who self-identify as not conforming to the conventions of male and female behavior (e.g., those who are transgender).
Heterocentric or Heterosexist: The presumption that everyone is heterosexual, or that heterosexuality is better or more normal than other orientations.
Heteronormative/ Heteronormativity: The general practice in our culture of assuming that heterosexuality and traditional gender identities are the norm. Also refers to societal pressure for everyone to look and act in a stereotypically heterosexual way. Heteronormativity can manifest as heterosexism, the biased belief that heterosexuality is superior to all other sexualities.
Heterosexism: The value and belief attitude that heterosexuality is the only valid or acceptable or natural sexual orientation and that it is inherently healthier or superior to other types of sexuality. Heterosexism can affect LGBTQIA+ people by causing internalized homophobia, shame, and a negative self-concept.
Heterosexual ("Straight"): A person who is attracted to people of the other binary gender – i.e., a woman who identifies as being attracted to men, or a man who identifies as being attracted to women. Some heterosexual people are attracted to people of the same sex but have sexual relations only with the opposite sex. Others who consider themselves heterosexual may have sexual relations with men and women, and still others may not have sexual relations.
Heterosexual Privilege: A term describing the benefits derived automatically from being heterosexual or perceived as heterosexual, which are denied to people of other sexual orientations.
Homophobia: The fear or hatred of LGBTQIA+ people or what they do and often used as a justification for discrimination. Homophobia in the hands of the dominant or more powerful in society results in heterosexism**.** Individuals, communities, policies, and institutions can be homophobic.
Homosexual: A historical term for a person who is attracted to people of the same gender. Some homosexual people are attracted to people of the opposite sex but have sexual relations only with the same sex. Others who consider themselves homosexual may have sex with men and women, and still others may not have sexual relations. (This term may be considered outdated and negative due to its historical use as a clinical term when being gay or lesbian was considered de facto a mental illness.)
Internalized Homophobia: The experience of shame, aversion or self-hatred internalized by LGBTQIA+ people in reaction to society's homophobia and discrimination due to their acceptance and belief of the negative messages of the dominant group regarding LGBTQIA+ people.
Intersex: refers to people born with sex chromosomes, external genitalia, and/or internal reproductive systems that are not typical for either male or female, but instead are mixed, blended, or indeterminate. Intersex people may be of any sexual orientation and any gender

identity. (The historical term "hermaphrodite" is now considered offensive by many because of the inaccurate implication that the person can self-reproduce.) Intersex conditions are caused by any number of prenatal genetic or hormonal anomalies, including those listed below. Individuals with these conditions are sometimes at higher risk for other medical conditions, for example, osteoporosis.

Adrenal Hyperplasia is the most prevalent cause of intersexuality among chromosomally XX people with a frequency of about 1 in 20,000 births and is caused by an anomaly of adrenal function causing the synthesis and excretion an androgen precursor, initiating virilization (development of male secondary sex characteristics) of a XX person in-utero. Because the virilization originates metabolically, masculinizing effects continue after birth.

Androgen Insensitivity Syndrome (AIS) is a genetic condition occurring in approximately 1 in 20,000 individuals. In an individual with complete AIS, the body's cells are unable to respond to androgen. Some individuals have partial androgen insensitivity. Partial androgen insensitivity typically results in ambiguous genitalia.

Progestin-Induced Virilization is caused by prenatal exposure to outside androgens, most commonly Progestin, a drug that was administered to prevent miscarriage in the 50's and 60's. It is converted to an androgen (a virilizing hormone which causes the development of male secondary sex characteristics) by the prenatal XX person's metabolism.

Klinefelter Syndrome (KS) is the set of symptoms that result from two or more X chromosomes in males rather than the typical inheritance of a single X chromosome from the mother and a single Y chromosome from the mother. Men with KS, which is also known as 47, XXY or XX, inherit an extra X chromosome from either father or mother; their karyotype is 47 XXY. KS is quite common, occurring in 1/500 to 1/1,000 male births.

Intersectionality: The idea that comprehensive identities are influenced and shaped by the interconnection of race, class, ethnicity, sexuality/sexual orientation, gender/gender identity, physical disability, national origin, religion, age, and other social or physical attributes.

"In The Closet": A lesbian, gay, bisexual, transgender or intersex person who chooses not to disclose sex, sexual orientation or gender identity to friends, family, co-workers or society. There are varying degrees of being "in the closet." For example, a person can be "out" in their social life, but "in the closet" at work or with family. Also known as **on the "Down-Low"** or **"D/L."**

Lesbian: A woman who identifies primarily as being attracted relationally and sexually to other women.

LGBT: An abbreviation for Lesbian, Gay, Bisexual, and Transgender. Used as an inclusive shorthand to refer to all of the currently identified sexual minorities. It is common to also see GLBT, LesBiGay, LGBTQ, LGBTQ+, GLBTI, GLBTQI, or LGBTA. The "Q" is added to include individuals who are *questioning* their sexual orientation/identity, the "I" is added to include *intersex* people, and the "A" is used by some to include *allies* and in other uses refers to *asexual*. In recent years, usage of this acronym has evolved in widening circles to *LGBTQ+2-S,* where *Q* represents *queer* or *questioning*; *I* represents *intersex*; and *2-S* refers to the Native American term that means *two-spirit*.

LGBTQ+: A widely-accepted identifier which explicitly and affirmatively includes people who identify as lesbian, gay, bisexual, transgender, questioning and intersex, and is intended to communicate inclusiveness as well as within-group differences.
LGBTQIA+: An acronym for lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and other sexual and gender minorities.
LGBTQIA2S+: An acronym that stands for Lesbian, Gay, Bisexual, Transgender, Questioning, Intersex, Asexual and Two-Spirit.
M to F: A "male to female" transgender or transsexual person. That is, someone who transitioned or is transitioning from living as a boy/man to living as a girl/woman.
Men Who Have Sex with Men/Women Who Have Sex with Women (MSM/WSW): Categories used in public health research and programs to describe people who engage in same-sex sexual behavior, regardless of how they identify their sexual orientation. People rarely use the terms MSM or WSW to describe themselves.
Minority Stress: The chronic stress experienced by LGBTQIA+ individuals related to stigmatization, marginalization, and lack of institutional and social supports within a predominantly heterosexual society. The negative effects of homophobia, transphobia, discrimination and violence on LGBTQIA+ people results in negative mental health outcomes. Minority stress is caused by external, objective events and conditions, expectations of such events, the internalization of societal attitudes, and/or concealment of one's sexual orientation or gender identity. Minority stress is compounded when a person holds multiple marginalized identities.
Misgender: To refer to a person by a pronoun or other gendered term (e.g., Ms./Mr.) that incorrectly indicates that person's gender identity.
Non-Binary: A person whose gender identity falls outside of the traditional gender binary structure of girl/woman and boy/man. Sometimes abbreviated as NB or *enby*.
Open Relationship: A relationship between two partners who consensually agree to non-monogamy (i.e., intimacy outside the primary partnership).
Outing: Involuntary or unwanted disclosure of another person's sexual orientation or gender identity.
Pangender: A person whose gender identity is comprised of many genders or falls outside the traditional cultural parameters that define gender.
Pansexual: A person who does not consider the gender label of others as a criterion for determining sexual or romantic attraction; a person who is emotionally and physically attracted to people of all gender identities, or whose attractions are not related to other people's gender.
Polyamorous: A sexual and/or romantic relationship comprising three or more people; a person in a polyamorous relationship. Sometimes abbreviated as *poly*.
Pronouns: The words people should use when they are referring to a person but not using their name. Examples of pronouns are she/her/hers, he/him/his, and they/them/theirs. The appropriate phrasing is "What are your pronouns?" when seeking this information.
QPOC: An acronym that stands for Queer Person of Color or Queer People of Color.
Queer: An umbrella term used by some LGBTQIA+ people to refer to themselves and to reflect an ongoing attitude of non-restriction toward sexual orientation, gender identity and/or one's gender expression. This is sometimes a preferred label for people who feel that other sexuality/gender labels are not appropriate. Although the term is used by some

heterosexist individuals as a derogatory term for LGBTQIA+ individuals, some members of the LGBTQIA+ community use it positively to refer to themselves or their community.
Questioning: A person who is unsure about their sexual orientation and/or gender identity, or who chooses at a given time to hold off in defining their sexual orientation and/or gender identity.
Recovery: A process of change through which individuals improve their health and wellness, live a self-directed life, and strive to reach their full potential.
Same-Gender Loving (SGL): A term most often used in communities of color to describe people with same sex attractions in order to avoid the negative connotations of the terms gay, homosexual, bisexual or lesbian.
Same-Sex Attraction/Attracted (SSA): The experience of a person who is emotionally and/or physically attracted to people of the same sex or gender but does not necessarily engage in same-sex sexual behavior. This term is used most commonly by people who live in religious communities that are not accepting of LGBTQIA+ identities. People who use SSA as an identity term may not feel comfortable with the terms gay, lesbian, queer, or bisexual.
Sex: A biological construct that is based primarily on physical attributes such as chromosomes, external and internal genital and reproductive anatomy and hormones.
Sex Assigned at Birth: The sex (male or female) assigned to an infant, most often based on the infant's anatomical and other biological characteristics. Sometimes referred to as birth sex, natal sex, biological sex, or sex; however, sex assigned at birth is the recommended term.
Sexual Behavior: Physical sexual activities a person engages in (which can be different from their sexual orientation).
Sexual Minorities: An encompassing term which includes lesbian, gay, bisexual, and pansexual people, however they may identify themselves.
Sexual Orientation: The term that is used to describe the gender to whom a person is attracted in relation to their own gender. Sexual orientation is distinct from sexual behavior – i.e., an individual's sexual behavior may not match their orientation (e.g., celibacy, experimentation, or prostitution).
Social Stigma: Negative stereotypes and lower social status of a person or group based on perceived characteristics that separate that person or group from other members of a society.
SOGIE: An acronym for sexual orientation, gender identity and gender expression. Everyone has a sexual orientation, gender identity and gender expression.
Straight: A man who is attracted to women or a woman who is attracted to men.
Structural Stigma: Societal conditions, policies, and institutional practices that restrict the opportunities, resources, and well-being of certain groups of people.
Top: A slang term for the chest. Also refers to the insertive partner in anal sex.
Top Surgery: Slang term for gender-affirming chest surgery.
Transfeminine: A person who was assigned male sex at birth and identifies with femininity to a greater extent than with masculinity.
Transgender: When a person's biological or assigned gender does not coincide with their personal inner sense of gender identity, the person may identify as transgender. Transgender persons live at least some of their lives as members of a different gender group; those who seek gender-affirming surgery form a subgroup. Some transgender

people undergo surgeries or take hormones to alter the sex characteristics of their bodies, and others do not. Transgender people may consider themselves to be gay, lesbian, bisexual, transsexual, heterosexual, or none of these. They may identify explicitly with being male or female, a man or a woman, or they may not identify with any of these.

Transgender Man / Trans Man: A person who was assigned female sex at birth but identifies as and is living as a man. Similar terms include: "trans man," "trans boy," "transgender boy" and "affirmed male." Some transgender people object to the use of "FTM" or "F2M," abbreviations for "female-to-male." Some transgender males identify their gender as "transgender male," whereas others identify their gender as simply "male."

Transgender Woman / Trans Woman: A person who was assigned a male sex at birth but identifies as and is living as a woman. Similar terms include: "trans woman," "trans girl" and "affirmed female." Some transgender people object to the use of "MTF" or "M2F," abbreviations for "male-to-female." Some transgender females identify their gender as "transgender female," whereas others identify their gender as simply "female."

Trans Masculine: A person who was assigned female sex at birth and identifies with masculinity to a greater extent than with femininity.

Transition: A process by which transgender people align their anatomy (medical transition) or gender expression (social transition) with their gender identity. Often individuals and medical services will instead use the terms gender affirmation or gender confirmation. Terms such as "sex change" or "sex change operation" should not be used.

Transphobia: The irrational fear and hatred or non-acceptance of people whose gender identity or gender expression differs from the gender they were assigned at birth. Individuals, communities, policies, and institutions can be transphobic.

Transsexual: Individual with biological characteristics of one sex who identifies themselves as the opposite gender. In other words, a person whose gender identity is not consistent with their biological gender. This term is most often used to describe the subgroup of transgender individuals who seek out or desire medical interventions to make their body more gender congruent with their internal gender identity through surgery and/or hormonal treatment. Transsexuals may be heterosexual, bisexual or homosexual in their orientation. Some people experience the term transsexual as pejorative, and the term *transgender* should be used unless an individual specifically asks to be described as transsexual.

Trauma-Informed Care: An organizational structure and treatment framework that centers on understanding, recognizing, and responding to the effects of all types of trauma.

Tucking: The process of hiding one's penis and testes with tape, tight shorts, or specially designed undergarments.

Two-Spirit (2-S): Adopted in 1990 at the third annual spiritual gathering of GLBT Natives, the term derives from the northern Algonquin word *niizh manitoag*, meaning *two-spirit*, and refers to the inclusion of both feminine and masculine components in one individual. This culture-specific term is used among some Native American, American Indian, and First Nations people.

References:

A. Intersex Society of North America: www.isna.org/faq

B. Lucksted, A., Elven, J., Pendegar, E. (Undated). *Enhancing Cultural Competence: Welcoming Lesbian, Gay, Bisexual and Transgender Clients in Mental Health Services.* [On-line]. Available: http://medschool.umaryland.edu/facultyresearchprofile/uploads/59eabd4ebe674d01ae00ebfad157c442.pdf.

C. Movement Advancement Project (2019). *Where We Call Home: LGBT People in Rural America.* Boulder, CO. [On-line]. Available: https://www.lgbtmap.org/file/lgbt-rural-report.pdf.

D. NAMI and the UPenn Collaborative on Community Integration and National Alliance on Mental Illness. (2009). *GLBTQI Mental Health: Recommendations for Policies and Services*. [On-line]. Available: https://www.naminys.org/images/uploads/pdfs/GLBTQI%20Mental%20Health%20Recommendations%20for%20Policies%20and%20Services.pdf.

E. National Association of Social Workers. (2015). *Sexual Orientation Change Efforts (SOCE) and Conversion Therapy with Lesbians, Gay Men, Bisexuals, and Transgender Persons.* Washington, DC. [On-line]. Available: https://www.socialworkers.org/LinkClick.aspx?fileticket=IQYALknHU6s%3D&portalid=0

F. SCCMHA Policy 02.03.05 – Recovery

G. SCCMHA Policy 02.03.08 – Welcoming

H. SCCMHA Policy 02.03.14 – Trauma-Informed Services and Supports

I. SCCMHA Policy 02.03.41 – SOGI Safe

J. Substance Abuse and Mental Health Services Administration. (2012). *A Provider's Introduction to Substance Abuse Treatment for Lesbian, Gay, Bisexual, and Transgender Individuals.* SAMHSA. Rockville, MD.: https://store.samhsa.gov/sites/default/files/SAMHSA_Digital_Download/sma12-4104.pdf.

K. Substance Abuse and Mental Health Services Administration. (2013). *Building Bridges: LGBT Populations: A Dialogue on Advancing Opportunities for Recovery from Addictions and Mental Health Problems.* Substance Abuse and Mental Health Services Administration. Rockville, MD.: https://store.samhsa.gov/shin/content/SMA13-4774/SMA13-4774.pdf.

L. Substance Abuse and Mental Health Services Administration. (2015). *Ending Conversion Therapy: Supporting and Affirming LGBTQ Youth.* SAMHSA. Rockville, MD.: https://store.samhsa.gov/sites/default/files/d7/priv/sma15-4928.pdf.

M. The Center for Counseling Practice, Policy, and Research. (2009). *ALGBTIC Competencies for Counseling LGBQIQA.* American Counseling Association. [On-line]. Available: https://www.counseling.org/docs/default-source/competencies/algbtic-competencies-for-counseling-lgbqiqa.pdf?sfvrsn=1c9c89e_14.

Exhibits:
None

Procedure:
None

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Interdisciplinary Treatment Teams	**Chapter**: 03 – Continuum of Care	**Subject No**: 03.02.45
Effective Date: 7/16/2021	**Date of Review/Revision**: 5/10/22, 4/11/23, 4/4/24, 4/8/25	**Approved By**: Sandra M. Lindsey, CEO
	Supersedes:	**Responsible Director:** Executive Director of Clinical Services
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Authored By**: Barbara Glassheim
		Additional Reviewers:

Purpose:
The purpose of this policy is to delineate standards for the provision of interdisciplinary treatment team-based care for persons served that supports their health and well-being in a collaborative, structured, and person-centered manner.

Policy:
SCCMHA recognizes that no single individual can provide all of the services and supports that may be of benefit to a person served; effective service delivery most often entails a variety of professionals and other staff with a variety of roles, responsibilities, skills and competencies working collaboratively together and in partnership with the person served/family/caregiver. SCCMHA also recognizes that effective collaboration among professionals and persons served/families: (1) reduces fragmentation and siloed care; (2) leads to improved outcomes and satisfaction of persons served; (3) results in improved staff morale, job satisfaction and organizational productivity; (4) allows professionals to work at the top of their training, licenses and credentials; and (5) is cost effective. In addition, studies have demonstrated that team-based care results in improved health outcomes for persons served when compared to standard care. Accordingly, SCCMHA shall foster teamwork by encouraging the provision of interdisciplinary team-based, person-centered care to all persons served.

Application:
This policy applies to services and supports for persons served who are enrolled in the SCCMHA CCBHC (Certified Community Behavioral Health Clinic), SCCMHA Behavioral Health Home (BHH), and the SCCMHA Health Home & Wellness Center. Other programs shall consider implementing team-based care as warranted.

Standards:

A. Department/unit teams shall develop and implement standardized team-based workflows for significant and recurrent situations commonly experienced by the population(s) of persons they serve.

B. Teams shall have a designated leader and/or facilitator.
   1. Teams may elect to rotate the role of the facilitator to expedite team-building and participatory leadership.

C. The team facilitator/leader shall, in concert with the treatment/care team and the person served/family/caregiver, establish expectations, including the articulation of norms and shared values, for teamwork and collaboration.
   1. All team members shall be made to feel valued and empowered to speak up when necessary.
   2. Teams shall select technology that allows visibility to the entire team and the work at hand in order to accommodate members who are not in a shared workspace (i.e., accessing meetings remotely).
   3. Each team member's roles and responsibilities shall be clearly articulated and teams shall promote a shared understanding of each member's roles and responsibilities.
   4. Teams shall use shared decision-making (see definition below) to foster collaborative relationships with persons served and families/caregivers and among team members.
   5. Teams shall consider holding briefing meetings to ensure that all members understand goals, everyone's roles and responsibilities, and have a chance to voice concerns.
   6. Teams shall consider holding debriefing (i.e., self-audit) meetings in order to review their effectiveness, promote team building and trust, celebrate successes and learn from breakdowns.
   7. Teams shall promote ongoing communication among members using a variety of mechanisms including curbside consults (see definition below), secure messaging via the EHR (electronic health record), telephone contacts, etc.

D. Team meetings shall consist of regular structured formal meetings that include persons served and families/caregivers as well as smaller, two-to-three-person teams that gather for huddles as well as curbside consults (see definition below).
   1. Persons served and/or families/caregivers may be included in a huddle to promote quick shared decision making when an issue that requires the input of the person served/family arises.

E. The frequency of team meetings shall be flexible and based upon the needs and functional status of the person served.
   1. Some teams may engage in daily or weekly huddles while others may huddle on a monthly basis.
   2. Some teams may hold formal meetings on a weekly or monthly basis depending on the needs and health status of the person served.
      a. At a minimum, teams shall hold formal meetings every 90-days to conduct periodic reviews in accordance with SCCMHA, BHH, and CCBHC standards.

3. Team meetings or huddles shall be triggered by sentinel events which include, but are not limited to, the following:
    a. Change in level of care
    b. Care transition
    c. Change in living situations
    d. 90-day periodic review
    e. Significant life event (e.g., loss of a loved one or caregiver)
    f. Medical or mental health crisis
    g. Change in health or functional status
    h. A new diagnosis or diagnoses
    i. The need to address complex comorbidities

F. External providers shall be integrated into the person-centered planning process and development of shared plans of care in accordance with the person served/family/caregiver wishes and needs.
    1. External providers shall be included in team meetings as warranted.

G. The composition of interdisciplinary teams shall be flexible and person served/family-driven with a focus on whole-person care that integrates mental health, substance use disorder treatment, social care, and general health care in a seamless, coordinated manner.
    1. The initial composition of the team shall start with those members the person served/family wishes to have included in the initial person-centered planning process.
    2. Additional members shall be added in accordance with the wishes of person served/family as well as treatment and support needs.
        a. Additional members may include the primary care provider, PA (physician's assistant), RN (registered nurse), PT (physical therapist), OT (occupational therapist), RD (registered dietician), MA (medical assistant), speech and language therapist as well as employment specialist, Housing Resource Center staff, pharmacist, peer(s), residential services provider, etc.

H. All formal team meetings shall be documented in the EHR of the person served in accordance with SCCMHA policy.
    1. Documentation of huddles shall be optional and based on any significant biopsychosocial updates discussed.
    2. All formal meetings shall be accounted for by an authorized billing code that aligns with the services provided.

I. A team meeting shall be held when the team is considering presenting a case to the SCCMHA Adult Clinical Risk Committee. (See Exhibit A for a suggested conceptual framework.)
    1. Should the case be sent to the Clinical Risk Committee, information gleaned from the team meeting shall be used to help inform the committee's work.

Definitions:

Behavioral Health Home (BHH): An integrated service delivery model that provides comprehensive care management and coordination services to Medicaid beneficiaries with a serious mental illness/serious emotional disturbance (SMI/SED). Beneficiaries work with an interdisciplinary team of providers that includes peer support specialists and community

health workers to develop a person-centered care plan. The BHH provides six core services: (1) comprehensive care management; (2) care coordination; (3) health promotion; (4) comprehensive transitional care; (5) individual and family support; and (6) referral to community and social services.

Certified Community Behavioral Health Clinic (CCBHC): A non-profit organization or unit of a local government behavioral health authority that must directly provide (or contract with partner organizations to provide) nine types of services, with an emphasis on the provision of 24-hour crisis care, evidence-based practices, care coordination with local primary care and hospital partners, and integration with physical health care. (Richardson & Ingoglia) The nine core services are: (1) crisis mental health services, including 24-hour mobile crisis teams, emergency crisis intervention services, and crisis stabilization; (2) screening, assessment, and diagnosis, including risk assessment; (3) patient-centered treatment planning or similar processes, including risk assessment and crisis planning; (4) outpatient mental health and substance use services; (5) outpatient clinic primary care screening and monitoring of key health indicators and health risk; (6) targeted case management; (7) psychiatric rehabilitation services; (8) peer support and counselor services and family supports; and (9) intensive, community-based mental health care for members of the armed forces and veterans, particularly those members and veterans located in rural areas.

Curbside Consult: A meeting held between two practitioners for the purpose of seeking information or advice regarding the care of a person served from a colleague.

Five Components of Effective Interdisciplinary Teams: (1) Established, open, safe communication patterns. (2) Well-defined and appropriate team goals. (3) Clear role definitions and expectations for team members. (4) A real-time, structured yet flexible decision-making process. (5) The ability of the team to "treat itself" by celebrating accomplishments and addresses breakdowns. (Leipzig, et al.)

Shared Decision-Making (SDM): An approach to care through which providers and recipients (i.e., persons served) of health care come together as collaborators in determining the course of care. Key characteristics include having the health care provider, person served, and sometimes family members and friends acting together, including taking steps in sharing a treatment decision, sharing information about treatment options, and arriving at consensus regarding preferred treatment options (Schauer, et al.).

Team Huddle: A brief meeting (e.g., 10 to 30 minutes) that can occur at a variety of frequencies and is scheduled to meet the unique needs of each team. Huddles are designed to address immediate care coordination needs of the person served in contrast to **team meetings** which occur on a regularly scheduled basis and include everyone involved in the care of the person served and may also include the person served and their family/caregiver.

References:

A. Leipzig, R., Hyer, K., Ek, K., et al. (2002). Attitudes Toward Working on Interdisciplinary Healthcare Teams: A Comparison by Discipline. *Journal of the American Geriatrics Society 50:* 1141–1148.

B. Michigan Department of Health and Human Services. (2024). *Behavioral Health Home Handbook Version 2.0.* (www.michigan.gov/bhh)

C. Michigan Department of Health and Human Services. (2025*). Michigan Certified Community Behavioral Health Clinic (CCBHC) Handbook Version 2.1*. (https://www.michigan.gov/mdhhs/keep-mi-healthy/mentalhealth/ccbhc)

D. Richardson, J., Ingoglia, C. (August 5, 2020). *What is a CCBHC?* National Council for Behavioral Health.
E. SAMHSA. Criteria for Certified Community Behavioral Health Clinic: https://www.samhsa.gov/sites/default/files/programs_campaigns/ccbhc-criteria.pdf.
F. Schauer, C., Everett, A., del Vecchio, P., et al. (2007). Promoting the value and practice of shared decision-making in mental health care. *Psychiatric Rehabilitation Journal 31(1):* 54-61.
G. SCCMHA Departmental Procedures for Interdisciplinary Treatment Teams – Children's Services, Community Support Services (CSS), Supports Coordination Services (SCS), and Health Home Huddle.

Exhibits:
None.

Procedure:
Each department shall be responsible for developing team-based procedures, protocols and work flows that are tailored to meet the needs of the population(s) served as well as the unique needs of the department or unit itself.

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Older Adult Services	**Chapter**: 03-Continuum of Care	**Subject No**: 03.02.48
Effective Date: 7/1/24	**Date of Review/Revision**: 4/8/25	**Approved By**: Sandra M. Lindsey, CEO
	Supersedes:	
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Responsible Director:** Executive Director of Clinical Services **Author:** Barbara Glassheim **Additional Reviewers**:

Purpose:
The purpose of this policy is to set forth principles and standards for delivering services to persons aged 50 and older with a diagnosed mental illness, substance use disorder (SUD), or intellectual/developmental disability (I/DD), including those with co-occurring or multiple diagnoses, including co-morbid general health conditions.

Application:
This policy applies to all SCCMHA-funded services and supports delivered by the entire provider network to older adults with a mental illness, SUD, and/or I/DD.

Policy:

SCCMHA recognizes that older adult persons served are at higher risk for complex health problems, chronic illness, and disability than their younger counterparts.

According to the US Administration on Aging and the Substance Abuse and Mental Health Services Administration (SAMHSA), approximately twenty percent (20%) of adults fifty (50) years and older have mental health concerns. Depression, anxiety, alcohol misuse, and psychoactive medication misuse are the most common types of mental health and substance use issues among older adults. Older men have the highest suicide rates. While there are effective prevention, treatment, recovery services, and supports for older adults, this population is significantly less likely to be diagnosed and referred to treatment than younger adults. Moreover, older adults may be reluctant to seek help from mental health providers due to misattribution of symptoms to general health conditions (i.e., medical problems) as well as the stigma associated with behavioral health treatment.

Adults with a diagnosis of a serious mental illness (SMI) are disproportionately affected by medical comorbidity, earlier onset of disease, and die up to 25 years earlier than their counterparts in the general population, and those with SUDs die up to 35 years earlier. (The average age of death for a person with an SMI is 53 and 45 years of age for a person with a substance use disorder.) Moreover, age-related changes in metabolism, physiology, and activity may contribute to the development of additional illnesses and worse

health outcomes. Comorbidities are common in this population; mental health disorders often co-occur with a number of common chronic illnesses such as diabetes, cardiac disease, and arthritis. In addition to co-morbid physical and behavioral health conditions, older adults are at greater risk for social isolation which is associated with poor health and emotional distress, particularly for those with multiple chronic conditions or functional limitations.

While adults with intellectual/developmental disabilities are living longer, healthier, more meaningful lives, adults with I/DD can have a shorter life span compared to older adults in the general population. This is thought to be caused by an accelerated aging process, manifest in increased rates of cataracts, hearing loss, osteopenia, and hypothyroidism and a genetically elevated risk of developing Alzheimer's disease. There is a higher incidence of dental disease, functional decline, mental illness, bowel obstruction, gastrointestinal cancer, and obesity among older adults with I/DD. Additionally, hearing impairment and vision loss are common in older adults with I/DD due to preexisting undiagnosed pathologies. Providers may be challenged to accommodate adults with I/DD who have communication and behavioral difficulties that create barriers to effective assessment and treatment. This population may display behavioral issues that could negatively impact their ability to cooperate with tests, injections, and other procedures. Communication issues may make interaction among the provider, caregiver, and person served challenging. Finally, physical challenges (e.g., cerebral palsy) may make it physically difficult to access a health care facility and environmental issues that may involve sensory challenges (e.g., lighting, sound, smells) can interfere with the ability of a person served to effectively participate in the visit.

SCCMHA recognizes the detrimental impact ageism has on both physical and mental health. It plays a role in social isolation, worse overall health, and reduced life expectancy. It also affects people in multiple areas including school, work, leisure activities and healthcare. SCCMHA also recognizes that good general health and social care are important for the promotion of older adults' health, disease prevention and the effective management of chronic illnesses.

Therefore, SCCMHA providers need to be knowledgeable about issues specific to older adults in order to ensure that services and supports are appropriate to the phase of life occupied by older adults. SCCMHA providers also need to be aware of specific resources for older adults and their caregivers such as wellness programs, nutritional support, educational programs about health and aging, and counseling services for caregivers, as well as general assistance with housing, finances, and home safety.

Specifically, SCCMHA providers need to take into consideration a number of factors when serving older adults including the following: (1) age-related changes in the metabolism of medications and alcohol that can exacerbate mental, physical and substance use disorders; (2) losses often occur in older age such as the death of a spouse, partner, close family member, or friend which can trigger emotional responses that can exacerbate mental health symptoms; (3) medications used to treat acute and chronic health conditions that can cause or exacerbate mental health conditions; (4) cognitive, functional and sensory impairments that can complicate the detection or diagnosis of mental health conditions as well as impair an older person's ability to adhere to recommended treatment regimens; (5) older adults are less likely to seek mental health treatment than their younger counterparts and may, instead, seek help from clergy or other trusted members of their community; and

(6) cultural and linguistic competence needed to effectively serve the growing diversity of the older adult population.

Standards:

A. SCCMHA shall promote healthy aging (see definition below) by encouraging older adult persons served to proactively take preventive health measures, learn how to self-manage chronic conditions, and participate in engaging, stimulating, and meaningful activities.

B. SCCMHA shall, resources permitting, offer continuing education regarding the unique needs of older adult persons served.
   1. SCCMHA shall encourage staff to understand issues associated with substance misuse, mental health, and I/DD conditions in older adults.
   2. SCCMHA shall encourage staff to become familiar with comorbid general health issues associated with older adults who have an SMI, SUD, COD, I/DD.
   3. SCCMHA shall encourage staff to understand, appreciate and combat the many myths associated with aging, particularly those associated with mental health issues and substance misuse in older adults.

C. The desires and functioning of each individual older adult person served shall be taken into consideration in the planning and delivery of services and supports.

D. Practitioners shall use standardized screening and assessment instruments to evaluate older adults that have been validated for this populations (e.g., PHQ-9, GAD-7).
   1. Universal screening for suicidality is recommended.

E. Practitioners shall use evidence-based interventions and treatments that are appropriate for older adults (e.g., CBT, DBT, Interpersonal Psychotherapy).
   1. Treatment decisions shall be made in a collaborative manner in partnership with the person served and their family/support system (where appropriate and available) using a shared decision-making approach.

F. Services and supports provided to older adult persons served shall be culturally relevant.
   1. Providers shall be aware of and seek to avoid stigma and ageism when working with older adult persons served.

G. Providers shall offer care management services to older adult persons served in order to help those with co-occurring conditions manage their health conditions. These care management services shall include:
   1. Assessing the needs of the person served.
   2. Developing a care plan in collaboration with the older adult person served and their natural and paid support system using shared decision-making.
   3. Ensuring preventive care services are provided.
   4. Providing medication reconciliation.
   5. Managing care transitions between providers/settings.
   6. Coordinating with home- and community-based providers.

H. SCCMHA providers shall support aging in place in accordance with the goals and wishes of person served.
   1. Providers shall focus on helping older adult persons served maintain their health and enabling them to remain safely in the community.

2. Providers shall ensure necessary supports (e.g., transportation, assistance with homemaking [domestic duties], recreation/leisure activities, etc.) are made available to older adult persons served.
3. Providers shall avoid nursing home placement to the greatest extent possible.
    a. Institutionalization shall be deemed a last resort *only* available after *all* other possible options have been exhausted.

    NOTE: Nursing homes are not considered appropriate settings for the care of individuals with a serious mental illness absent other functional impairments or medical conditions that warrant nursing home care.

I. SCCMHA network providers shall focus on helping older adult persons served function as independently as possible in the community.
    1. Providers shall assist older adult persons served to establish and maintain meaningful connections in the community.

J. SCCMHA network providers shall endeavor to recruit older adult peer support specialists and community health workers (CHWs) when feasible to help engage older adult persons served in their own care and self-management of chronic conditions.

K. SCCMHA network providers shall offer support to family caregivers of older adult persons served and link them to community resources (e.g., respite services, support groups, caregiver trainings) with a focus on helping families and caregivers maintain their own health and well-being to lessen caregiver burden and prevent burnout.

L. SCCMHA network providers shall endeavor to promote advance care planning, including resources for the provision of help with palliative care and end-of-life decision-making.
    1. SCCMHA providers shall connect older adult persons served and their caregivers with legal and social services as needed.

Definitions:

Ageism: Stereotypes, prejudice and discrimination towards others or oneself based on age (WHO). There are two primary types of ageism. The term ageism is usually used to apply to discrimination against older adults, while reverse ageism has been used to describe how younger adults can also face prejudice and discrimination because of their age (e.g.,. dismissing younger workers as too inexperienced, unprofessional, or not qualified for advancement).

Everyday examples of ageism include, but are not limited to:

- ‘Anti-aging’ products and services
- Praising older individuals by comparing them to younger ones (e.g., "You look good for [your age]," "You're young at heart" or "Inside, I feel 30 years younger)
- Describing minor forgetfulness as a "senior moment"
- Patronizing language (e.g., “sweetie”, “dear”, “honey”, “he's so sweet”, “isn't she cute”)
- Assuming that young people are computer whizzes and older people are technologically inept

- Pejorative labels (e.g., “geezer”, “gramps”, “little old lady”, “old bag”, “biddy”, “old fogey”)
- Directing comments about an older person at a younger companion or child of the older person

Ageism, a systemic form of oppression, can range from subtle actions to blatant acts of discrimination in the workplace, including but not limited to:

- Being excluded from the rest of the group
- Being passed over for promotions or raises
- Forcing older people to retire or laying off older workers
- Negative comments about a person's age
- Not accepting input from younger people or dismissing their input due to lack of experience
- Not getting the same benefits such as paid time off
- Only providing learning opportunities to younger people

Functional Abilities: The abilities to meet basic needs; learn, grow and make decisions; be mobile; build and maintain relationships; and contribute to society. (WHO)

Healthy Aging: The process of developing and maintaining the functional ability that enables wellbeing in older age. (WHO)

References:

A. SCCMHA. (2013). *A Guide to Evidence-Based Practices for Older Adults with Mental Illness*: https://www.sccmha.org/userfiles/filemanager/293/
B. SCCMHA Policy 02.03.12 – Alternatives to Guardianship
C. SCCMHA Policy 03.02.18 – Respite Services
D. SCCMHA Policy 03.02.46 – Whole-Person Care
E. SCCMHA Policy 10.01.01.01 – Care Transitions
F. Substance Abuse and Mental Health Services Administration. (2019). *Get Connected: Linking Older Adults with Resources on Medication, Alcohol, and Mental Health*. SAMHSA Rockville, MD.: https://www.store.samhsa.gov/sites/default/files/SAMHSA_Digital_Download/PEP20-02-01-011%20PDF%20508c.pdf
G. Substance Abuse and Mental Health Services Administration and Health Resources and Services Administration. (2016*). Growing Older: Providing Integrated Care for an Aging Population*. SAMHSA. Rockville, MD.: https://store.samhsa.gov/sites/default/files/d7/priv/sma16-4982.pdf
H. World Health Organization. Decade of Healthy Aging: 2020–2030. Update 1: March, 2019. WHO. Geneva, Switzerland.: https://www.who.int/docs/default-source/documents/decade-of-health-ageing/decade-healthy-ageing-update-march-2019.pdf?sfvrsn=5a6d0e5c_2

Exhibits:

None

Procedure:

None

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Behavioral Health Screening and Assessment Standards	**Chapter**: 03- Continuum of Care	**Subject No**: 03.01.01.07
Effective Date: 5/1/24	**Date of Review/Revision**: 4/8/25 **Supersedes**:	**Approved By**: Sandra M. Lindsey, CEO
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Responsible Director:** Executive Director of Clinical Services **Authored By**: Barbara Glassheim **Additional Reviewers**:

Purpose:
The purpose of this policy is to set forth methods used by SCCMHA to identify individuals with behavioral health (mental health and/or substance use) disorders and intellectual/developmental issues.

Policy:
SCCMHA shall adopt and promote the use of evidence-based, standardized, valid, reliable, population-specific, and developmentally and culturally appropriate screening and assessment instruments for evaluation purposes as well as to promote the provision of effective prevention and intervention services and supports, improve outcomes, and reduce excess morbidity and mortality among persons eligible for services.

Application:
This policy applies to all SCCMHA-funded providers of mental health and substance use disorder prevention, treatment, and recovery services as well as to providers of services and supports to individuals with an intellectual/developmental disability.

Standards:

A. SCCMHA shall adopt the use of screening and assessment instruments with strong psychometric properties that have a high degree of reliability and validity for the populations served by SCCMHA.
   1. These basic psychometric properties shall include:
      a. Reliability (the ability of a measure to produce consistent results)
      b. Validity (the ability to discriminate between an individual with a problem and one without such a problem)

c. Classification accuracy (the adequacy of cutoff scores used to indicate whether the individual has, or is at risk for having, a specific condition)
d. Sensitivity (the accuracy of the instrument in identifying a problem)
e. Specificity (the accuracy of the instrument in identifying individuals who do not have a problem)
f. Fairness (the extent to which the scores are equally reliable and valid for various populations)
g. Norm adequacy (whether reference groups used to assist in score interpretation adequately represent the population for which an instrument is designated)

B. SCCMHA shall conduct universal screening for general behavioral health and developmental conditions as well as the social determinants of health (SDOH).
1. Targeted screening and assessment shall occur on an individualized basis as clinically indicated.

C. Screening and assessment shall occur at intake and continue throughout the course of treatment as warranted in order to determine progress and the potential need for modification(s) to the IPOS in accordance with the frequency set forth in Standard D (below) and Exhibit A.

D. Instruments will be used to identify the strengths and areas of unmet need of persons served at intake, during periodic (90-day) reviews, and discharge as well as when indicated by progress toward goal achievement or lack thereof in accordance with the administration standards of each instrument.
1. Screening and assessment shall be conducted based on the individual's needs, presenting concerns, progress in meeting identified goals and objectives, and SCCMHA protocols.
a. An initial screening shall be conducted upon intake or entry into services to identify immediate mental health, substance use, and or developmental concerns.
b. A comprehensive assessment shall be conducted following the initial screening to gather detailed information about the individual's behavioral health status, history, and needs in order to help determine the need for further assessment and appropriate levels of care and support.
c. Regular monitoring shall be conducted throughout the course of treatment/service provision based on the individual's treatment plan, severity of symptoms/issues, response to interventions, and changes in levels of care or services and supports.
1). Monitoring may consist of brief check-ins, symptom rating scales, or structured assessments at scheduled intervals (e.g., weekly, bi-weekly, monthly).
b. Periodic reassessment shall be conducted at a minimum of every ninety (90) days to evaluate progress, identify changes in symptoms or functioning, and adjust treatment and /or support goals as needed.

1). Reassessment intervals may be increased in accordance with the individual's needs and plan of services such as when changes in level of care or supports occur.

c. Immediate assessments in response to crises or significant changes in the individual's mental health status shall be conducted as needed to assess risk, provide intervention, and ensure safety.

d. Assessments during transitions between levels of care or treatment/care settings (e.g., from inpatient to outpatient, from child to adult services) shall be conducted to help ensure continuity of care, identify ongoing needs, and facilitate appropriate referrals or adjustments to treatment/support plans.

e. Assessments prior to discharge from services shall be conducted to evaluate treatment/support outcomes, assess readiness for discharge, and provide appropriate referrals and/or follow-up recommendations.

f. Additional assessments shall be conducted as needed based on changes in the individual's circumstances, treatment goals, or presenting concerns.

1). Assessments may be prompted by factors such as lapse or relapse, significant life events, or requests for reevaluation.

E. All positive screenings for individuals who are deemed to be at-risk due to depression, anxiety, posttraumatic stress disorder, suicidality, trauma, substance misuse, and developmental delays shall be immediately followed up with a full assessment using a standard SCCMHA-approved assessment instrument and the current version of Diagnostic Statistical Manual of Mental Disorders, the International Classification of Disease, ASAM criteria, and other relevant standard diagnostic criteria.

F. Screening and assessment shall be conducted in accordance with the following principles:

1. Establish a private and comfortable space for the screening and assessment process, ensuring confidentiality.
2. Respect the autonomy and dignity of the individual/family throughout the screening and assessment process.
3. Provide an explanation of the purpose of the screening or assessment.
   a. Seek informed consent and provide clear explanations of the purpose, procedures, and potential risks and benefits of screening and assessment.
4. Take care to avoid biases and stereotypes and strive for cultural competence in working with diverse populations.
5. Adhere to the instructions provided with the instrument to ensure accuracy in administration.
6. Score the instrument in accordance with established instrument-specific guidelines.
7. Provide feedback to the individual/family regarding the results in a clear, empathic, and nonjudgmental manner.
8. Collaboratively develop treatment goals and recommendations based on the assessment findings, considering the individual's/family’s preferences and available resources.

9. Document the screening and assessment results, clinical impressions, and treatment and support services recommendations accurately and comprehensively in the individual's electronic health record.
10. Follow up with the individual/family as needed to monitor progress, adjust treatment/support plans, and provide ongoing services and assistance as needed.

G. SCCMHA shall endeavor assure that staff using instruments which require training and/or specific credentials meet the qualifications to effectively administer them and reliably interpret the results.
   1. Competent administration of screening and assessment measures shall require staff who use or supervise the use of the instruments to have skills and training appropriate for their assigned tasks.
      a. Specific training and skills may be include knowledge of appropriate measures for the specific referral issue(s), relevant information about the specific characteristics of the individual being assessed (e.g., age, race, gender, language, disability, etc.), and expertise in administration and/or scoring of the instrument.

Definitions:

Behavioral Health: For the purposes of this policy, this term is used all-inclusively to refer to mental health issues, substance use disorders, and intellectual/developmental disabilities. It includes all of the populations served by SCCMHA.

Screening: A formal interviewing and/or testing process that identifies areas of an individual's life that might need further examination. Screening evaluates the possible presence of a problem but does not diagnose or determine the severity of a disorder. When positive indicators are found, the individual is scheduled for an assessment.

Screening is used for the early identification of individuals at potentially high risk for a specific condition or disorder and can indicate a need for further evaluation or preliminary intervention. Screening is generally brief and narrow in scope and may be administered as part of a routine clinical visit. Screening is also used to monitor treatment progress, outcome, or change in symptoms or support needs over time. Screening instruments may be administered by clinicians, support staff with appropriate training, an electronic device (e.g., computer), or it may be self-administered. Staff follow an established protocol for scoring with a pre-established cut-off score and guidelines for individuals who score positive. It should be noted that screening is neither definitively diagnostic nor a definitive indication of a specific condition or disorder.

Assessment: A more in-depth evaluation that confirms the presence of a problem, determines its severity, and specifies treatment options for addressing the problem. It also surveys the individual’s strengths and resources for addressing life problems. Assessment typically examines not only possible diagnoses, but also the context in which a disorder manifests.

Assessment provides a more complete clinical picture of an individual, is comprehensive in focusing on the individual’s functioning across multiple domains and can aid diagnosis and/or treatment planning in a culturally competent manner as well as identify behavioral health problems and conditions, indicate their severity, and provide treatment recommendations. Assessment integrates results from screening, clinical interviews, behavioral observations, clinical record reviews, and collateral information and may include

screening measures that are used in conjunction with other information from the assessment, providing a broader context for interpreting the results.

References:

A. American Psychiatric Association: *Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision* (DSM-5-TR)
B. American Society of Addiction Medicine (ASAM) Criteria
C. SCCMHA Policy 02.03.17 – Outcome Tool for Adults (ANSA)
D. SCCMHA Policy 02.03.18 – PECFAS & CAFAS
E. SCCMHA Policy 02.03.19 – LOCUS
F. SCCMHA Policy 02.03.04 – Suicide Prevention
G. SCCMHA Policy 02.03.09 – Evidence-Based Practice
H. SCCMHA Policy 02.03.09.40 – SBIRT/YSBIRT
I. SCCMHA Policy 02.03.42 – DECA
J. SCCMHA Policy 03.01.01 – Eligibility Criteria
K. World Health Organization (WHO): *International Statistical Classification of Diseases and Related Health Problems (ICD)*

Exhibits:

A. SCCMHA-approved Screening and Assessment Instruments Chart

Exhibit A

SCCMHA SCREENING AND ASSESSMENT INSTRUMENTS

Instrument	Population	Frequency of Administration	Staff	Diagnostic Group/Construct/Dimension
CTAC (Children's Trauma Assessment Center) Trauma Screening Checklist	Children (ages 0 – 5) Children/Youth (ages 6 – 18)	• Intake • After a trauma experience	CAI, MRSS, CIS, Therapist	Trauma
GAD-7 (Generalized Anxiety Disorder 7-item scale)	Adolescents/Adults	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Anxiety
UCLA PTSD (Posttraumatic Stress Disorder) Reaction Index	Children/Adolescents (ages 7 – 17)	After a + trauma screen	Clinician	PTSD
PCL–5 (PTSD Checklist for DSM-5)	Adults	• Intake After a trauma experience	CAI, MRSS, CIS, Therapist	PTSD
YCPC (Young Child PTSD Checklist)	Children (ages 1 – 6)	After a + trauma screen	Clinician	Assessment of PTSD symptoms
DAST–10 (Drug Abuse Screening Test)	Adults	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Substance misuse/SUD
DAST–A (Drug Abuse Screening Test for Adolescents)	Adolescents	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Substance misuse/SUD
AUDIT (Alcohol Use Disorders Identification Test)	Adults & Older Youth	• Intake • Every 90 days during periodic review	CAI, MRSS, CIS, Therapist	AUD
AUDIT-C (3-question versions of the AUDIT)	Adults & Older Youth	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Alcohol misuse (risky hazardous drinking)/AUD
CRAFFT +N (Car, Relax, Alone, Forget, Friends, Trouble + Nicotine)	Youth (ages 12 – 21)	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Substance misuse
PHQ-9 (Patient Health Questionnaire)	Adults	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Depression

PHQ-A (PHQ-9 modified for Adolescents)	Adolescents	• Intake • Every 90 days during periodic reviews	CAI, MRSS, CIS, Therapist	Depression
ASQ (Ask Suicide-Screening Questions)	Youth (ages 10 – 21)	• Intake • Every 90 days during periodic reviews	Clinician	Suicide Risk
C-SSRS (Columbia-Suicide Severity Rating Scale)	Youth & Adults (ages 11+)	• After a + screen • Every 90 days during periodic reviews	Clinician	Suicide Risk
SIS (Supports Intensity Scale)	Individuals with I/DD	• Intake • Over time to document changing needs	CAI, Clinician	Level of services/supports needed
LOCUS (Level Of Care Utilization System)	Adults with MI	• Intake • Every 90 days during periodic reviews • During psych hospital preadmission screening • D/C	CAI, CIS, MRSS, Clinician	UM/LOC
ANSA (Adult Needs and Strengths Assessment)	Adults	• Intake • Semi-annually • When there is a significant change in functioning that results in the need to change the IPOS • D/C	CAI, Clinician/Case Holder	LOC
DD-ANSA (Developmental Disabilities Adult Needs and Strengths Assessment)	Adults with DD	• Intake • Semi-annually • When there is a significant change in functioning that results in the need to change the IPOS • D/C	CAI, Clinician/Case Holder	LOC

ASAM (American Society of Addiction Medicine) Criteria	Adolescents/Adults	• Intake • Every 90 days during periodic reviews	CAI, CIS, MRSS, Clinician	Utilization management/Level of care for SUD/COD
DECA (Devereux Early Childhood Assessment)	Infants – Children (4 weeks – age 6)	• Intake • Every 3 months throughout service provision • D/C	CAI Case Holder	• Behavior rating scales • Social and emotional skills and competencies
DECA Infant	Infants (4 weeks – 17 months)	• Intake • Every 3 months throughout service provision D/C	CAI Case Holder	• Behavior rating scales Social and emotional skills and competencies
DECA Toddler	Toddlers (18 months – 23 months)	• Intake • Every 3 months throughout service provision D/C	CAI Case Holder	• Behavior rating scales Social and emotional skills and competencies
DECA Clinical	Children (2 – 6 years)	• Intake • Every 3 months throughout service provision D/C	CAI Case Holder	• Behavior rating scales Social and emotional skills and competencies
PECFAS (Preschool and Early Childhood Functional Assessment Scale)	Children (ages 2 –6) with SED	• Intake SEDW application • Intake 1915(i) SPA application • Annual SEDW reassessment • Annual 1915(i) SPA reassessment • Exit from SEDW • Exit from 1915(i) SPA	CAI Case Holder	Day-to-day functioning across critical life domains
CAFAS (Child and Adolescent Functional Assessment Scale)	Youth (ages 7 –20) with SED Young adults 18 – 20 in Wraparound, TAY	• Intake SEDW application • Intake 1915(i) SPA application • Annual SEDW reassessment • Annual 1915(i) SPA reassessment • D/C	CAI Case Holder	• Day-to-day functioning across critical life subscales • Determining improvement in functioning over time
Accountable Health Communities (AHC) Health-Related Social Needs (HRSN) Screening Tool	All persons served	• Intake • Periodic reviews • D/C	Case Holder	• SDOH

Modified Checklist for Autism in Toddlers (M-CHAT)	Toddlers 16 – 30 months	• Intake	CAI	• ASD Screening
Michigan Child and Adolescent Needs and Strengths (MichiCANS)	Infants, children, youth and young adults (birth through age 20) Individuals with I/DD (ages 17 and younger) and their families	• Intake (eligibility determinations for the Waiver for Children with Serious Emotional Disturbances (SEDW) and the 1915(i) SPA) • Annual redetermination • Intake • Every 90 days during periodic reviews • During psych hospital preadmission screening • D/C	Clinician, CAI, Case Holder	• Eligibility determinations for services • Assist with initial determination of needs and strengths • Provide information for appropriate referrals for behavioral health services • Functional needs assessment
MichiCANS Screener	Children, youth	• Intake screening	CAI	• Eligibility determination
MichiCANS Comprehensive	Children, youth	• Intake • Annual redetermination • D/C (exit)	Clinician, CAI, Case Holder	
Social Communication Questionnaire (SCQ)	Ages 4 and older	• Intake screening	CAI	• ASD screening

Key:

PTSD/Trauma
Suicide Risk
Depression
SUDs
Functioning/needs & supports

+ – Positive
1915(i) SPA) – State Plan Amendment (SPA) program to provide eligible Medicaid beneficiaries additional home and community based (HCBS) services
Adolescent – 12 to 18 years
Adult – 18+ years
ASD – Autism Spectrum Disorder
AUD – Alcohol Use Disorder
CAI – Centralized Access & Intake (SCCMHA)
CIS – Crisis Intervention Services (SCCMHA)
COD – Co-occurring Disorder (MH/SUD)
D/C – Discharge
HRSNs – Health-related social needs
LOC – Level Of Care
MA – Medical Assistant
I/DD – Intellectual/Developmental Disability
IPOS – Individual Plan of Services
MH – Mental Health
MI – Mental Illness
MRSS – Mobile Response & Stabilization Services (SCCMHA)
PTSD – Posttraumatic Stress Disorder
Psych – Psychiatric
RN – Registered Nurse
SED – Serious Emotional Disturbance
SEDW – Children with Serious Emotional Disturbance Waiver
SDOH – Social Determinants of Health
SEDW – Children with Serious Emotional Disturbance Waiver
SUD – Substance Use Disorder
TAY – Transitional Age Youth
UM – Utilization Management

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Management of Medical Products, Supplies, and Devices	**Chapter**: 05 - Organizational Management	**Subject No**: 05.01.01
Effective Date: December 1, 2007	**Date of Review/Revision**: 6/8/12, 1/15/13, 6/24/14, 4/7/16, 3/15/17, 9/11/17, 6/11/18, 2/26/19, 6/12/19, 11/30/20, 4/12/22, 1/31/25	**Approved By**: Sandra M. Lindsey, CEO
	Supersedes:	**Responsible Director:** Chief of Health Services & Integrated Care
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Authored By:** Jen Kreiner **Additional Reviewers**: Medical Director

Purpose:
The purpose of this policy is to ensure the proper handling, storage, dispersing, and documentation of medical and pharmaceutical products, supplies, and devices, including interactions with persons served, colleagues, and representatives of the manufacturers.

Policy:
It is the policy of SCCMHA that all medical and pharmaceutical products, supplies, and devices be properly received, stored, and inventoried. They will be dispersed responsibly and documented accurately. Interactions with representatives of manufacturers will follow legal and ethical requirements, avoiding biases and financial inducements that may have the potential to influence medical decision-making or other aspects of care for persons served.

Application:
This policy applies to all staff in SCCMHA direct operated programs and representatives of manufacturers, contractors, and vendors of any medical products, supplies, and devices.

Standards:
A. Staff will abide by ethical standards to ensure the dispersing of samples is based solely on the medical needs of the person served. There should be no favoritism, discrimination, or dispersing based on personal biases or incentives.
B. Staff will maintain a high level of professionalism with persons served, staff, and representatives of manufacturers.
C. Staff will maintain records necessary to comply with Federal, State and other applicable laws, regulations, and requirements.
D. Staff will ensure the safe handling and storage of medical and pharmaceutical products, supplies, and devices. This includes following all safety necessary and

personal protective equipment when necessary and reporting any safety hazards immediately.

Staff will accurately and promptly document all steps in the handling, storage, and dispersing of medical and pharmaceutical products, supplies, and devices utilizing the agency's Medical Product Dispersing Form. **Definitions:**

Sample medications and/or products: limited quantities of a medication, product, or device provided at no cost, by the manufacturer or other organization.
Stock medications and/or products: medications, products, or devices purchased by SCCMHA to be administered to, or utilized in the treatment of persons served.
Dispersing: providing pre-package or pre-dispensed medication, product, or device to a person served or another entity.
Disposal: to safely waste, destroy, or render unusable, any medications, products, or devices according to guidelines set forth by the manufacturer, Environmental Protection Agency (EPA) and/or other applicable entities.
Standing order: a documented prescription by an authorized provider, practicing within their scope, that allows for the dispersing or administration of a medication, product, test, and/or device.

References:

A. 21 CFR 203.32 at https://www.ecfr.gov/current/title-21/section-203.32
B. FDA guidelines for the storage of stock and sample medications in an outpatient clinic.
C. Environmental Protection Agency guidelines for the disposal of medication and unused medical products.
D. Michigan Board of Pharmacy Rules
E. SCCHMA Visitor policy

Exhibits:

A. Medical Product Dispersing/Disposal Form.
B. EPA medication disposal graphic
C. Sentri Sample “dispense” note

Procedure:

ACTION	RESPONSIBILITY
Maintain records necessary to comply with Federal, State and all applicable requirements.	Medical and Nursing staff
Store medical products, supplies, and devices in locations that meet legal and manufacturer requirements for proper	Medical and Nursing staff

environmental storage and loss prevention.	
Maintain inventory of medical products, supplies, and devices.	Medical and Nursing staff
Follow visitor procedures at all locations.	Representatives of manufacturers, contractors, and vendors
Quarantine and dispose of medical products, supplies, and devices following EPA and/or FDA guidelines, in addition to any special instructions from the manufacturer.	Medical and Nursing staff
Document the disposal of medical products, supplies, and devices using the Medical Products, Supplies, and Devices Form, using a witness if the product is a controlled substance.	Medical and Nursing staff
Disperse medical products, supplies, and devices to person served after verification of a valid prescription or order from an SCCMHA prescriber.	Medical and Nursing staff
Approves special circumstances.	Medical Director and/or Chief of Health Services and Integrated Care

Disbursement
Order/Rx

Documentation

VIII. Procedure
Actions:
1. Receiving and storing of pharmaceutical samples.
2. Distribution of pharmaceutical samples to patients.
3. Documentation of received and distributed pharmaceutical samples.
4. Regular inventory checks and audits.

Responsible Party for Actions:
1. The Pharmacy Manager is responsible for the receipt and storage of pharmaceutical samples.
2. Psychiatrists, Nurse Practitioners, and other authorized prescribers are responsible for the distribution of samples to patients.
3. The Pharmacy Manager and authorized prescribers are responsible for the documentation of received and distributed samples.
4. The Pharmacy Manager is responsible for conducting regular inventory checks and audits.

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Psychiatric Supervision & SCCMHA Medical Director Role</td><td>Chapter: 05 - Organizational Management</td><td>Subject No: 05.01.04</td></tr>
<tr><td rowspan="2">Effective Date:
8/6/01</td><td>Date of Review/Revision:
6/30/09, 4/11/11, 6/18/12, 6/6/13, 4/7/16, 6/11/18, 2/26/19, 6/12/19, 11/25/20, 10/11/21, 9/14/22, 8/29/2025</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Jen Kreiner, Chief of Health Services & Integrated Care

Authored By: Jen Kreiner

Reviewed By: SCCMHA Medical Director, Service Management Team</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this Policy is to define the role, responsibilities, and authority of the Medical Director in accordance with the Michigan Mental Health Code, Michigan Medicaid Provider Manual, Michigan Department of Health and Human Services (MDHHS) requirements, Certified Community Behavioral Health Clinic (CCBHC) criteria, Behavioral Health Home (BHH), and Commission on Accreditation of Rehabilitation Facilities (CARF) standards. This policy ensures appropriate psychiatric supervision, clinical oversight, and medical leadership at Saginaw County Community Mental Health Authority (SCCMHA).

Policy:
It is the policy of SCCMHA that a qualified Medical Director shall be appointed who is responsible for the clinical oversight of psychiatric and medical services, ensuring compliance with all applicable federal and state laws, regulations, and accreditation standards. The Medical Director shall provide psychiatric supervision, clinical leadership, and direction for the delivery of integrated behavioral health services, including those provided under CCBHC and BHH models.

Application:
This policy applies to the entire SCCMHA Provider Network.

Standards:

A. The Medical Director must be a physician licensed to practice medicine in Michigan, and board-certified or board-eligible in adult and/or child/adolescent psychiatry.

B. The Medical Director must meet all requirements outlined in the Michigan Mental Health Code (MCL 330.1208), MDHHS contract requirements, and CCBHC/BHH certification standards.

C. The Medical Director may delegate specific clinical responsibilities to qualified psychiatric prescribers, consistent with their scope of practice and in compliance with Michigan law.

D. The Medical Director may delegate administrative responsibilities to qualified administrators, consistent with their scope of practice and in compliance with MMHC, MDHHS, CCBHC, and BHH requirements for CMHSP Medical Directors.

E. Responsibilities of the Medical Director:

1. Provide clinical leadership and oversight for all psychiatric and medical services.
2. Ensure compliance with the Michigan Mental Health Code, MDHHS regulations, and CCBHC/BHH requirements.
3. Clinically supervise and support psychiatric prescribers, including nurse practitioners and physician assistants, in accordance with state law and scope of practice.
4. Clinically support registered nurses and other ancillary/medical/healthcare providers in accordance with state law and scope of practice.
5. Develop, implement, and review clinical policies, procedures, and protocols.
6. Develop, implement, and review quality improvement, utilization management, and peer review activities.
7. Oversee the integration of physical and behavioral health services, including care coordination for BHH enrollees.
8. Ensure the provision of 24/7 psychiatric consultation and coverage as required by CCBHC standards.
9. Provide or delegate psychiatric consultation for complex cases, medication management, and diagnostic clarification.
10. Develop, implement, and review staff education, training, and competency assessment.
11. Serve as a liaison with external medical providers, hospitals, and community partners.

12. Participate in regional and state forums for community mental health medical leadership and advise the CEO, management team, and network psychiatrists, of emerging issues, new health care policy, best practices, and public mental health policy from the Michigan Department of Health and Human Services and other sources.

13. Participate in the credentialing of employed/contracted psychiatrists, physician assistants, nurse practitioners and other healthcare providers as well as for the network providers for all SCCMHA-funded programs, as part of the SCCMHA credentialing program.

.

F. The Medical Director shall be consulted by service directors in the development of new program directives, quality assurance measures and process improvements related to the care of persons served and service delivery.

G. The Medical Director shall ensure that legal, accreditation, and regulatory required policies and procedures are in place addressing health and safety and environmental health matters agency-wide, assisting service directors, program supervisors and the SCCMHA Human Resources Director in the interpretation of related issues.

H. The Medical Director shall be available for clinical and administrative consultation for agency business by appointment and as scheduled in accordance with contractual arrangements.

I. All contractual network providers that offer interdisciplinary team services shall provide psychiatric supervision of covered services as required by Medicaid, and contractually by SCCMHA.

Definitions: None

References:

A. Michigan Mental Health Code, Public Act 258 of 1974 as amended, Section: http://www.legislature.mi.gov/(S(k0s2thfrnstxwrw3qtc3bs5n))/mileg.aspx?page=getObject&objectName=mcl-330-1231&highlight=Mental%20Health%20Code330.1231

B. MDHHS/SCCMHA Master Contract

C. Michigan Medicaid Provider Manual: http://www.mdch.state.mi.us/dch-medicaid/manuals/MedicaidProviderManual.pdf

D. SCCMHA Policy 04.01.01 – Quality Improvement Program

E. CCBHC Handbook

F. BHH Handbook

G. CARF accreditation standards

Exhibits:
None

Procedure:
None

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Pest Prevention, Identification and Management</td><td>Chapter: 06 – Management of Health & Safety</td><td>Subject No: 06.03.01</td></tr>
<tr><td rowspan="2">Effective Date:
4/3/17</td><td>Date of Review/Revision:
10/10/23, 10/8/24, 10/14/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Fred Stahl, Director of Human Resources

Authored By:
EOC Sub-Committee

Additional Reviewers:
Environment of Care Committee. Director of Environmental Services, Customer Service & Security</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY
COMMUNITY MENTAL
HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of the Pest Prevention, Identification and Management Policy & Procedure is to provide and maintain, at all service site locations operated by SCCMHA, a safe, clean, pest-free environment.

Policy:
It is the policy of SCCMHA to seek to prevent and mitigate all identified insect/pest infestations to protect the health of customers, employees, contractors, vendors and other visitors to SCCMHA service site locations operated by SCCMHA. All employees and various program site locations must follow the reporting procedures contained in this policy. It will be the responsibility of the SCCMHA Facilities & Custodial Services Department to provide appropriate follow up to address any and all areas of concern at SCCMHA sites. Other SCCMHA network sites are responsible to promptly report, coordinate, and treat as noted in this policy. Upon suspicion of pest/insect reporting, appropriate referral for professional consultation is to take place.

Application:
This policy and procedure applies to all customers, employees, contractors, vendors and other visitors.

Standards:

I. To reduce any potential health hazard.
II. Prevent pests from spreading to the community or properties beyond the suspected/confirmed area of identification.
III. To provide a safe, clean, pest free environment in which individuals may render and/or receive health services.
IV. SCCMHA will provide training to staff on pest prevention and appropriate response.
V. Staff are required to report potential pest concerns to the appropriate parties.

References:
MDCH Michigan Manual for Prevention and Control of Bed Bugs
SCCMHA Employee Handbook

Definition: Use of the term *pest* is intended to include the following: Bed Bugs and Fleas. Other insects, as defined per Professional Exterminator/Pest Control Vendor, are addressed elsewhere in policy, procedure and/or protocol.

Exhibits:
Exhibit A: SCCMHA Pest Response Flow Chart per work locations
Exhibit B: MDCH Don't let Bed Bugs Bite
Exhibit C: University of Minnesota Extension *Let's Beat the Bed Bug* Campaign-Resource
- Have I Found a Bed Bug?
- What Not to do When You have Bed Bugs
- Understanding Bed Bug Treatments
- Bed Bug Control in Residences
- Prevention Tips for Employee's

Exhibit D: Terminex Contract Location Grid

Procedure:

ACTION	RESPONSIBILITY
1. SCCMHA will provide educational in-services, trainings, updates, and any additional necessary information concerning pest prevention and response to all staff.	1. Continuing Education Unit, General Utilities and Custodial Supervisor, Professional Exterminator vendor
2. These educational sessions are to be offered periodically and required annually.	2. Continuing Education Unit, Environment of Care Committee
3. A standard for staff response and reporting is located on the Pest Response Flow Chart for the designated work location (Refer to	3. All Staff

the SCCMHA Employee Handbook #622). All staff is expected to implement the procedures outlined in this policy.	
4. Standards for Supervisors will include education and adherence to policy standards.	4. All Supervisors
5. Standards for facilities and custodial response will be initiated per the Facilities policy and procedure.	5. General Utilities and Custodial Supervisor and Custodial staff
6. Quarterly updates will be provided to the Environment of Care Committee regarding Facilities response actions, outcomes, trends and/or patterns.	6. General Utilities and Custodial Supervisor, Environment of Care Committee, Contract Management Supervisor
7. Random, routine preventative inspections are done by the Custodial Services Department. Locations include: Hancock, A&W, CTN, CTS, FSU, TWL, Salter Place, and Supported Employment.	7. Professional Extermination vendor, Contract Management Supervisor
8. Discontinuation of individual services may be determined on a case by case analysis and only under the direction of the Clinical Services Director and Office of Recipient Rights.	8. Clinical Services Director and/or Office of Recipient Rights
9. Because an infestation can be transmitted via clothing, bags, or other personal items between SCCMHA operated or contracted program/office sites, all providers are expected to be alert for potential infestation. Supervisors of sites where infestation has been transferred or suspected of being transferred must communicate risk between programs where found. Although contractors are responsible for the cost of addressing infestation at their own sites, SCCMHA will	9. All network Supervisors will coordinate containment and treatment efforts within and between program sites. Contracted programs are expected to identify a lead person who is responsible to ensure the infestation is promptly and thoroughly addressed, as well as ensure ongoing prevention and monitoring for such at their program sites. This includes communication with SCCMHA and other community resource sites if an infestation is identified at their

make bed bug information and initial treatment kits available to all contracted programs (or partners) immediately upon request as issued by the SCCMHA Contracts & Properties Unit. In certain situations when landlords may not be responsible, housing assistance benefits can be used for fumigation.	program and before there is any interfacing with these resource sites.

Exhibit A

A & W Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to the lounge behind security.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

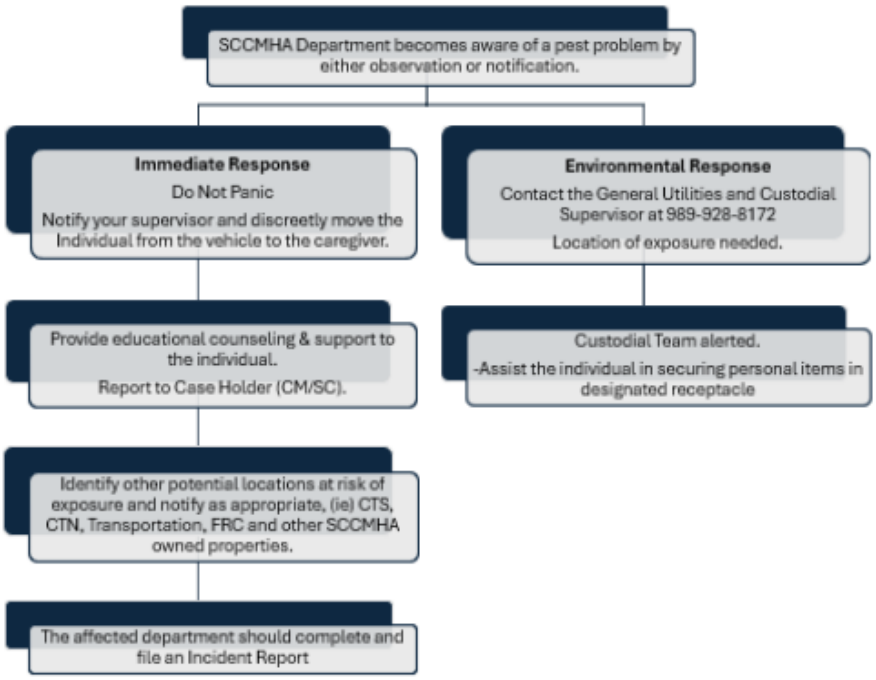
Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Transportation Pest Management Flow Chart



CTN Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to the gym.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

CTS Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to the gym.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Child, Family & Youth Services
Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to room 114.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Supported Employment Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and keep the individual in place.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Hancock Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to a diversion room in CAI/CIS.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Environmental Response

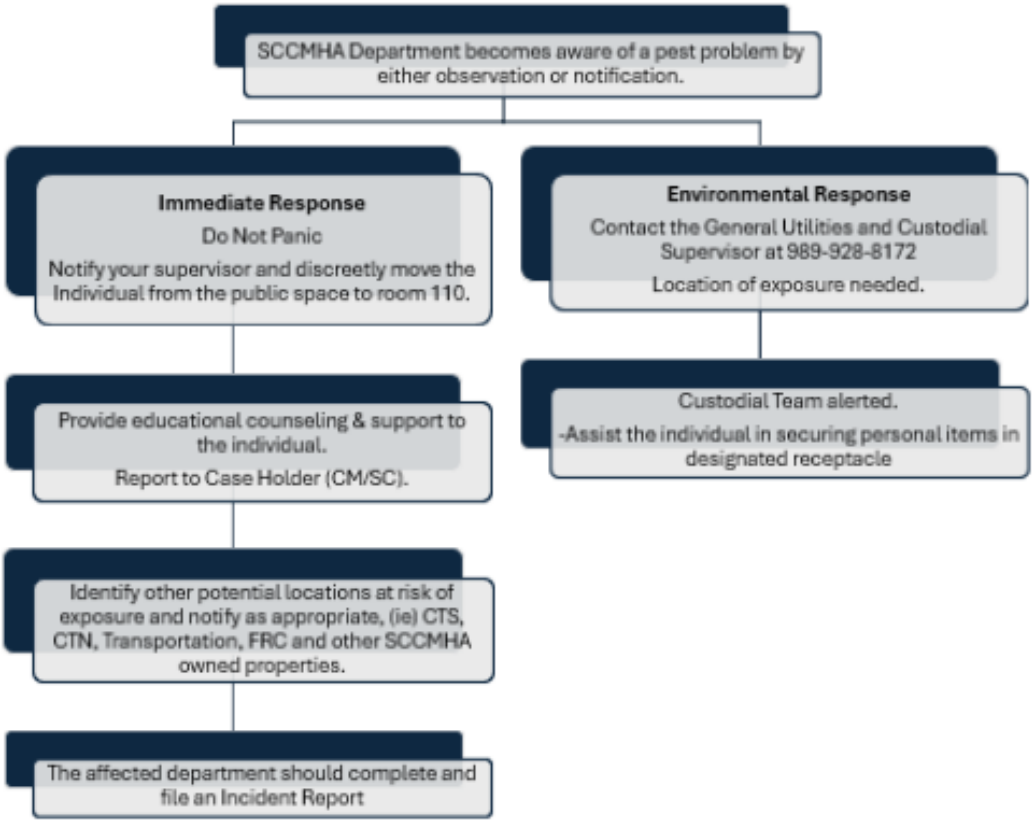
Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Salter Place Pest Management Flow Chart



Towerline Pest Management Flow Chart

SCCMHA Department becomes aware of a pest problem by either observation or notification.

Immediate Response

Do Not Panic

Notify your supervisor and discreetly move the Individual from the public space to room 102.

Environmental Response

Contact the General Utilities and Custodial Supervisor at 989-928-8172

Location of exposure needed.

Provide educational counseling & support to the individual.

Report to Case Holder (CM/SC).

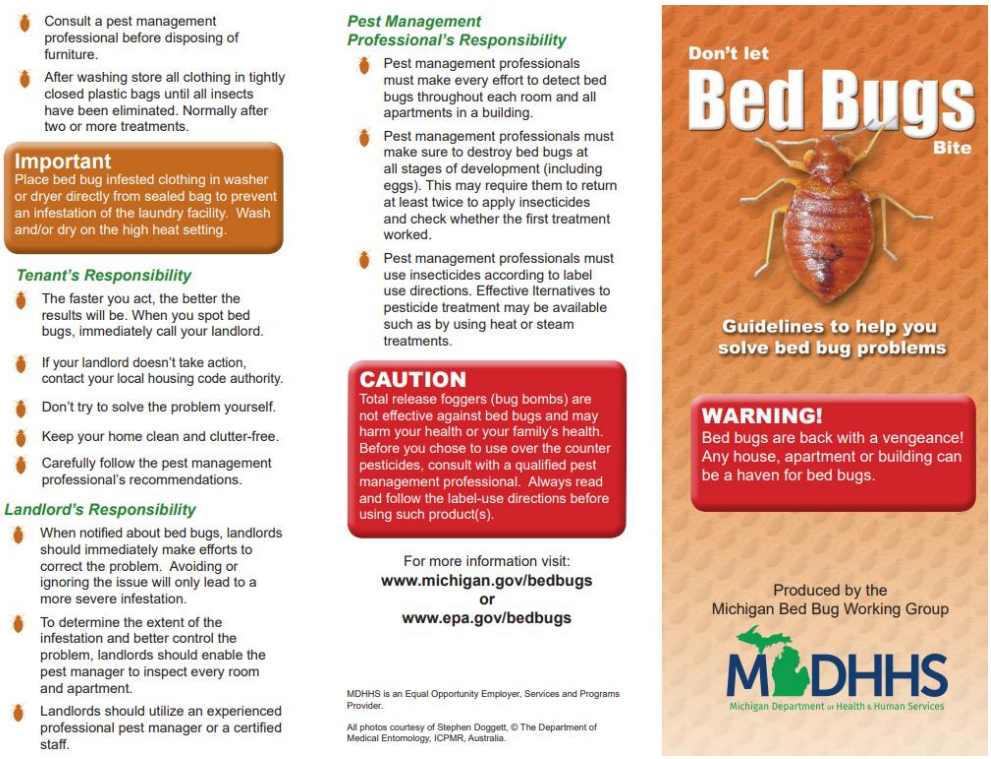
Custodial Team alerted.

-Assist the individual in securing personal items in designated receptacle

Identify other potential locations at risk of exposure and notify as appropriate, (ie) CTS, CTN, Transportation, FRC and other SCCMHA owned properties.

The affected department should complete and file an Incident Report

Exhibit B



- Consult a pest management professional before disposing of furniture.
- After washing store all clothing in tightly closed plastic bags until all insects have been eliminated. Normally after two or more treatments.

Important
Place bed bug infested clothing in washer or dryer directly from sealed bag to prevent an infestation of the laundry facility. Wash and/or dry on the high heat setting.

Tenant's Responsibility

- The faster you act, the better the results will be. When you spot bed bugs, immediately call your landlord.
- If your landlord doesn't take action, contact your local housing code authority.
- Don't try to solve the problem yourself.
- Keep your home clean and clutter-free.
- Carefully follow the pest management professional's recommendations.

Landlord's Responsibility

- When notified about bed bugs, landlords should immediately make efforts to correct the problem. Avoiding or ignoring the issue will only lead to a more severe infestation.
- To determine the extent of the infestation and better control the problem, landlords should enable the pest manager to inspect every room and apartment.
- Landlords should utilize an experienced professional pest manager or a certified staff.

Pest Management Professional's Responsibility

- Pest management professionals must make every effort to detect bed bugs throughout each room and all apartments in a building.
- Pest management professionals must make sure to destroy bed bugs at all stages of development (including eggs). This may require them to return at least twice to apply insecticides and check whether the first treatment worked.
- Pest management professionals must use insecticides according to label use directions. Effective Iternatives to pesticide treatment may be available such as by using heat or steam treatments.

CAUTION
Total release foggers (bug bombs) are not effective against bed bugs and may harm your health or your family's health. Before you chose to use over the counter pesticides, consult with a qualified pest management professional. Always read and follow the label-use directions before using such product(s).

For more information visit:
www.michigan.gov/bedbugs
or
www.epa.gov/bedbugs

MDHHS is an Equal Opportunity Employer, Services and Programs Provider.

All photos courtesy of Stephen Doggett, © The Department of Medical Entomology, ICPMR, Australia.

Don't let
Bed Bugs
Bite

Guidelines to help you solve bed bug problems

WARNING!
Bed bugs are back with a vengeance! Any house, apartment or building can be a haven for bed bugs.

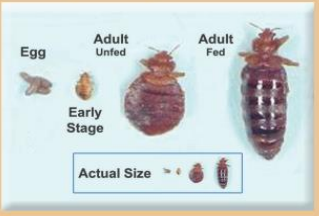
Produced by the
Michigan Bed Bug Working Group

MDHHS
Michigan Department of Health & Human Services

Bed bugs

Bed bugs are small brownish insects. They're about 4 mm long (1/8 in.) and visible to the naked eye. They're active at night and can usually be seen along the seams of mattresses. They feed on human blood.

Bed Bug Life Stages



Bed bug infestations may cause irritating, itchy bite reactions, and anxiety.
Over the past few years, bed bugs have been spreading in large cities worldwide.

How to detect them

Itchy skin and insect bites are clues that you may have bed bugs in your home. You'll usually see three or four bites in a straight line or grouped together. Exposed areas of your arms, legs and back are more susceptible to bites. Also look for small black stains "blood spots" on your sheets, pillows, or mattress seams. Bed bugs may also be hiding in cracks and crevices in your furniture.

How they spread

Bed bugs are usually brought into your home in suitcases and handbags and on clothing and furniture, especially previously used mattresses and other items.

They can also travel between apartments in a building. There's no need to be embarrassed if these bugs end up moving in with you. Bed bugs are not necessarily associated with dirty environments, but they flourish in clutter.

How To Prevent Them

Vacuum your home regularly. If you do have bed bugs, make sure you close the vacuum bag tightly and dispose of it outside your home.

Avoid picking up used mattresses or second-hand upholstered furniture because it's hard to see whether they harbor bed bugs.

Other used furniture must be carefully inspected and cleaned before you bring it home. Scrub furniture with soapy water or a household cleaning product to remove any possible bed bugs or their eggs.

Second-hand clothing should be placed in a sealed, plastic bag and emptied directly into the washing machine. Wash in hot water and dry on hot setting to kill bed bugs and their eggs.

When visiting hotels inspect the room for signs of bed bugs prior to unpacking luggage.

Important
Avoid bringing home discarded furniture, it may be infested with bed bugs. Also inspect any used item for bed bugs before bringing it into your home.

Pest Management

To ensure successful treatment, your cooperation and that of your landlord and the pest management professional are key.

The important thing is to act fast. As soon as you see these bugs, call your landlord, who will then contact a qualified, licensed pest management professional.

Preparing your home for the pest management professional

This step is extremely important. Closely follow the pest management professional's guidelines. Below are a few tips to keep in mind.

- Remove clutter as it provides hiding places for bed bugs.
- Place all bedding (sheets, mattress covers, bedspreads) in a sealed, plastic bag. Wash and/or dry bedding on high heat setting.
- Vacuum and dispose of the vacuum bag (outside the home). If a bagless vacuum is used, deposit all contents of the container into a plastic bag, seal and dispose of outside. Rinse collection container outside before re-attaching to vacuum.
- Empty dresser drawers and closets and place contents in a sealed, plastic bag. Wash and/or dry clothes on high heat setting.
- Don't bring home new furniture until bed bugs are eliminated.

Exhibit C

Let's Beat the Bug!

In Short:

- Bed bugs may have different shapes and sizes
- Bed bugs are small insects, about the size of an apple seed.
- Look for bed bugs , fecal spots and skins
- Bed bugs are night feeders, but sometimes feed during the day
- How can I tell that I found a bed bug
- What to do if I find a bed bug

For more information contact the Bed Bug *InformationLine* at 612-624-2200, 1-855-644-2200, bedbugs@umn.edu, or visit www.bedbugs.umn.edu

Have I Found a Bed Bug?

Bed bugs can be difficult to identify as they are similar to many other small insects. Also, their appearance will change depending on their age and if they have recently eaten.

Adult bed bugs are reddish brown in color and approximately ¼ to 3/8 inch long; they are nearly as wide as they are long. They are about the size of an apple seed. Juvenile bed bugs can be very small and very hard to see.

Bed bugs do not have wings, and cannot fly. Bed Bugs can move very quickly on both horizontal and vertical surfaces

If a bed bug has not recently eaten it is flat and oval shaped. Once a bed bug has bitten someone it swells in size, becoming longer and redder in color; frequently compared to the shape of a cigar.

If you have a bed bug infestation you may also notice cast skins. The cast skin of a bed bug is an empty shell that is left behind when a bed bug grows. This skin will be in the shape of a bed bug but it will be transparent.

Bed bugs are active mainly at night, so it is unlikely that you will see one during the day. They can become accustomed to feeding during the day if they become aware that people are resting or sleeping during the day. Bed bugs may be seen during the day if there is a big infestation, or if the insect you have found is actually a bat bug. Bat Bugs are very similar to bed bugs and are often found in places with bats or birds. Bugs should be sent to a professional for identification.

If you think you have found a bed bug, try to catch it on a piece of tape or put it in a plastic bag, you can then have this bug identified by a pest management professional (exterminator).

If an exterminator cannot verify it is a bed bug, send a sample on sticky tape to:

Bed Bug *InformationLine*
Rm 219 Hodson Hall
1980 Folwell Ave
St. Paul, MN 55108

If you find bed bugs, make a note of when and where you saw them. This will help the pest management professional in the inspection of your home and will increase the likeliness that treatment will be effective.

By Amelia Shindelar and Dr. Stephen Kells, 2011
Funding for "Let's Beat the Bug" Campaign provided by the United States Environmental Protection Agency and MDA. Additional assistance from the Minnesota Department of Health was greatly appreciated.

Updated on May 27, 2014

Let's Beat the Bug!

Bed Bug Basics

- Bed bugs are small insects, about the size of an apple seed. Adult bed bugs are flat, oval and reddish-brown in color. Juvenile bed bugs can be very small and hard to see.
- Bed bugs feed on human blood and can live for over a year without a meal.
- Bed bugs usually hide during the day near where people rest or sleep and then come out at night to feed. Bed bugs do not live on our bodies.
- Some people do not react when bitten by a bed bug.
- Most bed bugs are found within 8 feet of a person's resting place. As the infestation grows, bed bugs will spread further. You can find bed bugs in any of the following places:
  - In mattresses, box springs, bed frames, and bedding
  - In the cracks and crevices of furniture
  - Behind peeling wall paper
  - Behind pictures and clocks
  - In curtains
  - In cracks in hardwood floors
  - Under carpeting
  - Behind electrical outlets or switch plates

For more information contact the Bed Bug *InformationLine* at 612-624-2200, 1-855-644-2200 bedbugs@umn.edu, or visit www.bedbugs.umn.edu

What NOT to Do When You have Bed Bugs

- ⊗ Do not Panic. You can control bed bugs with careful inspection and by using proper control methods.
- ⊗ Do not try to kill bed bugs by using agricultural or garden pesticides. Using outdoor pesticides to control bed bugs can make you or your family very sick.
- ⊗ Do not use products that appear to be "homemade" or "custom formulated." Homemade products could be dangerous and they might make the problem worse.
- ⊗ Do not use products that have labels in a language other than English.
- ⊗ Do not apply pesticides directly to your body. This could make you very sick.
- ⊗ Do not use rubbing alcohol, kerosene or gasoline. These chemicals may cause fires.
- ⊗ Do not throw away your furniture. Beds and other furniture can be treated for bed bugs. Throwing away your furniture can spread the bugs and you have to buy new furniture.
- ⊗ Do not store things under the bed. Storing stuff under the bed gives bed bugs many new places to hide. This makes it more difficult to get rid of bed bugs.
- ⊗ Do not move things from room to room. Moving your things from the room with bed bugs to another room in your house may spread the bed bugs.
- ⊗ Do not wrap items in black plastic and place in the sun. It will not get hot enough to kill all the bugs.

Things you can do if you think you have bed bugs:

- ☑ Make sure it is a bedbug; see the factsheet *"Have I found a Bed Bug?"* at www.bedbugs.umn.edu/have-i-found-a-bed-bug
- ☑ Contact a Pest Management Professional or your landlord.
- ☑ Take steps to control the infestation; see the factsheet *"Bed Bug Control in Residences"* at www.bedbugs.umn.edu/bed-bug-control-in-residences

Updated on March 6, 2015

By Amelia Shindelar and Dr. Stephen Kells, 2011
Funding for "Let's Beat the Bug" Campaign provided by the United States Environmental Protection Agency and MDA. Additional assistance from the Minnesota Department of Health was greatly appreciated.

MINNESOTA DEPARTMENT OF AGRICULTURE
www.mda.state.mn.us

UNIVERSITY OF MINNESOTA EXTENSION

Let's Beat the Bug!

Bed Bug Basics

- Bed bugs are small insects, about the size of an apple seed. Adult bed bugs are flat, oval and reddish-brown in color. Juvenile bed bugs can be very small and hard to see.
- Bed bugs feed on human blood and can live for over a year without a meal.
- Bed bugs usually hide during the day near where people rest or sleep and then come out at night to feed. Bed bugs do not live on our bodies.
- Some people do not react when bitten by a bed bug.
- Most bed bugs are found within 8 feet of a person's resting place. As the infestation grows, bed bugs will spread further. You can find bed bugs in any of the following places:
  - In mattresses, box springs, bed frames, and bedding
  - In the cracks and crevices of furniture
  - Behind peeling wall paper
  - Behind pictures and clocks
  - In curtains
  - In cracks in hardwood floors
  - Under carpeting
  - Behind electrical outlets or switch plates

For more information contact the Bed Bug *InformationLine* at 612-624-2200, 1-855-644-2200 bedbugs@umn.edu, or visit www.bedbugs.umn.edu

Understanding Bed Bug Treatments

There are a number of options to effectively get rid of bed bugs, but sometimes it can get confusing when trying to decide which option would be best for your situation. Here is some basic information regarding the two most common methods used by pest management companies to kill bed bugs.

Whole Room Heat Treatments

Whole room heat treatments involve a Pest Management Professional (PMP) bringing in specially designed equipment to raise the temperature in your home to kill the bed bugs. Bed bugs and eggs die within 90 minutes at 118°F (48°C) or immediately at 122°F (50°C). During a heat treatment, the air temperature in the room is typically between 135°F (57.2°C) and 145°F (62.7 °C). The PMP will place remote thermometers throughout the home, to make sure the right temperatures are reached. The PMP watches the thermometers closely to ensure that it gets hot enough to kill bedbugs. A heat treatment typically takes between six and eight hours, depending on the condition of the area being treated.

During the heat treatment pets and any heat sensitive items that may melt or be damaged at temperatures up to 150°F degrees should be removed from the area being treated. Make sure you discuss this with your PMP as anything not treated with heat will need to be treated in another way.

Heat treatments do not offer any residual effects and your home could quickly become reinfested after a heat treatment if prevention steps are not taken.

Often, a residual insecticide will be applied to the border of the home/room being treated for bed bugs as a prevention step.

Let's Beat the Bug!

Insecticide Treatments

Insecticide treatments that are conducted thoroughly and correctly by a licensed PMP can be a very effective way of controlling bed bugs. Three different types of insecticides should be used in order to achieve the best result. There are many different brands of insecticides but one of each of the following broad categories should be used.

- A fast-acting, contact insecticide for use on surfaces that we frequently touch, i.e. sofas.
- A residual insecticide for inside furniture, cracks and crevices and the underside of surfaces we touch.
- A dust insecticide for cracks, crevices and voids, such as electrical outlets and baseboards.

Your PMP may offer other services such as container heat treatments, steam applications, or freezing infested items. Usually, items treated with these optional controls do not require an insecticide treatment and therefore fewer insecticides are needed.

A thorough insecticide treatment should involve 2-3 visits from the PMP, as it is unlikely all the bed bugs will be killed in the initial treatment. An insecticide treatment typically takes about 30 minutes to 2 hours per room depending on size and condition of the room. Once the treatment is complete you should wait until all the insecticides have dried before reentering your home, or until the PMP says it is safe to re-enter.

Before any treatment the PMP should provide you with a detailed list of instructions for how to prepare your home. It is very important to follow these directions closely as properly preparing the home is a very important step in any treatment process. Improper preparation is one of the main reasons that treatment for bed bugs fail.

We strongly recommend against trying to conduct an insecticide treatment for bed bugs by yourself. Controlling bed bugs with insecticides is a challenging and time consuming process which requires expertise and in many states a license is required to apply the insecticides which kill bed bugs. The insecticides that can be purchased in a hardware store, such as foggers, are not effective in controlling bed bugs and we strongly recommend against their use.

Updated on May 28, 2014

By Amelia Shindelar and Dr. Stephen Kells, 2013
Funding for "Let's Beat the Bug" Campaign provided by the United States Environmental Protection Agency and MDA. Additional assistance from the Minnesota Department of Health was greatly appreciated.

Let's Beat the Bug!

Bed Bug Control in Residences

Bed Bug Basics

- Bed bugs are small insects, about the size of an apple seed. Adult bed bugs are flat, oval and reddish-brown in color. Juvenile bed bugs can be very small and hard to see.
- Bed bugs feed on human blood and can live for over a year without a meal.
- Bed bugs usually hide during the day near where people rest or sleep and then come out at night to feed. Bed bugs do not live on our bodies.
- Some people do not react when bitten by a bed bug.
- Most bed bugs are found within 8 feet of a person's resting place. As the infestation grows, bed bugs will spread further. You can find bed bugs in any of the following places:
  - In mattresses, box springs, bed frames, and bedding
  - In the cracks and crevices of furniture
  - Behind peeling wall paper
  - Behind pictures and clocks
  - In curtains
  - In cracks in hardwood floors
  - Under carpeting
  - Behind electrical outlets or switch plates

For more information contact the Bed Bug *InformationLine* at 612-624-2200, 1-855-644-2200 bedbugs@umn.edu, or visit www.bedbugs.umn.edu

When trying to control bed bugs in your home:

- ***DO NOT*** use pesticides meant for garden or agricultural use.
- ***DO NOT*** use products that appear to be "homemade" or "custom formulated" or products purchased from someone without a license.

The most effective way to control bed bugs in your home is through a combination of chemical measures and heat treatments applied by a Pest Management Professional (PMP). Unfortunately, the service of a PMP can be costly. So we are providing information on how to control a bed bug infestation on your own.

Controlling bed bugs by yourself is very difficult and time consuming. It involves moving furniture, household goods and personal items. Plan how you want to treat each room. Set up a "clean zone".

How to set up a "Clean Zone"?

- ✓ Start with corners and edges of an open wall, dig things out of cracks and crevices with a plastic card.
- ✓ Inspect and clean along all cracks and crevices
- ✓ You can use a damp cloth or mop to clean if you have bare tile or wood floors, otherwise vacuum thoroughly
- ✓ Don't forget to clean pictures and other wall hangings
- ✓ Inspect other items and put them into the clean zone
- ✓ Sort clothes, bedding, and other items that can be laundered into plastic bags for future laundering, as this can be very effective to treat infested items.
- ✓ See http://www.bedbugs.umn.edu/bed-bug-control-in-residences/controlling-bed-bugs-by-hand/ for more details on setting up a clean zone.

Killing bed bugs by hand is not 100% effective but will help you reduce the number of bugs in your home. You can capture and squash them or capture them on sticky tape and throw away the tape.

Tools for hunting and destroying bed bugs: Flashlight, old credit card (or similar) clear tape, plastic bags, a cloth and hot soapy water.

Steps: Use the flashlight and a credit card to search out bed bugs by moving the card along cracks and crevices to push out the bugs. Use the sticky tape to trap the bugs. Use the hot soapy water to wipe up infestations, the bugs, blood stains, droppings, eggs and shed skins.

Vacuuming helps to quickly capture and contain bed bugs. Vacuum crevices around baseboards, electronic items (such as TVs and stereos) and any other likely hiding places, such as beds, couches, bedframes, and dressers. If using a canister vacuum, immediately empty the contents into a plastic bag, seal and throw away. Clean the

Exhibit D

FY26 SCCMHA Locations Serviced by Terminix

2723 State St. (HRC)
3830 Lamson St. (CTN)
3875 Bay Road Suite 7N & 4S
1 Germania Platz (A&W)
1901 Maple St.
500 Hancock St.
2720 W. Genesee (Drop-In)
1040 N. Towerline Rd.

Updated 10/20/2025

Environment of Care/Health/Safety

Pest Prevention Tips for SCCMHA Employee's

All SCCMHA Employee's are encouraged to follow the recommendations below in an effort to reduce the risk of transmission during work assignments and tasks.

1. Know or ask ahead of a visit/entering the home if the space has a pest problem
2. Protective foot covering will be available for all staff whose daily assignments/tasks are required to provide services in customer homes. Foot coverings are to be applied upon entering the home, not in staff vehicle. Remove and dispose of immediately upon exit.
3. It is recommended staff wear light colored clothing as this will enhance visual inspection prior to entering your vehicle.
4. You may choose to have a hand mirror in your vehicle to aid with visual inspection of your clothing prior to entering your vehicle.
5. It is recommended you take into the home only those supplies you absolutely need to complete your job duties.
6. Do not place bags, brief cases, totes, or other personal items in the floor of a residence of other building. Many pests are hitch-hikers and may travel on your mishandled items.
7. Do not sit on upholstered furniture. Recommendation in to stand whenever possible if you need to sit, do so on hard surface only after a quick visual inspection.
8. You may choose to keep a change of clothing available if needed.
9. For additional prevention tips/recommendations, please refer to the exhibits attached to this policy.

Tab 5

Regulatory Management/ HIPAA Compliance

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Compliance and Ethics Program - Corporate Compliance Plan (CCP)</td><td>Chapter: 05 - Organizational Management</td><td>Subject No: 05.07.01</td></tr>
<tr><td>Effective Date:
August 15, 2002</td><td>Date of Review/Revision:
8/15/05, 3/9/06, 8/7/06, 7/7/09, 8/10/15, 5/9/16 3/15/17, 6/1/18, 6/11/19, 8/1/21, 8/26/22, 6/23/23, 7/9/24,10/14/25
Supersedes:</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers:
Kentera Patterson, Officer of Recipient Rights and Compliance</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure that Saginaw County Community Mental Health Authority (SCCMHA) conducts all aspects of service delivery and administration with integrity, in conformance with the highest standards of accountability and applicable laws, while utilizing sound business practices, through the development of and adherence to the SCCMHA Corporate Compliance Plan (CCP), guaranteeing the highest standards of excellence.

Policy:

A. Corporate Compliance

1. **Follow the Law:** SCCMHA shall establish, implement, and maintain a Corporate Compliance Plan that is in accordance with federal and state statutes, laws, and regulations. SCCMHA will furthermore adhere to regulations required by:
   a. The Mid-State Health Network (MSHN)
   b. The Michigan Department of Health and Human Services (MDHHS)
   c. The Michigan Attorney General's Office

d. Office of Inspector General (OIG)
e. Centers for Medicaid and Medicare Services (CMS)
f. Any accreditation agencies (like CARF or The Joint Commission)
- U.S. Department of Justice (DOJ)

2. **Purpose of the CCP:** The SCCMHA Corporate Compliance Plan provides the framework for SCCMHA to comply with:
   a. Applicable laws, regulations, and program requirements
   b. Minimize organizational risk
   c. Maintain strong internal controls
   d. Encourage the highest level of ethical and legal behavior.

3. **Preventing Fraud, Waste, & Abuse:** SCCMHA shall maintain policies and procedures necessary to comply with the SCCMHA CCP and shall ensure effective processes for:
   a. Identifying and reporting suspected fraud, abuse, and waste
   b. Respond quickly to detected offenses
   c. Take appropriate corrective action, including the reporting thereof to the SCCMHA Chief Executive Officer.

4. **Compliance Officers and Team:** SCCMHA shall identify a Chief Compliance Officer, a Compliance Officer, and a Compliance and Policy Team. They are responsible for making sure SCCMHA follows the CCP.

5. **Training Staff:** SCCMHA shall provide staff training on compliance with the SCCMHA CCP and will maintain records of staff attendance. Training courses shall include but are not limited to:
   a. Federal False Claims Act
   b. Michigan False Claims Act
   c. Whistleblowers Protection Act
   d. Advance Directives
   e. Consumer Privacy Protections.

6. **Compliance with Rules:** SCCMHA shall require all Board members, employees, and contractors to comply with the CCP and report an violations to the right people or agencies.

7. **Annual Review:** SCCMHA shall review its compliance activities at least annually and will participate in an annual review of the SCCMHA CCP and provide recommendations for revisions as needed.

B. Ethical Standards/Program Integrity

1. **Standards of Conduct:** All services within SCCMHA shall be provided with commitment to appropriate business, professional, and community standards for ethical behavior.

2. **Written Standards of Conduct:** SCCMHA shall develop and maintain Standards of Conduct applicable to all SCCMHA staff. These will help guide proper behavior in all roles.
3. **Use of Resources:** SCCMHA shall conduct business with integrity and not engage in inappropriate use of public resources.
4. **Protecting People Served:** SCCMHA shall ensure that services are provided in a manner that maximizes benefit to persons served while avoiding risk of physical, emotional, social, spiritual, psychological, or financial harm.
5. **Avoiding Conflicts of Interest:** All SCCMHA staff shall conduct themselves in such a way as to avoid situations where prejudice, bias, or opportunity for personal or financial gain, could influence, or have the appearance of influencing, professional decisions.
6. **Support for Compliance Leaders:** Those individuals with "day-to-day operational responsibility" for the Compliance and Ethics Program will:
    a. Be provided with adequate resources and authority they need
    b. Have direct access to the operational and governing authority of SCCMHA.

Application:
This policy applies to all SCCMHA employees, board members, contractors, and network providers, including those who work directly for the board or are contracted to provide services to people served.

Standards:
None

Definitions:
None

References:
- Federal False Claims Act (31 U.S.C. §§ 3729–3733)
- Michigan False Claims Act (MCL 400.601 et seq.)
- Whistleblowers Protection Act (MCL 15.361 et seq.)
- 42 C.F.R. §§ 438.608 and 455.2 (Compliance Program Requirements)
- MSHN Compliance Requirements
- MDHHS Medicaid Contract Requirements

Exhibits:
None

Procedure:
None

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: SCCMHA Network HIPAA Compliance</td><td>Chapter: 05 - Organizational Management</td><td>Subject No: 05.07.02</td></tr>
<tr><td>Effective Date:
June 1, 2005</td><td>Date of Review/Revision:
8/2/05, 6/23/09, 6/7/12, 6/3/14, 5/6/16, 6/13/17, 7/5/18, 7/1/20, 8/1/21, 8/26/22, 6/26/23, 9/9/24,10/14/25
Supersedes:</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Jennifer Keilitz, Director of Network Services, Public Policy & Continuing Ed

Additional Reviewers:
Kentera Patterson, Officer of Recipient Rights and Compliance / HIPAA Privacy Officer</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure that all SCCMHA service staff and network providers understand and adhere to the full scope of the Health Insurance Portability and Accountability Act (HIPAA) regulations, including security, electronic transaction, and privacy requirements.

To provide a general broad HIPAA policy that will direct varied network providers in compliance with HIPAA requirements.

Policy:
1. **SCCMHA is a "Covered Entity" as defined by HIPAA**. This means all staff and providers must follow federal rules to protect the privacy and security of health information for the people we serve. All staff, programs and providers, must follow current HIPAA regulations as part of their employment and contractual obligation.

2. **Authentication & Access Control Policy Compliance:** To safeguard the confidentiality, integrity, and availability of electronic protected health information (ePHI), all users accessing SCCMHA-managed information systems must comply with SCCMHA's authentication and access control requirements.

a. All network users must use unique usernames and strong passwords that meet SCCMHA's complexity standards, including minimum character length and a combination of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed regularly to reduce the risk of compromise.
b. In alignment with HIPAA Security Rule requirements and SCCMHA security protocols, Multi-Factor Authentication (MFA) is required for all systems that handle or provide access to ePHI and other sensitive data.

3. **User Authentication Auditing:** All authentication activities are subject to ongoing auditing and monitoring to detect unauthorized access and ensure compliance.

Application:
This applies to SCCMHA network providers, business associates, and any subcontractor that is required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own policy and procedure which complies with the applicable section of the HIPAA Security Rule.

Standards:

A. **HIPAA Training:** SCCMHA will make routine HIPAA training available. All staff and providers must complete training in both HIPAA privacy and security as required from SCCMHA to comply.
B. **HIPAA Officers:** SCCMHA has two HIPAA required officers appointed by the CEO who are responsible to oversee HIPAA compliance:
    a. SCCMHA HIPAA Security Officer
    b. SCCMHA HIPAA Privacy Officer.
    c. SCCMHA HIPAA officers are available for staff or provider consultation on HIPAA related matters.
C. **Privacy Contacts at Provider Sites:** Business Associates and Contractual providers who are a ‘covered entity’ according to HIPAA regulations, as is SCCMHA, are expected to identify their HIPAA Privacy Officer to SCCMHA; all other service contractors are asked to identify a ‘privacy liaison’ to SCCMHA.
D. **Provider Manual:** SCCMHA will include all relevant HIPAA policies in the SCCMHA Network Services Provider Manual.
E. **Provider Policies:** Business Associates and Contractual providers who are covered entities are expected to have appropriate and required HIPAA policies and procedures that are available for SCCMHA review by audit and compliance individuals.
F. **HIPAA Transaction Rules:** Providers who conduct or purchase electronic billing must abide by HIPAA transaction requirements.
G. **Non-Covered Providers:** Providers who are not covered entities are expected to be familiar with and adhere to SCCMHA HIPAA policies as applicable to their service provision.
H. **HIPAA Questions:** Providers will direct HIPAA compliance related questions to SCCMHA whenever indicated or appropriate.

I. **Protecting Health Information:** Providers must make every reasonable effort to protect the privacy and security of protected information of people served as defined and required in HIPAA regulations.
J. **Reporting Violations:** Providers are expected to promptly report HIPAA violations to SCCMHA regarding SCCMHA recipients of services and assist with any remedy.
K. **Consequences of Non-Compliance:** Providers may be sanctioned by SCCMHA for non-compliance on HIPAA-related requirements.
L. **Using and Sharing PHI:** Primary providers and record holders must abide by SCCMHA policies (or their own comparable policies that meet HIPAA requirements) in the notice, use and disclosure of all protected health information.
M. **Ongoing Guidance:** SCCMHA will offer HIPAA-related guidance for network providers.
N. **"Protecting Personal Health Information (PHI) in Email"** Exhibit must be fully complied with.

Definitions:
See SCCMHA Policy 08.05.00.01 – Compliance Definitions policy

References:
All SCCMHA HIPAA related Policies and Procedures
SCCMHA Regulatory Management Policy
SCCMHA Competency Requirements for the SCCMHA Network, Policy 05.06.03

Exhibits
Protecting Personal Health Information (PHI) in Email

Procedure:
None

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Protecting Personal Health Information (PHI) in email

Saginaw County Community Mental Health Authority (SCCMHA) is committed to keeping all personal health information (PHI) safe, private and confidential. This includes PHI shared or referenced in **email communications**. All SCCMHA staff and contracted providers must follow these standards to comply with **HIPAA Privacy and Security Rules** and SCCMHA policy.

What You Must Do

1. **Use the secure Sentri II messaging system whenever possible** to share information about persons served with contracted providers.
    - Sentri II messaging is the **preferred** and **most secure** method of communication for PHI.
    - If you need help using Sentri messaging, ask your **supervisor** or **SCCMHA IT**.

2. **If Sentri II messaging is not available**, you may use one of the following **secure methods**:
    - Encrypted email (contact IT for setup assistance)
    - Fax
    - USPS mail delivery
    - Hand delivery
    - Secure voicemail (if appropriate and limited to minimal PHI)
    - TigerConnect secure text messaging

3. **For internal SCCMHA or contracted organization emails that include PHI:**
    - Add the subject line phrase **"PHI Content Caution: "**.
    - Do **not** include any PHI in the subject line itself, especially names.
    - This alerts others to handle the message carefully and not to forward it externally.

4. **Use PHI in internal emails only when necessary** and based on the **"need to know"** and **"minimum necessary"** principles.
    - Include only the minimum amount of PHI required for the communication.
    - When possible, identify the individual using their **Sentri case number** instead of their name or initials.

5. **All emails containing PHI must be treated as private and confidential**, even if they contain only limited or basic identifying details.

What You Must Not Do

1. **Never include the name of a person served or any PHI in external emails** (emails sent outside the SCCMHA Outlook system).
    - This includes any **attachments** that contain PHI.

- *External* includes communication with **contract providers or other agencies**, even when they have a legitimate business need for the information.

2. **Even with a signed release**, do not send PHI in an external email unless the message or attachment is **encrypted**.
   - A release of information does **not** override SCCMHA's security requirements.

1. **Do not forward emails containing PHI outside SCCMHA**, especially if you did not write the original message.
   - PHI may be hidden in **attachments**, **email chains**, or prior message content.
   - Forwarding such an email externally without encryption or to unauthorized recipients constitutes a **HIPAA Security Rule violation**.

2. **Do not include PHI in the subject line** of any email.

3. **Do not assume it is acceptable to email PHI** simply because the recipient has access to other records.
   - Always confirm both **authorization** and **secure transmission method** before sending.

Be Aware

1. **Protected Health Information (PHI)** includes any detail that could identify an individual when linked to health data.
   Under HIPAA, these **18 identifiers** make health information "protected":
   Note: Any one of these identifiers, when linked with health information, qualifies as PHI. Using multiple identifiers increases the risk of a breach.

   Personal & Geographical Identifiers
   1. Names
   2. Street address, city, county, precinct, ZIP code (any subdivision smaller than a state)
   3. All dates related to an individual (birth, admission, discharge, death, etc.)
   4. Ages over 89 (must be grouped as "90 or older")

   Contact & Digital Identifiers
   5. Telephone or fax numbers
   6. Email addresses
   7. Web URLs
   8. IP addresses

   Financial & Professional Identifiers
   9. Social Security numbers
   10. Medical record numbers
   11. Health plan beneficiary numbers

12. Account numbers
13. Certificate or license numbers

Device & Biometric Identifiers

14. Vehicle identifiers or license plate numbers
15. Device identifiers or serial numbers (e.g., MAC, IMEI, ESN)
16. Biometric identifiers (fingerprints, retina scans, voiceprints)
17. Full-face photographic or comparable images

Any other unique identifying number, characteristic, or code

18. This refers to any code, characteristic, or combination of information that could be used to uniquely identify an individual.

2. **Emails are not part of the official health record.**
   - Service notes, plans, and progress must be entered into **Sentri II**.
   - If an email contains important details that should be included in the health record, the **author of the email** must summarize and document it in Sentri II.
   - Other recipients should not copy or enter the content on the author's behalf.

3. **Sentri II messages are part of the medical record.**
   - Treat all Sentri II messages containing PHI with the same privacy and confidentiality standards as the rest of the record.

4. **Information related to treatment, payment, or service delivery** must always be sent via **Sentri II** or **encrypted Outlook email**.
   - The Sentri II messaging module is the **preferred** method.
   - Keep messages brief and limited to necessary PHI.
   - Never include PHI in the email subject line.

5. **If you observe or suspect inappropriate or questionable PHI email use**, report it immediately.
   - Contact the **SCCMHA Office of Recipient Rights and Compliance** or the **Chief Quality & Compliance Officer**.
   - You may also report anonymously through the **Rights and Compliance Hotlines**.

Final Reminders

- HIPAA and SCCMHA violations may result in **employee discipline** and/or **provider sanctions**.
- Always follow the principles of **minimum necessary** and **secure communication**.
- When in doubt, **ask before you send.**
  - Contact your **supervisor**, the **Privacy Officer**, or the **Security Officer** for guidance.
- Protecting PHI protects **our persons served**, **our agency**, and **you**.

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Reporting of Medicaid Fraud, Waste, and/or Abuse</td><td>Chapter: 05 - Organizational Management</td><td>Subject No: 05.07.05</td></tr>
<tr><td rowspan="2">Effective Date:
August 6, 2015</td><td>Date of Review/Revision:
3/15/17, 6/1/18, 6/11/19, 8/1/21, 8/26/22, 6/23/23, 7/9/24, 10/14/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Kentera Patterson, Officer of Recipient Rights and Compliance

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
Saginaw County Community Mental Health Authority (SCCMHA) will maintain a process to collect information about the nature of fraud, waste, and abuse complaints, as well as maintain a process to report to the Mid-State Health Network information regarding the complaints of fraud, waste, and abuse that warrant investigations.

Policy:
It is the policy of SCCMHA to collect information about the nature of fraud, waste, and abuse complaints, and to report to Mid-State Health Network on a semi-annual basis any suspicion of fraud, waste, or abuse within the Medicaid program.

Application:
This policy applies to all provider network members, including contracted and direct board operated service programs that provide services to persons served.

Standards:

1. **Information to Be Collected:** SCCMHA will collect information about the nature of fraud, waste, and abuse complaints which will include:
    a. The **name** of the individual(s) or entity involved in suspected fraud, waste, or abuse
    b. The **address** of the individual(s) or entity involved in suspected fraud, waste, or abuse

c. The **telephone number** of (or other contact information for) the individual(s) or entity involved in the suspected fraud, waste, or abuse
d. The **Medicaid identification** number and/or any other identifying information.
e. The source of the complaint of the suspected fraud, waste, or abuse,
f. The nature of the complaint of the suspected fraud, waste, or abuse,
g. The type of provider involved in the suspected fraud, waste, or abuse,
h. The approximate number of dollars involved in the suspected fraud, waste, or abuse,
i. The legal or administrative disposition of the case including actions taken by law enforcement officials to whom the case has been referred.

2. **Reporting to Mid-State Health Network:** SCCMHA will report semi-annually (on or about April 1 and October 1) to Mid-State Health network regarding the complaints of fraud, waste, and abuse made to SCCMHA that warrant investigation.

Definitions:
None

References:
None

Exhibits:
Exhibit A - SCCMHA Health Care Fraud Hot Line Poster

Procedure:

ACTION	RESPONSIBILITY
Written Policies, Procedures and Standards of Conduct:	
1. SCCMHA maintains a Health Care Fraud Hot Line telephone number to facilitate the reception of notification of suspected fraud, waste, or abuse occurrences. This contact opportunity (local number as well as toll free number) is one of several avenues available for SCCMHA employees, Network Providers, people served, or general public to report instances of suspected health care fraud, waste, or abuse to SCCMHA.	SCCMHA Compliance Officer or the Quality & Medical Records Supervisor if not available
2. SCCMHA will collect and maintain information about the nature of fraud,	SCCMHA Compliance Officer

waste, and abuse complaints which include the information listed under Standard 1 items a-i.	
3. SCCMHA will report to Mid-State Health Network on a semi-annual basis the information maintained under Standard 1 items a-i.	SCCMHA Compliance Officer

Exhibit A


Saginaw County
Community Mental
Health Authority
Report
Health Care Fraud
Report fraud and/or misconduct relating
to Medicare or Medicaid Services
If you know, or have a good faith suspicion,
that fraud or misconduct relating to
Medicare or Medicaid has been committed,
contact the SCCMHA hotline.
SCCMHA has a no retaliation policy.
SCCMHA Hotline: 855-797-3417
Local Phone: 989-797-3574
SCCMHA Compliance Office
500 Hancock Street
Saginaw, MI 48602

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Break the Glass Policy</td><td>Chapter: 08 Management of Information</td><td>Subject No: 08.04.02.01</td></tr>
<tr><td rowspan="2">Effective Date:
04/01/2025</td><td>Date of Review/Revision:</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td><td>Responsible Director:
Chief Information Officer and Chief Quality & Compliance Officer

Authored By:
Christina Saunders, Administrative Assistant to CIO|CQCO

Additional Reviewers:
Kentera Patterson, Officer of Recipient Rights and Compliance</td></tr>
</table>

Purpose:
The purpose of this policy is to define the standards and responsibilities for accessing restricted behavioral health information through the "Break the Glass" (BTG) functionality in SCCMHA's electronic health record (EHR) systems. This policy ensures access is granted only under legitimate, urgent, or exceptional clinical circumstances while protecting the privacy of our people served and complying with applicable laws and regulations, such as Health Insurance Portability and Accountability Act (HIPAA) Privacy & Security Rules.

Application:
This policy applies to all SCCMHA employees, volunteers, students, contractors, and business associates who have access to the EHR system.

Policy:
SCCMHA is committed to protecting confidentiality, integrity, and security of sensitive information of people served, including behavioral health records, in compliance with federal and state regulations such as the HIPAA and 42 CFR Part 2. Due to the sensitive nature of behavioral health data, additional safeguards are in place to limit access to only those individuals with a direct and legitimate need to know.
BTG functionality is a critical privacy and security control designed to restrict routine access to sensitive information while still enabling access in exceptional circumstances

where clinical care requires it. BTG access is not a substitute for standard role-based access and must only be used when access is essential for the immediate provision of care or in other rare, justifiable circumstances.
Improper or unauthorized use of BTG undermines the trust bestowed by people served on the organization, violates privacy regulations, and poses additional risks to SCCMHA. Any misuse of BTG access — including access out of curiosity, for non-clinical purposes, or without proper justification — will be considered a violation of this policy.
This policy reinforces our organization's commitment to safeguarding behavioral health information, maintaining ethical standards, and fostering a culture of accountability and privacy in all aspects of care delivery.

Standards:
1. All users authorized to access the EHR are required to adhere to the following standards when engaging BTG access:

a. Conditions for BTG Access

- BTG must only be used when health information is needed to support immediate and necessary care of the people served.
- Routine, curiosity-based, or unauthorized access is strictly prohibited.
- BTG should not be used as a workaround for normal role-based access limitations.

b. Documentation of Justification

- Users must provide clear, specific clinical justification before proceeding with BTG access.
- Blanket or vague reasons (e.g., "general review") are not acceptable.

c. Audit and Monitoring

1) All BTG access is logged into and subject to regular audit by Access Management Group, the Compliance Department, and the HIPAA Privacy and Security Officers.
2) Users may be required to justify BTG use during audit reviews if justification is not provided when accessing information.
3) Patterns of inappropriate access will be investigated.

d. Training and Awareness

1) All users must complete mandatory annual review of this policy and complete routine training on the importance and compliance of this policy.

e. Business Associates and Contractors

- Business associates and contractors must be contractually obligated to comply with this policy.
- Their access must be role-based and monitored, and they are subject to the same standards and audits as employees.

2. **Additional Guidelines**

1. **Do Not Share Credentials**: Accessing BTG through another user's account is a serious violation.
2. **Report Suspicious Activity**: If you suspect BTG misuse by another individual, report it to the Compliance Officer or Chief Information Officer, Chief Quality & Compliance Officer immediately.
3. **Know When Not to Use BTG**: If you are unsure whether BTG is appropriate, consult your supervisor or the Privacy Office before proceeding.

Definitions:

Break the Glass (BTG) - A security control within the EHR system that restricts access to sensitive patient data—such as behavioral health records—unless the user explicitly overrides the restriction with a documented justification for access.

Role-Based Access Control (RBAC) - A system of restricting access to information based on a user's role or job responsibilities within the organization.

Justification for Access – A clear and specific explanation provided by the user, documenting why BTG access is necessary for person served care or another permitted purpose.

Audit Log – A system-generated record of all BTG access events, including user identity, date/time, person served record accessed, and justification entered.

Authorized User – Any employee, contractor, business associate, or other individual who has been granted access to the organization's EHR system for the purpose of performing approved job duties.

Business Associate - A person or entity that performs functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of protected health information (PHI), as defined under HIPAA.

References:

Health Insurance Portability and Accountability Act (HIPAA) of 1996 – 45 CFR Parts 160 and 164
42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
HITECH Act (Health Information Technology for Economic and Clinical Health Act)
SCCMHA Privacy and Security Policies
SCCMHA Electronic Health Record (EHR) Access Policy
National Institute of Standards and Technology (NIST) SP 800-53 – Access Control Guidelines

Exhibits:

Exhibit A: Sample BTG Access Justification Examples
Exhibit B: BTG Access Workflow Diagram

Procedure:

ACTION	RESPONSIBILITY
1) Determine Need for Access a) Before initiating BTG access, the user must determine whether behavioral health information is **essential and related to the immediate care or safety of the person served**. b) If the need is routine or non-urgent, users should follow standard access protocols or request access through appropriate supervisory channels.	1) EHR User
2) Initiate Break the Glass Access a) When prompted by the EHR system due to access restrictions, the user must **activate BTG**	2) EHR User

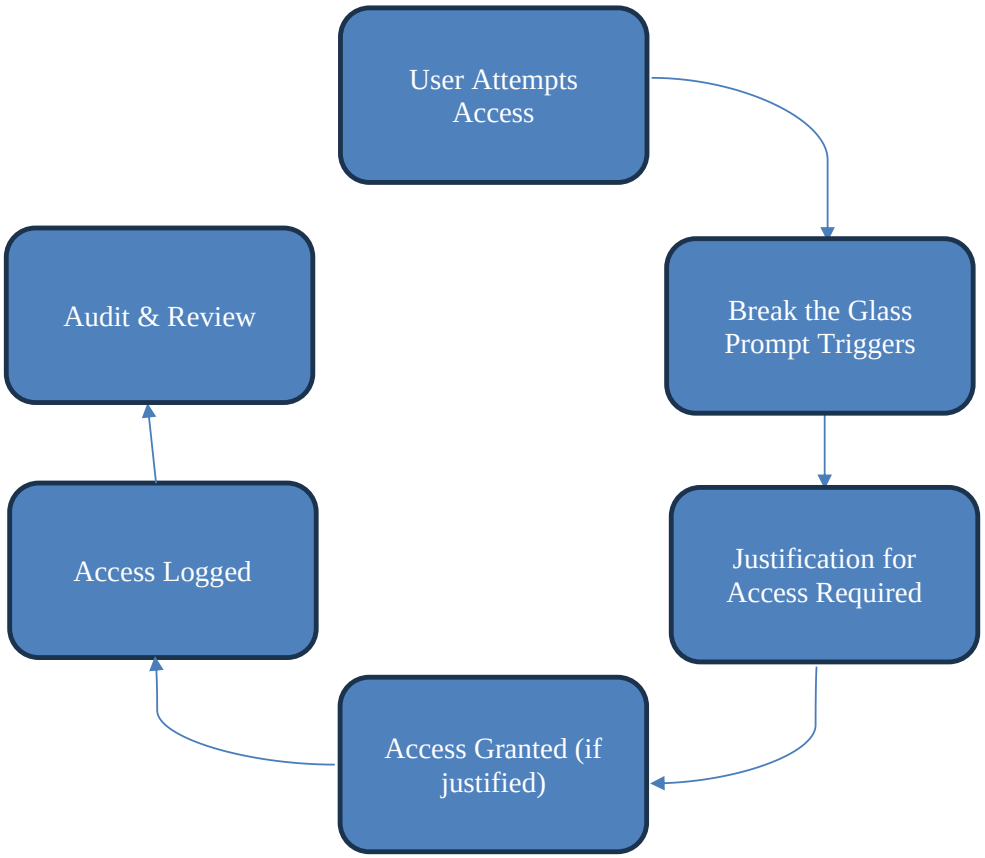
access by selecting the appropriate option. b) Users should not attempt to bypass the restriction by asking another user with access to view or share information on their behalf. 3) Provide Justification a) The system will require the user to enter a **specific clinical justification** for BTG access. b) Acceptable justifications include: i) "Person served is in crisis and behavioral health history is needed to inform care." ii) "Person served presented with suspected overdose or suicidal ideation." c) Unacceptable justifications include vague entries such as "Need to check" or "Just in case." 4) Access Information a) Once justification is entered, access will be granted. b) Users must access only the information that is necessary for care delivery and must **not browse or review unrelated records**. 5) BTG Access will be logged into and audited for compliance purposes. 6) Cooperation with Audit or Follow-up a) All BTG access is subject to **periodic audit by Compliance or Privacy teams**. b) Users may be contacted to provide additional context or explanation for their access. c) Users are expected to **respond promptly and transparently** to any inquiries.	3) EHR User 4) EHR User 5) Sentri System 6) EHR User

Exhibit A: Sample BTG Access Justification Examples

Acceptable Justifications	**Unacceptable Justifications**
"Person served is in crisis and behavioral history is needed for treatment."	"Just checking person served background."

Acceptable Justifications	Unacceptable Justifications
"Person served presented in Emergency Department with possible overdose; mental health data critical to treatment."	"Wanted to see patient history out of curiosity."
"Primary care provider requested behavioral health coordination support."	"Thought it might be helpful later."

Exhibit B: BTG Access Workflow Diagram



<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA – HITECH: Breach Notification: Protected Health Information</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.05.03.03</td></tr>
<tr><td rowspan="2">Effective Date:
February 1, 2010</td><td>Date of Review/Revision:
5/13/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 6/23/23, 9/9/24,11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer, Chief Quality & Compliance Officer

Authored By:
Kentera Patterson, Officer of Recipient Rights and Compliance / HIPAA Privacy Officer

Additional Reviewers:</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure timely and compliant breach notification following the improper or unauthorized access, acquisition, use and/or disclosure of SCCMHA's protected health information (PHI). This policy complies with the HIPAA Privacy and Security Rules, Health Information Technology for Economic and Clinical Health Act (HITECH), as well as any other applicable federal or state notification law.

Policy:

1. **Discovery of Breach**: A breach of PHI is considered "discovered" on the first day it becomes known to SCCMHA or should have been known using reasonable diligence by SCCMHA or its business associates. Following the discovery of a potential breach, SCCMHA shall begin an investigation, conduct a risk assessment, and base on the results of the risk assessment, begin the process to notify each person served whose PHI has been, or is reasonably believed by SCCMHA to have been, accessed, acquired, used, or disclosed because of the breach. SCCMHA shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. **Breach Investigation**: The SCCMHA Privacy Officer shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The Privacy Officer shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years (In accordance with 45 CFR Sec. 164.530(j)(2)).

3. **Risk Assessment:** For acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. The use or disclosure of PHI that is incident to an otherwise permissible use or disclosure occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to persons served , media, or the HHS secretary under breach notification requirements, SCCMHA will need to perform a risk assessment to determine if there is significant risk of harm to the person served as a result of the impermissible use or disclosure SCCMHA shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. SCCMHA has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, SCCMHA will determine the need to move forward with breach notification. SCCMHA must determine whether an impermissible use or disclosure constitutes a breach using a four-factor risk assessment (45 CFR §164.402):
    A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
    B. The type and amount of PHI involved.
    C. The potential for significant risk of financial, reputational, or other harm.
    D. The extent to which risk was mitigated. SCCMHA documents and maintains evidence of the assessment and outcome.

4. **Timeliness of Notification**: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by SCCMHA or the business associate involved. It is the responsibility of SCCMHA to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. **Delay of Notification Authorized for Law Enforcement Purposes**: If a law enforcement official states to SCCMHA that a notification, notice, or posting would

impede a criminal investigation or cause damage to national security, SCCMHA shall:

A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. **Content of the Notice**: The notice shall be written in plain language and must contain the following information:

   A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
   C. Any steps the person served should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what SCCMHA is doing to investigate the breach, to mitigate harm to people served, and to protect against further breaches.
   E. Contact procedures for people serve to ask questions or learn additional information, which include a toll-free telephone number, an e-mail address, Web site, or postal address.

7. **Methods of Notification**: The method of notification will depend on the persons served/entities to be notified. The following methods must be utilized accordingly:
   A. <u>Notice to Person(s) Served:</u> Notice shall be provided promptly and in the following form:
      1. Write notification by first-class mail to the person served at the last known address of the person served or, if the person served agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. Notification shall be provided in one or more mailings as information is available. If the organization knows that the person served is deceased and has the address of the next of kin or personal representative of the person served, written notification by first-class mail to the next of kin or person representative shall be carried out.
      2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice calculated to reach the person served shall be provided. A substitute notice need not be

provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 people served, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b. In the case in which there is insufficient or out-of-date contact information for 10 or more persons served, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in SCCMHA's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where a person served can learn whether his or her PHI may be included in the breach.

3. If SCCMHA determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. **Notice to Media**: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 people served. The Notice shall be provided in the form of a press release.

C. **Notice to Secretary of HHS**: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the **unsecured** PHI of more than 500 persons served is accessed, acquired, used, or disclosed.

1. For breaches involving 500 or more people served, SCCMHA shall notify the Secretary of HHS as instructed at www.hhs.gov the same time notice is made to the people served.

2. For breaches involving less than 500 people served, SCCMHA will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

8. **Maintenance of Breach Information/Log**: As described above and in addition to the reports created for each incident, SCCMHA shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of people served

affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):

A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of people served affected, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
C. A description of the action taken regarding notification of people served regarding the breach.
D. Resolution steps taken to mitigate the breach and prevent future occurrences.

9. **Business Associate Responsibilities**: The business associate (BA) of SCCMHA that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify SCCMHA of such breach. Such notice shall include the identification of each person served whose unsecured protected health information has been or is believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide SCCMHA with any other available information that SCCMHA is required to include in notification to the person served at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, SCCMHA will be responsible for notifying affected persons served, unless otherwise agreed upon by the BA to notify the affected persons served (note: it is still the burden of SCCMHA to document this notification).

10. **Workforce Training:** SCCMHA shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members should also be trained in how to identify and report breaches within SCCMHA.

11. **Complaints**: SCCMHA provides a process for people served to make complaints concerning the organization's privacy policies and procedures or its compliance with such policies and procedures. Persons served have the right to complain about SCCMHA's breach notification processes.

12. **Sanctions**: SCCMHA has in place and applies appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

13. **Retaliation/Waiver**: SCCMHA does not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any person served for the exercise by the person served of any privacy right. SCCMHA does not require people to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Application:
SCCMHA workforce and Business Associates

Standards:
None

Definitions:
See *SCCMHA Policy 08.05.00.01 Compliance Definitions for the following terms:*
Access
Breach
Disclosure
Individually Identifiable Health Information
Official Law Enforcement
Protected Health Information (PHI)
Unsecured Protected Health Information
Workforce

References:

- HITECH Act (ARRA Title XIII Section 13402 – Notification in the Case of Breach)
- FTC Breach Notification Rules – 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules

Exhibits:

- Exhibit A - Examples of Breaches of Unsecured Protected Health Information
- Exhibit B - Breach Penalties
- Exhibit C - Sample Notification Letter to Persons Served
- Exhibit D - Sample Notification Letter to Secretary of Health & Human Services
- Exhibit E - Sample Media Notification Statement/Release
- Exhibit F - Sample Talking Points
- Exhibit G - Examples of Violations and Notification Recommendations
- Exhibit H - Sample Breach Notification Log
- Exhibit I – Breach Notification Risk Assessment Tool

Procedure:

ACTION	RESPONSIBILITY
1. Notify the SCCMHA Privacy Officer of HIPAA violations as they become aware of them	1. SCCMHA Workforce and Business Associates
2. Conduct Breach Investigation, Risk Assessment and Notification, as necessary.	2. SCCMHA Privacy Officer
3. Maintain Breach Information Log	3. SCCMHA Privacy Officer

Exhibit A

Examples of Breaches of Unsecured Protected Health Information

- Workforce members, who do not have a legitimate work-related need to know the information, access the electronic health records of a prominent local figure that is treated by SCCMHA.
- Stolen or lost laptop containing unsecured protected health information.
- Papers containing protected health information were found scattered along the roadside after improper storage in truck by business associates responsible for disposal (shredding).
- Posting of patient's HIV+ health status on social media by a clinician.
- Misdirected e-mail of listing of drug seeking people served to an external group list.
- Lost flash drive containing database of people participating in a clinical study.
- EOB (Explanation of Benefits) sent to wrong guarantor.
- Member of SCCMHA workforce accessing the health record of divorced spouse for information to be used in a custody hearing.
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- Workforce members take cell phone pictures of people served and transmit photos to friends.
- Medical record copies in response to a request lost in mailing process and never received.
- Misdirected fax of person served records to a local grocery store instead of the requesting provider's fax.
- Briefcase containing person served records stolen from car.
- PDA with person served -identifying photos or other records lost.
- Intentional and non-work-related access by workforce member of neighbor's information.
- Medical record documents left in public access areas – such as cafeteria.
-
- Unauthorized sharing of screen during a virtual meeting that displays PHI to individuals without a need to know.
-
- Improper disposal of printed PHI (e.g., tossing documents in regular trash instead of shredding).
-
- Using personal cloud storage (e.g., Google Dropbox) to store or share documents containing PHI without proper encryption or approval.
-
- Accessing or sharing PHI via unsecured texting or personal email accounts.

-
- Verbal disclosures of PHI in public spaces, such as hallways, elevators, or restaurants.
-
- Recording a therapy session that includes PHI on a personal device, even with good intentions, without appropriate consent and safeguards.
-
- Posting photos on internal social media or Teams channels where people served are visible or identifiable.
-
- Neglecting to log off shared workstations, resulting in unauthorized users accessing open EHR systems.
-
- Allowing family/friends to use a work-issued device where PHI is stored or accessible.
-
- Printing PHI at home without secure storage or transport back to the office

Exhibit B

Breach Penalties

Penalties for Breach: Penalties for violations of HIPAA have been established under HITECH as indicated below. The penalties do not apply if the organization did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty days.(See HIPAA Enforcement Rule, 45 CFR Part 160, Subpart D, and 42 CFR 1320d-5 as Amended by ARRA Section 13410(d)(3)). Penalties will be based on the organization's culpability for the HIPAA violation. The Secretary of HHS will base its penalty determination on the nature and extent of both the violation and the harm caused by the violation. The Secretary will still have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

The maximum penalty is $50,000 per violation, with a cap of $1,500,000 for all violations of an identical requirement or prohibition during a calendar year.

The minimum civil monetary penalties are tiring based upon the entity's perceived culpability for the HIPAA violation, as follows:

Tier A – *If the offender did not know.*

- $100 - $50,000 for each violation, the total for all violations of an identical requirement during a calendar year cannot exceed $25,000.

Tier B – *Violation due to reasonable cause, not willful neglect*

- $1,000 - $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $100,000.

Tier C – *Violation due to willful neglect but was corrected.*

- $10,000 - $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $250,000.

Tier D – *Violation due to willful neglect but was NOT corrected.*

- $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $1,500,000.

The maximum penalty per violation remains $50,000, and the overall maximum annual penalty cap per violation type remains $1.5 million under Tier D.

Exhibit C

Sample Notification Letter to Persons Served
Document to be Reviewed and Customized Prior to Use

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

[Date]

[Name here]
[Address 1 Here]
[Address 2 Here]
[City, State Zip Code]

Dear [Name of Organization Person served, or Person served Name]:

I am writing to you with vital information about a recent breach of your personal information from SCCMHA. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe events and include the following information:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
C. Any steps the person served should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to persons served, and to protect against further breaches.
E. Contact procedures for people serve to ask questions or learn additional information, which include a toll-free telephone number, an e-mail address, Web site, or postal address.

Other Optional Considerations:

To ensure that this information is not used inappropriately, SCCMHA will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [N**eed to document the process for how this would work].**

We also advise you to immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

    - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role in safeguarding your personal information and using it in an appropriate manner. SCCMHA apologizes for the stress and worry this situation has caused you and is doing everything it can to rectify the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call XXXXXXX during normal business hours with any questions you have.

We have also established a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

[Insert Closing Paragraph Based on Situation]

Sincerely,

[Insert Applicable Name/Contact Information]

Exhibit D

Sample Notification Letter to Secretary of Health & Human Services
Document to be Reviewed and Customized Prior to Use

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

[Date]

Secretary of Health & Human Services
The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Toll Free: 1-877-696-6775

Dear Secretary:

In compliance with the American Recovery and Reinvestment Act of 2009 (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), we are notifying you of a recent breach of unsecured protected health information (PHI). The breach involved [Insert Number] people served. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information as communicated to the victims:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which include a toll-free telephone number, an e-mail address, Web site, or postal address.

On behalf of SCCMHA I am communicating this information to you in compliance with ARRA/HITECH.

If you have any questions or require further information, please contact me at [Insert Contact Information].

Sincerely,

[Insert Applicable Name/Contact Information]

Exhibit E

Sample Media Notification Statement/Release
Document to be Reviewed and Customized Prior to Use

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

[Insert Date]

Contact: [Insert Contact Information Including Phone Number/E-Mail Address]

IMMEDIATE RELEASE

SCCMHA NOTIFIES PERSONS SERVED OF BREACH OF UNSECURED PERSONAL INFORMATION

SCCMHA notified [Insert Number] people served of a breach of unsecured personal protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which include a toll-free telephone number, an e-mail address, Web site, or postal address.

In conjunction with local law enforcement and security experts, SCCMHA is working to notify impacted persons served to mitigate the damages of the breach. [Name of Organization] has in place safeguards to ensure the privacy and security of all people served

health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risks.

In a notification to persons served, [Name of Organization] has offered their resources as well as …. [Insert as Applicable]. [Name of Organization] also has encouraged its people served to contact their financial institutions to prevent unauthorized access to personal accounts.

[Name of Organization] has trained staff available for people served to call with any questions related to the data breach. People who served may call [Insert Phone Number Here] from [Insert Hours] with any questions. In addition, people served may visit [Name of Organization's] Web site at [Insert Web Address] for further information.

[Name of Organization] understands the importance of safeguarding our persons served' personal information and takes that responsibility very seriously," said [Insert Name], President and CEO. "We will do all we can to work with persons served whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to preventing such occurrences in the future. We appreciate the people who served support during this time.

Please direct all questions to [Enter Contact Information].

Exhibit F

Sample Talking Points (Based on an Example)
Document to be Reviewed and Customized Prior to Use

Talking Points to Respond to Inquiries About Breach of Unsecured Person Served Protected Health Information

What Happened

Describe Incident Objectively (see sample below).

- *An employee of SCCMHA has been arrested for using the personal health information of XX persons served to obtain loans and credit cards.*
- *The employee has been charged with identity theft, bank fraud, and credit card fraud.*
- *The employee also illegally obtained $XXXXX in reimbursement for fraudulent health claims he/she submitted.*
- *The employee allegedly also sold the personal information of our people served to her brother. He also has allegedly obtained credit cards using the persons served identities.*
- *[Insert Law Enforcement Agency Name] is investigating to identify the people served affected by the identity theft.*
- *The employee worked as a supervisor in our claims administration area.*
- *The employee has been suspended without pay. Her access to [Insert Name of Organization] facilities and any [Insert Name of Organization] computer systems has been terminated.*
- *As a supervisor, the employee had access to personal information of [Insert Name of Organization] patients.*
- *Her access to person served information was based on her ability to do the job she was assigned.*
- *The employee has been with the [Insert Name of Organization] for XX years.*
- *The employee underwent a full background check, including criminal check, upon her hire in 20XX.*

- *There have been no other charges against this employee in her time at [Insert Name of Organization].*
- *This is the first and only time this type of situation has happened at [Insert Name of Organization].*
- *[Insert Name of Organization] has contacted the affected persons served and has provided credit monitoring services and a contact for additional guidance.*

What is SCCMHA Doing Now

Customize as Applicable

- We are notifying each person served that has been affected by the incident and offering resources to answer any questions or concerns that he or she may have about the current situation.
- *We are contacting the Secretary of the Department of Health & Human Services to notify her of the breach.*
- *We are working with our Compliance Department, IT Department, Legal Department, and Human Resources, to review procedures to see if there are additional safeguards we should implement to prevent this type of action in the future.*
- *We are working with the law enforcement officials to provide them with any information to expedite the investigation and prosecution of this matter.*

What SCCMHA Will Do for Our Patients

- *We would continue to make our compliance department available if the people served have any questions or concerns regarding their credit.*
- *We have established a special toll-free number for [Insert Name of Organization] people served to call those who have questions regarding their personal information.*
- *We will also encourage the people served to contact any of the three credit reporting agencies and establish a fraud alert.*

Exhibit G

Examples of Violations and Notification Recommendations

Type of Privacy or Security Violation	Notify Person Served?	Notes / Regulation Reference
PHI mistakenly faxed to a public location (e.g., grocery store, workplace, pharmacy)	Yes	Presumed breach unless risk assessment shows low probability of compromise.
Lab results or test orders sent to wrong provider, facility, or faxed to old organization	Yes	Even if not viewed, it is still considered a breach unless insignificant risk shown per 45 CFR §164.402.
Lab requisition with wrong person's name handed to another patient	Yes	Improper disclosure of individually identifiable health info.
EOB (Explanation of Benefits) mailed to the wrong guarantor	Yes	Breach of financial + medical information.
Test results or paperwork given to wrong person in clinic or waiting room	Yes	Unintended disclosure in a public/shared setting.
Briefcase, laptop, USB, or mobile device with unencrypted PHI lost or stolen	Yes	Must notify unless device is encrypted by NIST standards. See HITECH 13402(h).
PHI disclosed via social media, blog, or text by staff (e.g., EMT posts photo of person served after MVA)	Yes	Unauthorized use/disclosure; must report. 45 CFR §164.502(a)(1).
Medical records left publicly visible (e.g., cafeteria, hallway)	Yes	Improper disclosure.
PHI emailed or mailed to wrong individual	Yes	Applies even if promptly retrieved unless low probability of compromise determined.
PHI disclosed in voicemail, left on wrong answering machine	Yes	Risk assessment needed, but usually reportable.
Patient name and diagnosis overheard in shared waiting room	Yes	Must take reasonable safeguards to prevent incidental disclosure.
PHI accessed by a staff member without job-related need (snooping, celebrity access)	Yes	Inappropriate access regardless of whether info was further disclosed.

Temp/contract staff improperly access PHI	Yes	Workforce must be trained and limited by role.
Use of unsecured communication for PHI (e.g., texting PHI without secure app)	Yes	Use of unsecure medium is considered a breach.
Unencrypted data (USB, laptop, email) sent or lost	Yes	Encryption safe harbor only applies if strong enough to meet standards (NIST SP 800-111).
Authorized disclosures under a court order or valid legal process	Not Required	If the disclosure was permissible under HIPAA and made appropriately.
PHI sent to business associate, but they experience breach (e.g., truck scattered papers, email hack)	Yes	Business associates must report to covered entity. Covered entity must report to person served.
Subpoena or court order issued for records	Not Required*	If not privileged and legally authorized. Otherwise see 330.1748 and SCCMHA privileged info policy.
Unauthorized disclosure of PHI in research study (by employee or contractor)	Yes	HIPAA + HITECH require reporting to individuals, media, and HHS if over 500 affected.
Disclosure of non-medical identifier tied to health app without consent (e.g., FTC breach rule for mHealth app)	Yes	May also trigger FTC Health Breach Notification Rule if app is not HIPAA-covered.
Failure of MFA or compromised login to system containing PHI	Yes	Unauthorized access breach if data exposed. Evaluation for risk level.
Person served records accessed via misdirected login (wrong MRN entered)	Yes	Still a reportable breach unless insignificant risk of compromise determined.
Social worker discusses person served PHI with unauthorized third party (e.g., family member w/o authorization)	Yes	Violation of minimum necessary standard.
PHI sent to terminated provider's fax or email	Yes	Considered unauthorized recipient unless active BAA or contract exists.

Criteria	**Requirement**
Notify Individual	Without unreasonable delay, and no later than **60 calendar days** after discovery.
Notify HHS	Within **60 days of the end of the calendar year** (if <500 affected) or within **60 days** (if >500).
Notify Media	If more than 500 residents of a state/region are affected.
Risk Assessment Required?	Yes, under 45 CFR §164.402: Evaluate nature, unauthorized person, access, and mitigation.

Exhibit H

Sample Breach Notification Log

The organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of people served affected. A record of the complete investigation of the potential breach as well as the risk assessment carried out to determine notification requirements should be created. The risk assessment and the incident report should be cross referenced so that the Secretary of HHS require more information; it is easy to locate and provide.

Note: Reconfigure Width of Data Fields for Landscape Document or Spreadsheet

Incident #	Date of Discovery	Date of Breach	Location	Brief Description of Breach*	Number of Persons Served Involved	Notification Dates			Actions Taken Resolution Steps
						Persons Served	Media	HHS	

- A description of what happened, including a description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).

Exhibit I

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Summary of HIPAA Breach Notification Rule, 45 CFR § 164.400-414

The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI). A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information. An impermissible use or disclosure is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates through a thorough risk assessment (as outlined below) that there is a low probability that the PHI has been *compromised* based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used or had access to the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Was Protected Health Information (PHI) Involved?
PHI is health information that identifies, or there is a reasonable basis to believe it can be used to identify, the individual. Health information includes any demographic information of the individual (e.g. name, address, birth date, Social Security number, medical record number) and information relating to the physical or mental health or condition of an individual, the health care provided to an individual (e.g. diagnosis, treatment plan, medication, medical history and test results), or payment for health care provided to an individual:

☐ Yes ☐ No

If yes, PHI was involved, please continue completing this risk assessment tool.
If no, PHI was not involved, then no breach occurred.

Date Incident Occurred:	

Date Incident Reported:		**Breach Notification Due Date:** *(If applicable, 60 days from incident report date)*	

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Name & Title of Person Who Reported Incident:

Brief Description of Incident

1. **Who accessed or disclosed the PHI?**
2. **Was the person authorized to access the PHI? Explain why or why not.**
3. **How did the person access and/or disclose the PHI? Explain in detail.**
4. **What was the person's explanation for accessing and/or disclosing the PHI?**
5. **Was the PHI received by the intended recipient?**
6. **What did the intended recipient do with the PHI? Was the PHI forwarded to any other person or entity?**
7. **Was the PHI recovered and/or did Denver Health receive confirmation that the PHI was destroyed?**
8. **Was the incident reported to law enforcement?** If so, include name of agency, name of contact at agency (if known), date reported, report number and known status.

Description of PHI (*e.g., Type of Information, Fields, # of Records*):

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Was PHI accessed, used, or disclosed as permitted by the Privacy Rule? (Was use or disclosure limited to the "minimum necessary" for treatment, payment and health care operations (TPO)?)

☐ Yes ☐ No

If yes, PHI was accessed, used or disclosed as permitted by the Privacy Rule, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, PHI accessed, used or disclosed was not limited to the "minimum necessary" for TPO, please continue to the next question.

Was information held by SCCMHA in its capacity as an employer? (For example, SCCMHA obtains PHI from another entity and uses/discloses PHI information for purposes of FMLA, Workers Compensation, and/or HR employment related activities. If SCCMHA obtains and uses PHI in this capacity, then it is not considered PHI and not considered a breach.)

☐ Yes ☐ No

If yes, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, then please continue to the next question.

Was PHI encrypted, destroyed or properly de-identified (limited data set with no direct identifiers *and* does not include dates of birth or zip codes)?

☐ Yes ☐ No

If yes, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, then please continue to the next question.

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Does an exception to the Breach Notification Rule apply? Please review Exceptions A-C below.

☐ Yes ☐ No

If yes, Exception A, B or C applies (please check one below), then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, Exception A, B or C does not apply, then please continue to the Risk Assessment below.

☐ **Exception A.** Was PHI unintentionally accessed or used by a workforce member (employee, volunteer, trainee) or person acting under the authority of a SCCMHA or business associate within his/her scope of authority, and the PHI was not further impermissibly used/disclosed?

☐ Yes ☐ No

Briefly explain your answer:_____

_____

☐ **Exception B.** Was PHI inadvertently disclosed by an authorized person at SCCMHA or business associate to another authorized person at SCCMHA or business associate, and the PHI was not further impermissibly used/disclosed?

☐ Yes ☐ No

Briefly explain your answer: _____

_____

☐ **Exception C.** Does SCCMHA or business associate have a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information? (For example, PHI sent via mail to the wrong address and returned unopened could not reasonably have been read or retained by the improper addressees.)

☐ Yes ☐ No

Briefly explain your answer: _____

_____

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Risk Assessment

An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below.

Can this breach be determined to have a ***low probability*** that the PHI was compromised based on the following assessment?

1) What type and amount of PHI was involved and how likely is it that individuals could be identified if PHI is combined with other available information? Consider whether more sensitive identifiable information was involved (e.g., date of birth, SSN, financial information) or sensitive clinical information (e.g. mental health, test results, STD results) that could increase the risk of identity theft, financial fraud, reputational or other harm to the individual.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe the nature and amount of the PHI:

2) Who impermissibly used the PHI and/or to whom was the PHI impermissibly disclosed? Consider this factor if the PHI was impermissibly used or disclosed within SCCMHA. Consider whether the person has legal obligations to protect the information. For example, is the person a covered entity required to comply with HIPAA, or a government employee, etc.? If so, there may be a lower probability that the PHI has been compromised.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe who received or used the PHI:

3) Was the PHI actually acquired or viewed or was there only the opportunity to acquire or view but actual viewing or acquisition of PHI did not occur? (If electronic PHI is involved, this may require a forensic analysis of the computer to determine whether the PHI was accessed, viewed, acquired, transferred or otherwise compromised.)

☐ Yes, this factor supports low probability of compromise. ☐ No

SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

Describe whether the PHI was actually acquired or viewed:

4) To what extent was the risk to the PHI mitigated? For example, by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement, declaration or similar means), has been returned, or has been/will be destroyed.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe steps SCCMHA took or intends to take to mitigate risk:

Breach Risk Assessment Result

SCCMHA performed a risk assessment, as required under the Department of Health and Human Services, Breach Notification for Unsecured Protected Health Information; Final Rule, effective on March 26, 2013 and reached the following conclusion.

☐ **Breach notification is required.** SCCMHA concludes that notification is required because the assessment above supports that there is greater than low probability that the PHI has been compromised.

☐ **Breach notification is not required. SCCMHA** concludes that notification is not required because the assessment above supports that there is a low probability that the PHI has been compromised.

Scope of Notification ***(Note: If more than 500 individuals OCR and Media Notice is required)***

Other corrective action(s) required:

• SCCMHA Privacy Officer recommendation(s)

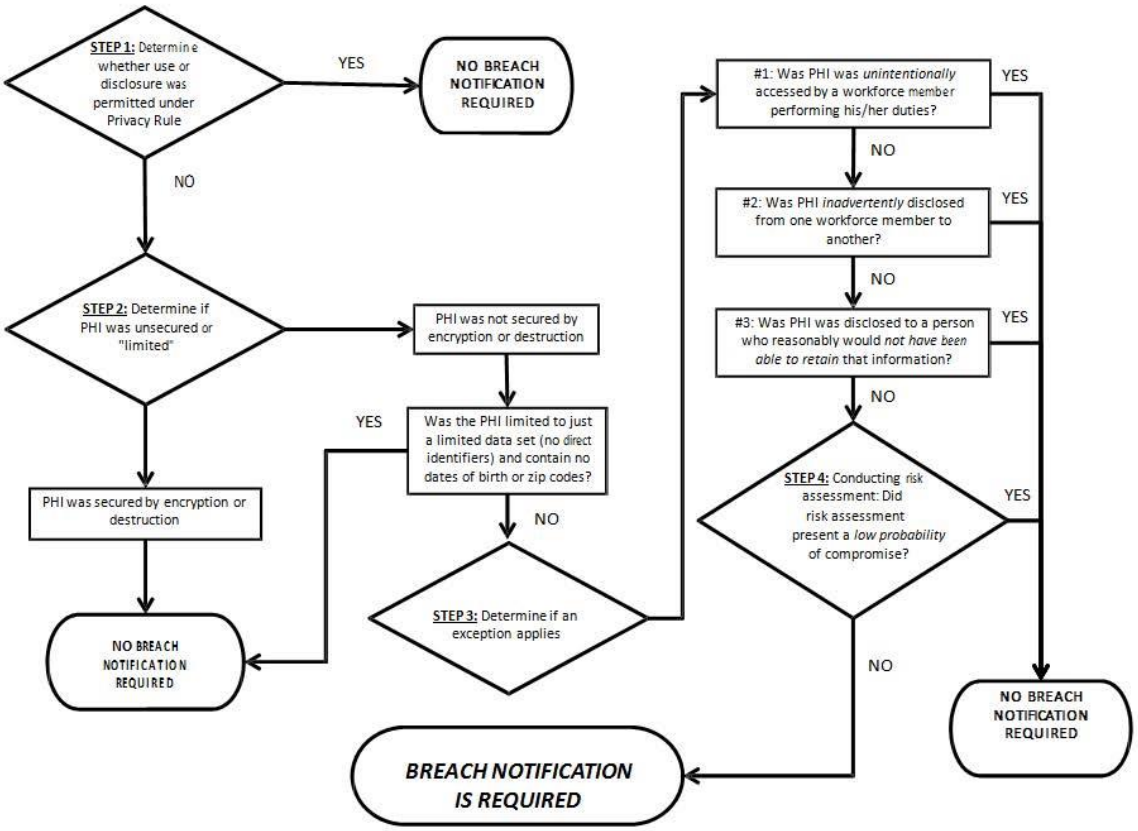
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

Breach Notification Risk Assessment Tool

• Manager(s) responsible for implementing corrective action
Date corrective action should be delivered:
• Date of corrective action; confirmation by Human Resources Department

Preventive action(s) required:
Describe who, what, when and how the preventative action(s) will be carried out:

HIPAA/HITECH Decision Tree to Determine Whether Breach Notification is Required



SCCMHA Breach Notification Risk Assessment Tool (5/16) Page 8 of 8

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Privacy Set: Employee Education and Training - Employee Training Regarding the Use and Disclosure of PHI</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.05.14.01</td></tr>
<tr><td rowspan="2">Effective Date:
April 14, 2003</td><td>Date of Review/Revision:
3/5/03, 6/30/09, 6/4/14, 5/12/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 10/26/22, 6/27/23, 9/9/24, 10/14/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Kentera Patterson, Officer of Recipient Rights and Compliance

Additional Reviewers:
Holli McGeshick, Quality and Medical Records Supervisor

Alecia Schabel, Continuing Education Supervisor

Jennifer Keilitz, Director of Network Services, Public Policy, CE, EHS and OBRA</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

Saginaw County Community Mental Health Authority (SCCMHA) is committed to ensuring the privacy and security of a person served health information. In accordance with the HIPAA Privacy and Security Rules, Michigan Mental Health Code, and other applicable federal, state, and/or local laws and regulations have established standards with which health care organizations must comply when using or disclosing a person served protected health information. To support our commitment to person served confidentiality, all employees, contractors, volunteers, interns, and applicable network providers of SCCMHA will receive timely and appropriate role-specific training regarding the policies and

procedures for using and/or disclosing protected health information, as required under the HIPAA Privacy Rule, 45 CFR §164.530(b), 164.308(a)(5), and MCL 330.1748.
SCCMHA will provide required training and regular updates to reflect material changes in law, regulation, or organizational policy.

Policy:

1. **Initial Training Requirement:**
    a. SCCMHA will train all employees, contractors, volunteers, interns, and network providers regarding proper use and disclosure, safeguarding electronic PHI, reporting breaches, and individual rights under HIPAA and the Michigan Mental Health Code of protected health information within 30 calendar days of hire or contract, or earlier if accessing PHI.
2. **Role-Specific and Functional Training:** SCCMHA will train all employees on:
    a. SCCMHA's privacy and security policies and procedures with respect to protected health information as necessary and appropriate for the employees to carry out their function at SCCMHA.
    b. Specific documentation, access, or communication workflows
    c. How to appropriately use, disclose, or request PHI based on minimum necessary standards.
3. **Periodic and Refresher Training:** SCCMHA shall:
    a. Periodic re-training will be provided as policies change in addition to refresher training at least annually.
    b. Provide real-time updates or targeted trainings in response to privacy and security incidents, breaches, or audit findings,
    c. Document all completion of retraining efforts.
4. **Policy and Regulation Updates:** SCCMHA shall promptly update training materials and deliver additional training when:
    a. There are material changes to federal or state law (e.g., HIPAA Final Rule updates),
    b. SCCMHA updates or adopts new privacy/security policies,
    c. Findings from internal compliance audits or external investigations indicate deficiencies.
5. **Documentation and Retention:** Documentation of training completion (initial and refresher) shall be:
    a. Maintained by Continuing Education Unit and/or the Compliance Department for information security training.
    b. Records should be retained for at least 6 years from the date of training, in compliance with 45 CFR §164.530(j).
6. **Enforcement and Accountability:** Failure to complete required training within specified timeframes may result in:
    a. Delayed access to systems containing PHI,
    b. Corrective action plans,
    c. Report to supervisors, department heads, or licensing agencies as appropriate.

Application:
All SCCMHA Board operated programs and applicable Network Providers.

Standards:
1. New employees will receive HIPAA Privacy Rule training within 30 days of hire.
2. All workforce members must complete annual refresher training or sooner if required.

Definitions:
See SCCMHA Policy 08.05.00.01 Compliance Definitions

References:
HIPAA Privacy Rule, 45 CFR §164.530(b) – Training
HIPAA Security Rule, 45 CFR §164.308(a)(5) – Security Awareness and Training
HIPAA Documentation Standard, 45 CFR §164.530(j)
Michigan Mental Health Code, MCL 330.1748
HHS Final Rule 2023–2024: HIPAA Privacy Rule to Support Reproductive Health Care Privacy

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. Employee training regarding the use and disclosure of protected health information will include the following: a. the process by which a person served may request access to his or her protected health information. b. the documents to be used for persons served to request access to their protected health information. c. the process by which SCCMHA may request the use or disclosure of a person served protected health information. d. the documents to be used for SCCMHA to solicit a request for a person served protected health information. e. the right of the person served to revoke consent. f. the identification of defective consents. g. the recognition of when SCCMHA may condition the provision to a person served of treatment, payment, enrollment, or eligibility for benefits on the provision of obtaining a consent.	HIPAA Privacy Officer

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject HIPAA Privacy Set: Employee Education and Training - Employee Training on Privacy Awareness	**Chapter**: 08 - Management of Information	**Subject No**: 08.05.14.02
Effective Date: April 14, 2003	**Date of Review/Revision**: 3/5/03, 6/30/09, 6/4/14, 5/12/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 10/26/22, 6/27/23, 9/9/24, 10/14/25 **Supersedes**:	**Approved By**: Sandra M. Lindsey, CEO **Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: Kentera Patterson, Officer of Recipient Rights and Compliance **Additional Reviewers**: Holli McGeshick, Quality and Medical Records Supervisor Alecia Schabel, Continuing Education Supervisor Jennifer Keilitz, Director of Network Services, Public Policy, CE, EHS and OBRA
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		

Purpose:

Saginaw County Community Mental Health Authority (SCCMHA) is committed to ensuring the privacy and security of a person served health information in compliance with the HIPAA Privacy Rule (45 CFR §164.530(b)), Security Rule (45 CFR §164.308(a)(5)), the Michigan Mental Health Code (MCL 330.1748), and other applicable laws. To support our commitment to person served confidentiality, all employee of SCCMHA – including interns, volunteers, contractors, and applicable network providers - will receive appropriate training, regarding the policies and procedures for ensuring the secure and confidential receipt, transmission, storage, use and/or disclosure of protected health information.

Policy:

1. **Initial Training Requirement:**
    a. All new members of SCCMHA's workforce will receive HIPAA Privacy and Security training within 10 calendar days of initial employment or prior to being granted access to systems containing PHI.
    b. Training shall cover that HIPAA Privacy and Security Rules, SCCMHA privacy practices, and confidentiality under the Michigan Mental Health Code regarding the proper use and disclosure of protected health information.
2. **Ongoing and Refresher Training:**
    a. Training will occur upon initial employment, and at least annually or more frequently in response to:
        i. Significant updates to regulations, policies, or procedures.
        ii. Finding from internal audits or incidents involving PHI breaches.
        iii. Role changes involving new access to PHI or electronic systems.
    b. SCCMHA may supplement annual training with targeted modules or real-time alerts as needed.
3. **Role-Based Training Content:**
    a. Training will be tailored to the workforce member's role and job functions, ensuring understanding of:
        i. Proper use and disclosure of PHI,
        ii. Access limitations based on minimum necessary standards,
        iii. Incident reporting requirements,
        iv. Safeguards for electronic or paper-based PHI,
        v. Individual rights under HIPAA and the Michigan Mental Health Code.
4. **Documentation and Retention:**
    a. Completion of all training will be documented and tracked by the Continuing Education Department or the designated office.
    b. Records will be retained for a minimum of 6 years in compliance with 45 CFR §164.530(j).
5. **Enforcement and Sanctions:**
    a. Failure to complete required training within the designated timeframes may result in disciplinary action, up to suspension or termination of access to PHI.
    b. Workforce members are expected to maintain ongoing awareness of PHI confidentiality and must report potential violations to the Chief Compliance Officer immediately.

Application:
All SCCMHA Board operated programs, employees, interns, volunteers, contracted personnel, and applicable Network Providers.

Standards:

1. New employees will receive training within 10 days of initial employment.

2. Refresher training is required annually, or more frequently as needed based on changes or incidents.

Definitions:
Refer to SCCMHA Policy 08.05.00.01 – *Compliance Definitions* for:

- Protected Health Information (PHI)
- Disclosure
- Use
- Workforce

References:

- HIPAA Privacy Rule, 45 CFR §164.530(b) – Training Requirements
- HIPAA Security Rule, 45 CFR §164.308(a)(5) – Security Awareness and Training
- Michigan Mental Health Code, MCL 330.1748
- SCCMHA Human Resources - Temporary Employee Orientation checklist
- SCCMHA Policy 05.06.03 - Competency Requirements for the SCCMHA Provider Network

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. All new employees will receive training regarding the privacy and confidentiality of a person served health information within ten days of initial employment.	HIPAA Privacy Officer
2. Training will be provided to all employees whose functions are affected by a material change in the policies or procedures, within a reasonable period after the material change becomes effective.	HIPAA Privacy Officer
3. Training regarding the privacy and confidentiality of a person served health information will include the following: a. Uses and disclosures of protected health information for treatment, payment, and health care operations. b. Uses and disclosures of protected health information pursuant to person served consent. c. Uses and disclosure of protected health information pursuant to the person served opportunity to agree or disagree with the use or disclosure. d. Uses and disclosure of protected health information that do not require person served consent, or opportunity to agree or disagree. e. People served rights concerning their protected health information.	HIPAA Privacy Officer

f. Any other information as necessary for the respective members of the workforce to carry out their duties and responsibilities with respect to the proper use or disclosure of protected health information.	
4. Documentation regarding training for SCCMHA's workforce will be retained for a period of at least six years from the date of its creation or the date when it last was in effect, whichever is later.	SCCMHA Continuing Education Department

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Privacy Set: Marketing – Using and Disclosing PHI for Marketing	**Chapter**: 08 - Management of Information	**Subject No**: 08.05.15.01
Effective Date: April 14, 2003	**Date of Review/Revision**: 3/5/03, 6/30/09, 5/12/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 10/26/22, 6/27/23, 7/9/24, 10/14/25	**Approved By**: Sandra M. Lindsey, CEO
	Supersedes:	**Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Authored By**: Kentera Patterson, Officer of Recipient Rights and Compliance **Additional Reviewers**: Holli McGeshick, Quality and Medical Records Supervisor Ryan Mulder, Manager of the Office of the CEO Andrew Fergerson, Public Relations Specialist

Purpose:
Saginaw County Community Mental Health Authority (SCCMHA) is committed to ensuring the privacy and security of person served health information in all interactions, including those that support limited marketing activities, which may serve to solicit feedback relative to person served care and services. In alignment to the HIPAA Privacy Rule (45 CFR §164.508) and the Michigan Mental Health Code (MCL 330.1748) SCCMHA will ensure that any protected health information used or disclosed for marketing purposes will comply fully with all applicable federal, state, and/or local laws and regulations, including the proper authorization when required.

Policy:
1. **General Marketing Authorization Requirements:**

   a. SCCMHA will obtain a written authorization from the person served to use and disclose person served health information for the purpose of marketing, except as otherwise stated under HIPAA or state law.
2. **Exceptions – No Authorization Required:** SCCMHA may, without obtaining person served consent, use and disclose person served health information for the purpose of marketing only if:
   a. The communication is made face-to-face by SCCMHA staff to the individual.
   b. Communication involves a promotional gift of nominal value provided by SCCMHA.
   c. The communication is about a health-related product or service offered by SCCMHA and the communication is for treatment or care coordination.
3. **Prohibition of Sale of PHI for Marketing:** SCCMHA will not sell PHI or receive any form of direct or indirect remuneration in exchange for PHI for marketing purposes unless:
   a. The individual has signed a valid HIPAA authorization explicitly acknowledging the remuneration.
   b. Such disclosures are documented in compliance with 45 CFR §164.508(a)(4).
4. **Content of Required Authorizations:** When marketing requires authorization, the authorization must include:
   a. A clear description of the PHI to be used/disclosed.
   b. The name of the organization making and receiving the disclosure.
   c. The specific purpose of the marketing activity.
   d. An expiration date or event.
   e. A statement of the individual's right to revoke the authorization.
   f. Notice of potential redisclosure risk.
   g. A statement noting if SCCMHA is receiving compensation for the marketing disclosure.
   h. Signature and date of the individual or legal representative.
5. **Substance Use Disorder Records (42 CFR Part 2):**
   a. Marketing disclosures involving records of individuals receiving SUD services are subject to more stringent regulations under 42 CFR Part 2, which differ from HIPAA and require explicit written consent in compliance with SCCMHA Policy 08.05.01. SCCMHA 08.05.01 should be consulted prior to disclosing the records of a person served receiving SUD services from SCCMHA. Redisclosure of SUD-related information without consent is strictly prohibited.

Application:
All SCCMHA Board operated Programs and applicable Network Providers.

Standards:
1. SCCMHA will retain all authorizations for marketing disclosures for a minimum of six years, per 45 CFR §164.530(j).

2. Any marketing-related activities must be pre-approved by the Compliance Officer and the Office of CEO.

Definitions:
See SCCMHA Policy 08.05.00.01 Compliance Definitions

References:
HIPAA Privacy Rule, 45 CFR §164.508 – Marketing and Authorization Requirements
Michigan Mental Health Code: MCL 330.1748 – Confidentiality and Disclosures
42 CFR Part 2 – Substance Use Disorder Confidentiality
SCCMHA Policy 08.05.01 – 42 CFR Part 2 and Comp. Regarding the Use and Disclosure of SUD Patient Records

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. Except as otherwise provided in these procedures, SCCMHA will obtain person served consent for the purpose of marketing in accordance with the SCCMHA policy: Obtaining a Consent for Use or Disclosure of Treatment, Payment, Health Care Operations (TPO).	HIPAA Privacy Officer, Clerk Typist - Medical Records & ROI, appropriate clinical staff
2. If applicable, the consent for marketing will state that remuneration to SCCMHA is involved in the marketing activity, regardless of whether such remuneration is direct or indirect.	HIPAA Privacy Officer
3. Blanket consents for marketing will be considered by SCCMHA to be defective.	All SCCMHA staff
4. SCCMHA will document and retain the signed consent for a period of at least six years from the date of its creation or the date when it last was in effect, whichever is later.	HIPAA Privacy Officer, Clerk Typist – Medical Records & ROI
5. SCCMHA may, without obtaining person served consent, use or disclose PHI for the following purposes: a. to make a face-to-face marketing communication to a person served; and	HIPAA Privacy Officer, Clerk Typist - Medical Records & ROI

b. to provide a promotional gift of nominal value to the person served.	
6. SCCMHA will not disclose PHI to a business associate or other third party, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a marketing communication that promotes that entity's products or services.	HIPAA Privacy Officer, Clerk Typist - Medical Records & ROI
7. Consistent with the policies and procedures herein, SCCMHA may otherwise disclose protected health information to a business associate to assist in SCCMHA's marketing activities.	HIPAA Privacy Officer, Clerk Typist - Medical Records & ROI
8. SCCMHA may, without consent, communicate information to persons served: a. to describe a health-related product or service, or payment for such product or service, which is provided by, or included in a plan of benefits of SCCMHA. b. for treatment of the person served. c. for case management or care coordination for the person served; or d. to direct or recommend to the person served alternative treatments, therapies, health care providers or settings of care.	HIPAA Privacy Officer, Quality & Medical Records Supervisor, appropriate clinical staff
9. Knowledge of a violation or potential violation of this policy must be reported directly to the HIPAA Privacy Officer, Compliance Officer or to the Compliance hotline.	All SCCMHA staff

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Privacy Set: Recordkeeping - Documentation</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.05.16.01</td></tr>
<tr><td rowspan="2">Effective Date:
April 14, 2003</td><td>Date of Review/Revision:
3/5/03, 6/30/09, 6/4/14, 5/12/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 10/24/22, 6/27/23, 9/9/24, 10/14/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Kentera Patterson, Officer of Recipient Rights and Compliance / HIPAA Privacy Officer

Additional Reviewers:
Holli McGeshick, Quality and Medical Records Supervisor</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
This policy establishes SCCMHA's responsibility to develop, implement, and retain written or electronic documentation of all privacy-related policies and procedures, and other administrative documents. This supports SCCMHA's compliance with provisions of HIPAA Privacy and Security Rules (45 CFR §164.530(i)-(j)), Michigan Mental Health Code (MCL 330.1748), and 42 CFR Part 2, requiring provisions governing the documentation of policy revisions, communications, and workforce training.

Policy:
1. **Policy Development and Implementation:** SCCMHA will develop and implement written policies and procedures with respect to protected health information that are designed to comply with:
    a. HIPAA Privacy and Security Rule requirements
    b. the standards, implementation specifications, or other requirements of the 42 CFR Part 2 which focuses on confidentiality protections for SUD information.
    c. Michigan Mental Health Code provisions relating to health record confidentiality.

2. **Retention of Documentation:** SCCMHA will maintain documentation, in written or electronic form, of policies, procedures, communications, and other administrative documents as required by the HIPAA Privacy Rule, 45 CFR 164.530(i) and (j), for a period of at least six years from the date of creation or the date when last in effect, whichever is later. This includes:
    a. Current and former versions of HIPAA-related policies and procedures
    b. Records of complaints and their disposition
    c. Privacy practice notices
    d. Workforce privacy training logs
    e. Business Associate Agreements
    f. Consent and authorization forms
    g. Records required under 42 CFR Part 2 and the Michigan Mental Health Code.
3. **Timely Updates for Legal and Regulatory Changes:** SCCMHA will:
    a. Monitor updates to federal and state privacy laws and regulations
    b. Integrate required changes into its policies, procedures, and other administrative documents and any changes in law.
    c. Document any modifications and provide necessary training to impacted workforce members.
4. **Verification and Availability:** SCCMHA shall ensure all current documentation:
    a. Is readily retrievable for review by regulatory agencies
    b. Is accessible to employees on a need-to-know basis
    c. Reflects the most up-to-date compliance practices in accordance with HIPAA, 42 CFR Part 2, and state law.

Application:
All SCCMHA Board operated programs, departments, and applicable Network Providers involved in the use, disclosure, storage, or management of protected health information.

Standards:
1. All HIPAA Privacy and Security Rule related policies and documentation will be maintained for a period of six years from the date of creation or the date when last in effect, whichever is later consistent with 45 CFR §164.530(j).
2. Documentation related to SUD records sha

Definitions:
See SCCMHA Policy 08.05.00.01 – *Compliance Definitions* for definitions of:
- Protected Health Information (PHI)
- Documentation
- Use
- Disclosure

References:
HIPAA Privacy Rule: 45 CFR 164.530(i)-(j)
HIPAA Security Rule: 45 CFR §§164.306–316
Michigan Mental Health Code: MCL 330.1748

42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. SCCMHA's policies have been reasonably designed to consider the size and type of activities undertaken by SCCMHA with respect to protected health information.	HIPAA Privacy Officer
2. In implementing a change in the Notice of Privacy Practices, SCCMHA will: • Ensure that the policy or procedure, as revised to reflect a change in SCCMHA's privacy practice, complies with the standards, requirements, and implementation specifications of the Privacy regulations. • Document the policy or procedure as revised. • Revise the notice to state the changes in practice and make the revised notice available (see Policy, Notice of Privacy Practices – Content of Notice); and • SCCMHA will not implement a change in policy or procedure prior to the effective date of the revised notice.	HIPAA Privacy Officer
3. SCCMHA may change policies or procedures that do not affect the content of the Notice of Privacy Practices, provided that the policy or procedure complies with the Privacy regulations and is documented as required in this policy.	HIPAA Privacy Officer
4. The following documentation will be maintained in an organized manner: • Policies and procedures related to the use or disclosure of PHI. • Forms for the consent to use or disclose PHI.	HIPAA Privacy Officer

• Requests for the use or disclosure of PHI. • Agreements with business associates referring to the use or disclosure of PHI. • Notice of Privacy Practices and any changes made there too.	
5. Documentation will be maintained in a manner that allows necessary availability, while also ensuring the security of information.	HIPAA Privacy Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject
Individual Rights to PHI – Suspension</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.05.17.03</td></tr>
<tr><td rowspan="2">Effective Date:
April 14, 2003</td><td>Date of Review/Revision:
4/7/03, 6/30/09, 6/4/14, 5/12/16, 3/15/17, 6/1/18, 6/11/19, 8/1/21, 6/27/23, 9/9/24, 10/14/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Kentera Patterson, Officer of Recipient Rights and Compliance / HIPAA Privacy Officer</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure SCCMHA upholds the individual rights of people served by providing a clear process to request and receive an accounting of certain instances when protected health information about them is disclosed by a covered entity, in accordance with the HIPAA Privacy Rule 45 CFR §164.528, and to remain consistent with applicable provisions of the Michigan Mental Health Code. This requirement is subject to exceptions for disclosures made to the person served; for treatment, payment, and health care operations; or authorized by the person served; as well as certain time-limited exceptions for disclosures to law enforcement and oversight agencies. However, there are certain instances where the right to an accounting right may be 'suspended'. SCCMHA has developed policies and procedures to address the instances when the right to obtain an accounting of when protected health information has been used or disclosed for purposes other than treatment, payment, or health care operations have been suspended.

Policy:
1. **Accounting Rights:** SCCMHA will comply with the requirements set forth in 45 CFR §164.528, to allow people served to receive an account of all instances where protected health information about them is used or disclosed for a period of up to 6 years prior to the date of request, unless a shorter timeframe is requested.

2. **Exemptions from Accounting:** SCCMHA will allow persons served to receive an accounting of all instances where protected health information about them is used or disclosed, except for the following purposes:

(a) to carry out treatment, payment and health care operations.
(b) under the authority of a written authorization given by the subject of the protected health information.
(c) to the people served about their own protected health information.
(d) for SCCMHA's facility directory'
(e) to persons involved in the person served care or other notification purposes.
(f) for national security or intelligence purposes.
(g) to correctional institutions or law enforcement custodial situations.
(h) SCCMHA will not allow the person served to receive an accounting of instances where protected health information about them is used or disclosed prior to April 13, 2003.

3. **Temporary Suspension of Accounting Rights:** SCCMHA may temporarily suspend the individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, if:
    (a) That agency or official provides a written request stating that the accounting would impede their activities,
    (b) The suspension is for a specific, time-limited period
    (c) Verbal request may be temporarily (up to 30 days) honored pending a written follow-up.
4. **Documenting and Tracking Disclosures:** SCCMHA will utilize a chart completed by the medical records department for documenting and maintaining an account of when person served protected health information has been disclosed for purposes other than treatment, payment or health care operations. The information that must be logged includes:
    (a) The date of the disclosure
    (b) The name and address (if known) of the recipient
    (c) A brief description of the PHI disclosed
    (d) The purpose of the disclosure or a copy of the request

5. **Response Timelines:** SCCMHA will respond to requests no later than 60 calendar days from the receipt of the request. One 30-day extension is permitted if the individual is notified in writing of the delay and the reason.
6. **42 CFR Part 2 Considerations (SUD Information):** Records subject to the regulations under 42 CFR Part 2 differ from HIPAA. SCCMHA Policy 08.05.01 should be consulted prior to disclosing the records of person served receiving SUD services from SCCMHA.

Application:
All SCCMHA Board operated programs and applicable Network Providers.

Standards:
1. SCCMHA will act on the person served the request for an accounting not later than 60 days after the receipt of the request, with one allowable 30-day extension with written notice.
2. Logs will need to be retained for a minimum of 6 years from the date of disclosure.

Definitions:
Refer to SCCMHA Policy 08.05.00.01 – Compliance Definitions for:

- Protected Health Information (PHI)
- Disclosure
- Designated Record Set
- Authorization

References:
HIPAA Privacy Rule, 45 CFR §164.528 – Accounting of disclosures
HIPAA Privacy Rule, 45 CFR §164.530(j) – Documentation retention
Michigan Mental Health Code, MCL 330.1748
SCCMHA Policy 08.05.01 – 42 CFR Part 2 and Comp. Regarding the Use and Disclosure of SUD Patient Records

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. SCCMHA may temporarily suspend a person served right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency official.	HIPAA Privacy Officer
2. SCCMHA will obtain from such agency or official a written statement that such an accounting to the person served would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.	HIPAA Privacy Officer
3. If the health oversight agency or law enforcement official statement to suspend a person served right to receive an accounting of disclosure to that agency or official is made orally, SCCMHA will: (a) document the statement. (b) document the identity of the agency or official making the statement.	HIPAA Privacy Officer
4. If a person served right to an accounting of disclosures subject to the statement is temporarily suspended, SCCMHA will limit the temporary	HIPAA Privacy Officer

suspension to not longer than 30 days from the date of the oral statement.	
5. SCCMHA will extend the temporary suspension only pursuant to a written statement submitted from the agency or official during that time.	HIPAA Privacy Officer

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Information Technology Definitions	**Chapter**: 08 - Management of Information	**Subject No**: 08.06.00.01
Effective Date: 7/5/23	**Date of Review/Revision**: 9/9/24, 11/12/25 **Supersedes**:	**Approved By**: Sandra M. Lindsey, CEO
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: Christina Saunders **Additional Reviewers:**

Purpose:
The purpose of this policy is to establish standard definitions for all Information Technology and Information Security policies and procedures.

Policy:
All terms identified in this policy shall be referenced when they are used in any SCCMHA policies and procedures.

Application:
This policy applies to all staff, contractors, and business associates of SCCMHA.

Standards:
These definitions will be updated annually to reflect any additions or modifications that are needed.

A.

- **User Access or Authentication:** the ability to log into and use SCCMHA's information systems for clinical or administrative purposes by providing 2 points of authentication (2-Factor Authentication).
- **Access Reviews** is periodic evaluations of user access rights to ensure compliance with security policies.
- **Ambient temperature** the temperature of the air within a room, for purposes of this policy, this refers to server rooms, communication rooms, storage rooms, offices, and any other location which IT equipment is stored...

- **Anomalous Access** is any activity inconsistent with expected patterns, including high-volume record access or attempts to access restricted data.
- **Anti-virus software** the software that detects or prevents malicious software from entering a network or workstation.
- **Application Programming Interface (API)** a program that allows a developers to access certain data securely within other applications.
- **Audit Trail** is a chronological record of system activities that enables the reconstruction and examination of the sequence of events and transactions.
- **Authorized staff / personnel / users** Refers to a group of individuals, including staff, students, contractors**,** business associates and volunteers, engaged in the provision of SCCMHA (Saginaw County Community Mental Health Authority) services or business functions.
- **Authentication** is the process of verifying the identity of a user before granting access to a system or resource.
- **Authorization** is the process of granting or restricting access to specific systems, data, or functions based on a user's role.

B.

- **Backup** creating a retrievable, exact copy of data.
- **Breach** (defined by 45 CFR §164.402) is a violation of the HIPAA Privacy or Security Rule. The acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule, which compromises the security or privacy of the information.
- **Break the Glass** is a type of record access which is accessible by any user which requires them to document an explanation of why they need access to that record. and the user's actions when accessing these records are logged, tracked, and possibly monitored as needed.
- **Business Associate** as defined in 45 CFR §160.103: a person or entity that performs functions or services on behalf of a covered entity and receives, transmits, or maintains PHI.
- **Business Intelligence (BI)** is a technology driven process for analyzing data and delivering actionable information that helps executives, managers and workers make informed business decisions.

C.

- **Computer Resource** Any computer hardware, software, purchased computer service, and/or computer support services.
- **Confidential or Private Information** information that, if disclosed, could violate the privacy of individuals, or cause significant damage to the agency. Examples of confidential information are medical records, personnel records, operating plans, strategic plans, etc.
- **Confidentiality** when data or information is not to be made available or disclosed to unauthorized persons or processes.
- **Confidential medical information** individually identifiable health information in any form (paper or electronic) aka e-PHI (electronic patient health information).

- **Contingency Activation Notification** are the requirement that a BA or subcontractor notify the covered entity when its contingency (emergency) plan is activated.
- **Contingency Plan or Operations** procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations in the event of an emergency.
- **Controlled Access** is the practice of restricting access to systems, data, and physical areas to authorized individuals based on job responsibilities.

D.

- **Data Classification** is the categorization of data based on sensitivity levels to determine access restrictions.
- **Data Integrity (DI)** the overall accuracy, completeness, and consistency of data.
- **Disaster** means an event that causes harm or damage to SCCMHA information systems. Disasters include earthquakes, fires, extended power outages, equipment failures, or a significant computer virus outbreak.
- **C drive** the fixed, internal hard drive inside workstation PCs.
- **G drive** the network drive on which SCCMHA employees save business documents and data which apply to agency wide operations or department specific operations.
- **H drives** the network drive on which SCCMHA employees save their personal work files and data.
- **DRP (**Disaster Recovery Plan) a policy or procedure designed to assist an organization in executing recovery processes in response to a disaster to protect business IT infrastructure and promote expedited recovery.

E.

- **Electronic storage media** includes memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, digital memory card, or USB Drives.
- **Electronic protected health information (EPHI)** means individually identifiable electronic patient health information that is transmitted or maintained by electronic media.
- **Emergency** A situation where normal daily functioning has been interrupted to the point where the staff person can no longer function without having Information Systems render an immediate service to remedy the situation.
- **Encryption** means the conversion of data into scrambled or unreadable code which is only readable with a key known by the user.
- **External Service** An external IT service provided by an external vendor or provider.

F.

- **Facility Security Plan** policies and procedures to safeguard the facility and the equipment from unauthorized physical access, tampering, and theft.

G.

- **Generic or group identifier** a user ID that is shared by more than one user and does not uniquely identify an individual.

H.

- **Hardware** refers to the tools, machinery, and other durable equipment such as the computer's tangible components or delivery system that store and run the written instructions provided by the software.
- **Highly Sensitive Information** is data that requires the highest level of protection due to its potential impact if disclosed or accessed by unauthorized users.
- **HIPAA Privacy Rule** is the rule that requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.
- **HIPAA Security Rule** establishes national standards to protect individuals' electronic personal health information that is created, received, used, and maintained by a covered entity.

I.

- **Incident Response** is a structured approach to identifying, investigating, and mitigating security breaches or unauthorized access events.
- **Information Access Management** a framework to identify, track, control and manage authorized or specified users' access to a system.
- **Information Custodian** the staff designated by the owner to the responsible for maintaining safeguards established by the owner.
- **Information Owner** the staff responsible for creating the information.
- **Information system (IS)** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
- **Information Technology (IT)** equipment used for storing, retrieving, and sending data.
- I.S. Service: The scope of I.S. service includes, but is not necessarily limited to, Sentri II system work, PC workstation hardware issues, hardware set up, phone issues or set up, all questions or development work involving any SCCMHA license-owned software, network analysis and troubleshooting, proprietary databases, proprietary systems, operating systems, etc.
- **IT Equipment** this refers to old, retired pieces of computer hardware and software, printers, mice, keyboards, cables, monitors, or other PC peripherals
- **Internal Use** information that is intended for use by all employees when conducting agency business. Examples of internal use information are operational business reports, agency phone book, agency policies, standards and procedures, internal agency announcements, etc.
- **Internet Key Exchange (IKE)** a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN).

- **Internet Protocol Security (IPsec)** is a robust VPN standard that covers authentication and encryption of data traffic over the internet.
- **Internet Service Provider (ISP)** a company that provides subscribers with access to the internet.
- **Intranet** SCCMHA's internal website.
- **IS/IT Administrator** Staff and/or Department identified as the entity responsible for staff and equipment related to IS/IT Systems.

J.

K.

L.

- **Least Privilege Access (PoLP)** is the security principle that ensures users have only the minimum access necessary to perform their job functions.
- **Local Area Network (LAN) is** a computer network that links devices within a building or group of adjacent buildings.
- **Logical Access Controls** are technological measures used to restrict system and data access, such as passwords, encryption, and access logs.

M.

- **Management of Information Systems (MIS)** people, technology, organizations, and the relationships among them.
- **Monitoring and Logging** is the process of tracking and recording access to systems and data to detect suspicious activities.
- **Multi-Factor Authentication (MFA)** is a security mechanism that requires users to provide two or more verification factors to access a system.

N.

- **Need-to-Know Principle** is a security principle ensuring that individuals access only the information necessary for their tasks.
- **Network user** Any SCCMHA staff member that has a network account and uses a PC to connect to the network.

O.

P.

- **Peripherals** IT equipment that plugs into via cord, Wi-Fi, or Bluetooth such as cameras, microphones, speakers, keyboards, and mice.
- **Physical Access Controls** are security measures that restrict entry to facilities or specific areas where sensitive data is stored.
- **Physically Secure Area** an area where unauthorized persons do not have access to IT equipment. These areas must always be locked when the staff member is not present, even if only for a few minutes.
- **Privacy** ensuring the authorized control and access of electronic health information.
- **Privacy Officer** A person identified by the organization to administer Privacy Regulations. Typically, at SCCMHA the Compliance Officer is the Privacy Officer,

SCCMHA also requires all provider contract agencies to have a designated Privacy Officer.

- **Proprietary Information** information that belongs to SCCMHA.
- **Protected Health Information (PHI)** individually identifiable patient health information in any form (paper or electronic) that has been maintained or transmitted by a covered entity- that includes but is not limited to, AIDS/HIV information, mental health and developmental disabilities information, alcohol and drug abuse information, and other sexually transmitted disease information.
- **Point-to-Point Tunneling Protocol (PPTP)** a networking technology that supports multi-protocol virtual private networks (VPN), enabling remote users to access corporate networks securely across the Microsoft Windows operating systems and other point-to-point protocol (PPP)- enables systems to dial into a local internet service provider to connect securely to their corporate network through the internet.
- **Public Information is** information that has been made available for public distribution through authorized company channels. Examples of public information are the agency annual report, public service bulletins, newsletters, marketing brochures, advertisements, etc.
- **Purchased Computer Service** An external computer service. Such as, an Internet account, provided by an external vendor.

Q.

R.

- **Restoration** means the retrieval of files previously backed up and returning them to the condition they were at the time of backup.
- **Risk** means the likelihood of a given threat exercising a particular vulnerability and resulting impact of that event.
- **Role-based access control (RBAC)** is a means of restricting access to data or objects based on a user's role and the mapping of that user's role to a system-defined role.

S.

- **Satisfactory Assurances** are written assurances (typically via BAA) that the BA will comply with HIPAA standards including safeguards, incident reporting, etc.
- **Server files** All computer files that reside on the SCCMHA servers.
- **Secure Folder** A storage area where only the user or a select few are approved for access to a non-public folder the requesting individual must obtain permission from the "owner" of the folder and that employee's Director.
- **Security incident** (defined by 45 CFR §164.304) means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- **Security Measures** means security policies, procedures, standards, and controls.
- **Security Officer** a person identified by the organization to administer the HIPAA/HITECH Security Regulations. Typically, at SCCMHA the Security Officer is the Chief Information Officer.

- **Sentri** is the software system used to capture medical records, billing for fee or service reimbursement information. Also known as EHR- Electronic Health Record or EMR – Electronic Medical Record.
- **Share drive** A designated public or private drive set up as a work area for the Agency staff on the server.
- **Software Information systems**. **Examples include but are not limited to** software products that control Desktop computers, central processing computers, network servers, modems, scanners, printers, computer mice, computer cards, and any computer peripheral that is connected to any of the hardware. Exclusions to the definition of software are Fax machines, copiers, any computer-related supplies (I.E., wrist supports, glare screens, power plugs), and the phone system (if the phone system & the administrative computer system are not linked).
- **Subcontractor** as defined in 45 CFR § 160.103: a person to whom a BA delegates a function involving PHI.

T.

- **TDX Portal**: Saginaw County Community Mental Health Authority Team Dynamix Portal
- **The State Medicaid Health Information Technology Plan (SMHP)** provides the foundation for Medicaid health system transformation and administration that enables care coordination among clinicians.
- **Technical Evaluation** means an evaluation of the technical components of the computer network and related devices.
- **Transmission media** used to exchange information in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, Virtual Private Networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice, via telephone, are not considered transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission. **Two-Factor Authentication (MFA)** is a second method of authentication to ensure the person logging into the system is the intended user.

U.

- **Unauthorized Access** is any access to systems, data, or areas by an individual without proper authorization.
- **User** a person granted access to systems. OR employees authorized by the owner to access information and use the safeguards established by the owner.
- **User ID** an identifier chosen for the user to represent themselves when logging into the electronic health records or other network system. The User ID should never be changed, it is permanently associated that user.

V.

- **Virtual Private Network (VPN)** a method of tunneling securely through the internet to a network, whereby a personal PC becomes an extension of that private business's network allowing a user to access data files remotely.
- **Vulnerability** means a flaw or weakness in system security procedures, design, implementation, or internal controls that can be exploited and result in misuse or abuse of data.

W.

- **Workstation** An electronic computing device, for example, a laptop or desktop computer, tablet or any other device that performs similar functions, and electronic media stored in its immediate environment.
- **Workforce member** employees, volunteers, and other persons whose conduct, in the performance of work for SCCMHA, is under the direct control of SCCMHA, whether or not they are paid by SCCMHA. This includes full and part time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities who provide services to SCCMHA.

References:
None.

Exhibits:
None.

Procedure:
None

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Security Sanctions</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.06.04</td></tr>
<tr><td>Effective Date:
April 20, 2005</td><td>Date of Review/Revision:
9/13/22, 11/14/18, 9/8/04, 8/4/23, 9/9/24, 11/12/25
Supersedes:</td><td>Approved By:
Sandra M. Lindsey, CEO</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td><td>Responsible Director:
Amy Lou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Amy Lou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers:
Brett Lyon, Senior Applications, Information Security & BI Administrator
Chad Brown, Senior Data Warehouse and Applications Administrator
Ben Pelkki, Senior Database & Microsoft 365 Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Matthew Devos, Senior Network Administrator,
Fred Stahl, Director of Human Resources
Kentera Patterson, Officer of Recipient Rights and Compliance</td></tr>
</table>

Purpose:
To outline the procedures and criteria to *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."* as required under 45 CFR 164.308(a)(1)(ii)(C) and 164.530(e).
This policy ensures adherence to Health Insurance Portability and Accountability Act (HIPAA), the Confidentiality of Substance Use Disorder Patient Records regulation (42 CFR Part 2), and other relevant regulations by enforcing sanctions for violations to maintain the confidentiality, integrity, and availability of SCCMHA information systems.

Policy:
SCCMHA is committed to enforcing appropriate sanctions against workforce members who fail to comply with security policies and procedures.
Sanctions are designed to be fair and proportionate to the severity of the violation and to ensure compliance with all applicable laws and regulations.
Under HIPAA, penalties for misuse or misappropriation of health information can include both civil and criminal penalties. Civil penalties range from $100 for each violation to a maximum of $25,000 per year for the same violations. Criminal penalties vary from $50,000 and/or 1 year imprisonment to $250,000 and/or 10 years imprisonment (42USC §1320d).
Violations involving 42 CFR Part 2 – protected data, psychotherapy notes, or intentional disclosures of sensitive behavioral health information may be subject to additional disciplinary and legal actions.

Application:
This policy applies to all workforce members of Saginaw County Community Mental Health Authority (SCCMHA) including employees, contractors, subcontractors, network providers, temporary workers, interns, volunteers, and business associates with access to SCCMHA information systems or Protected Health Information (PHI).

Standards:
1. Compliance Requirements:
    - Obligation: All SCCMHA workforce members must comply with all applicable privacy, security, and confidentiality policies and procedures to ensure the confidentiality, integrity, and availability of SCCMHA information systems and PHI.
    - Education: SCCMHA will provide initial and ongoing training and resources to ensure that all members are aware of and understand the policies and procedures related to information security.
2. Application of Sanctions:
    - Sanction Levels: Sanctions will vary based on factors such as:
        i. The nature, scope, severity, and intent of the violation,
        ii. whether it was a one-time incident or part of a pattern of improper behavior,

iii. the impact on SCCMHA's operation and data security,

iv. Prior violations and corrective actions

- Types of Sanctions: Potential sanctions include, but are not limited to, verbal or written warnings, mandatory retraining, suspension, demotion, revocation of access, or discharge. The decision of appropriate sanctions will be made in accordance with SCCMHA's disciplinary processes.
- Consistency Review: Sanctions will be applied consistently across comparable incidents. The Compliance Department and Human Resources will jointly review proposed sanctions to ensure fairness and uniformity.

3. Investigation and Documentation:
    - Incident Reporting: All security violations must be reported to the designated security officer, privacy officer, or compliance department immediately upon discovery.
    - Investigation Process: An objective investigation will be conducted to determine the facts and extent of the violation, including interviews with parties involved and review of relevant documentation (access logs, records, etc.).
    - Documentation: All investigations, findings, sanctions, and corrective actions imposed will be documented thoroughly and maintained in accordance with SCCMHA record keeping policies.
    - Retention: Documentation of sanctions will be retained for a minimum of six (6) years from the date of its creation or the date it was last in effect, whichever is later.
4. Legal & Regulatory Notifications:
    - Severe Violations: Employees, agents, and other contractors should be aware that violations of a severe nature may result in notification to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.
    - Compliance: SCCMHA will cooperate with investigations conducted by the Office for Civil Rights (OCR), the Department of Health and Human Services (HHS), and other oversight authorities and provide necessary documentation and information.
5. Protection for Whistleblowers & Legal Rights:
    - Whistleblower Protections: The policy does not apply when members of SCCMHA's workforce acts as a whistleblower in accordance with HIPAA and 42 CFR Part 2. Employees are protected when activating the right to file a complaint with HHS, testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI.
    - Opposition to Unlawful Acts: Employees may oppose any act made unlawfully by HIPAA or related regulation; provided the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition

is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA Security Rule.

- Disclosure by Whistleblower: disclose protected health information as a whistleblower and the disclosure is in a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal option with regard to the whistleblower activity; or
- Victim Disclosure: an employee who is a victim of a crime and discloses protected health information to a law enforcement official, provided that the protected health information is about a suspected perpetrator of the criminal act and is limited to the information listed in the SCCMHA policy related to Disclosing Protected Health Information for Law Enforcement Release.

6. Post-Sanction Actions:
    - Remediation: Following any sanction, SCCMHA may require retraining, counseling, or other corrective action to prevent recurrence.
    - Monitoring: The Privacy and Security Officers will monitor repeated or systemic violations to identify training or policy improvement needs.

Definitions:
See IT/IS Policy 08.06.00.01 for definitions of terms used in this policy.

References:
- HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(C)
- HIPAA Privacy Rule, 45 CFR 164.530(e)
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
- SCCMHA Employee Handbook
- Policy 05.07.01 – Regulatory Management Policy
- SCCMHA Policy Number 801 – Information Technology

Exhibits
None

Procedure:

ACTION	RESPONSIBILITY
1. Sanctions for failure to comply with SCCMHA policies or procedures or with the requirements of HIPAA or 42 CFR Part 2 regulations will be made by the management of SCCMHA.	SCCMHA Management Team
2. All sanctioning of employees, agents and contractors will be documented and retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.	Officer of Recipient Rights and Compliance. HIPAA Privacy Officer. Director of Human Resources

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security - Security Management Process</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.01</td></tr>
<tr><td rowspan="2">Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/13/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers:
Brett Lyon, Senior Applications, Information Security & BI Administrator
Chad Brown, Senior Data Warehouse and Applications Administrator
Ben Pelkki, Senior Database & Microsoft 365 Administrator
Matthew Devos, Senior Network Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Fred Stahl, Director of Human Resources
Matthew Briggs, Chief of Network Business Operations
Chad Revell, Inventory Management and Mobile Device Specialist</td></tr>
<tr><td>Supersedes:
08.06.02</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA (Health Insurance Portability and Accountability) Security Rule, §164.308(a)(1) – Security Management Process, by establishing a framework for identifying, assessing, and managing risks to the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI) at SCCMHA. This policy also supports compliance with the HIPAA Privacy Rule, the 2023–2025 proposed HIPAA Privacy and Security Rule modernization provisions, and 42 CFR Part 2 confidentiality requirements for behavioral health information. SCCMHA will integrate these frameworks to ensure that all electronic systems and administrative processes uphold the highest standards of data protection, patient confidentiality, and breach accountability.
Policy:
SCCMHA will develop, implement, and maintain policies and procedures to prevent, detect, contain, and correct security violations related to the EPHI. SCCMHA will designate a HIPAA Security Officer responsible for implementing and maintaining administrative, technical, and physical safeguards that meet the requirements of §164.308, §164.310, and §164.312. This includes conducting regular risk assessments, implementing appropriate security measures, and enforcing compliance with HIPAA requirements.
SCCMHA's security management program will also incorporate procedures for identifying and reporting cybersecurity events, ransomware attacks, and potential breaches of unsecured PHI, consistent with OCR and HHS guidance on emerging cybersecurity threats.

Application:
This policy applies to SCCMHA, its business associates, and subcontractors who require access to or use of EPHI to fulfill their contractual obligations. Business associates and subcontractors may choose to adopt SCCMHA's policies or develop their own, provided they comply with the applicable sections of the HIPAA Security Rule. Business Associates and subcontractors must provide documentation of their Security Rule compliance, including their own risk analyses, upon request. SCCMHA will maintain and periodically review signed Business Associate Agreements (BAAs) to verify current compliance.

Violations of this policy may result in disciplinary action up to and including termination of employment or contract. Compliance with this policy is mandatory for all relevant parties, and SCCMHA will ensure adherence through regular reviews, monitoring, and enforcement measures.

Standards:
Policies and procedures to prevent, detect, contain, and correct security violations related to the EPHI of SCCMHA consumers will be implemented.

A. Risk Identification and Assessment:
    - Risk Identification: SCCMHA must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI. Security Risk Assessment (SRA): An accurate and thorough SRA (Security Risk Assessment) of the potential risks and vulnerabilities. This assessment will include:

i. Inventory and Assessment: All information systems that house EPHI are to be identified and periodically inventoried, including all hardware and software that are used to collect, store, process, or transfer EPHI.

- The SRA Components:
  i. The SRA & Process- Evaluation of the overall SRA process.
  ii. Security Policies – Review of existing security policies.
  iii. Security & Workforce – Assessment of workforce training and compliance.
  iv. Security & Data - Evaluation of data protection measures.
  v. Security & the Practice – Review of security practices and procedures.
  vi. Security & Business Associates – Assessment of security measures related to business associates
  vii. Contingency Planning – Evaluation of contingency plans and disaster recovery measures.
- Risk Analysis Methodology: The method of risk analysis SCCMHA chooses must be based on the following steps:
  i. Inventory. SCCMHA must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems.
  ii. Threat identification. SCCMHA must identify all potential threats to its information systems containing EPHI. Such threats may be natural, human, or environmental.
  iii. Vulnerability identification. SCCMHA must identify all vulnerabilities on its information systems containing EPHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.
  iv. Security control analysis. SCCMHA must analyze the security measures implemented or will be implemented to protect its information systems containing EPHI; this includes both preventive and detective controls.
  v. Risk likelihood determination. SCCMHA must assign ratings to specific risks that indicate the probability that a vulnerability will be exploited by a particular threat. Three factors should be considered: 1) threat motivation and capability, 2) type of vulnerability, and 3) existence and effectiveness of current security controls
  vi. Impact analysis. SCCMHA must determine the impact to confidentiality, integrity or availability that would result if a threat were to successfully exploit a vulnerability on a SCCMHA information system containing EPHI.
  vii. Risk Determination. SCCMHA must use the information obtained in the above six steps to identify the level of risk to specific information systems containing EPHI. For each vulnerability and associated threat, SCCMHA must make a risk determination based on:

1. The likelihood a certain threat will attempt to exploit a specific vulnerability.
2. The level of impact should the threat successfully exploit the vulnerability.
3. The adequacy of planned or existing security controls.

viii. Documentation: The results of each of the above steps must be formally documented and securely maintained. The above steps do not prescribe any method, but the method selected for the Risk Analysis should address all the concerns. The Security Risk Analysis will be reviewed and updated annually and whenever there are significant changes to technology, workflows, or threats (e.g., introduction of new software, telehealth platforms, or data-sharing partnerships). SCCMHA will align its process with NIST SP 800-66 Revision 2 and 800-30 Revision 1.

B. Security Measures:

- Implementation: SCCMHA will implement a documented Risk Management plan that prioritizes corrective actions identified through the Security Risk Assessment. This plan will include implementation timelines, responsible parties, and evidence of follow-through. Additionally, implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a) of the HIPAA Security Rule will be implemented. Specifically, SCCMHA must:

    1. Confidentiality, Integrity & Availability: Ensure the confidentiality, integrity, and availability of all EPHI that SCCMHA creates, receives, maintains, or transmits,

    2. Threat & Hazard Protection: Protect against any reasonably anticipated threat or hazard to the security or integrity of such information,

    3. Unauthorized Use or Disclosure: Protect against any reasonably anticipated use or disclosure of such information that are not permitted or required under the HIPAA Security Rule, and

    4. Workforce Compliance: Ensure compliance with the HIPAA Security Rule by its workforce. SCCMHA will employ layered technical safeguards including encryption of ePHI in transit and at rest, multifactor authentication (MFA) for all remote or privileged access, and endpoint protection measures. Encryption key management and device-level protections will follow NIST 800-111 standards. Physical safeguards, including facility access controls (Policy 08.06.10.01) and workstation security (Policy 08.06.10.04), will be reviewed annually to ensure continued protection of systems containing ePHI.

C. Workforce Training & Compliance:
- Training: SCCMHA workforce members are expected to comply with all applicable policies and procedures related to the HIPAA Security Rule. Training will be issued prior to being issued a user ID and access to ePHI, annual refresher training is required. Additional training will be provided for high-risk positions (e.g., IT, billing, clinical documentation, or compliance staff). All workforce members must complete privacy and security awareness updates within 30 days of any significant policy or technology change. Training completion will be tracked and documented.
- Sanctions: SCCMHA will apply appropriate sanctions against members of its workforce who fail to comply with SCCMHA policies and procedures, including disciplinary action up to and including discharge in compliance with the SCCMHA Employee Handbook. Members of the SCCMHA workforce should be aware that severe violations may result in notification to law enforcement officials and regulatory, accreditation, and/or licensure organizations (see SCCMHA Policy *08.06.04 – HIPAA Security, Security Sanctions* for more information.

D. Monitoring & Review:
- Activity Review: regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports will be implemented.
- Incident management: Procedures will be established for reporting, investigating and documenting security incidents. The Security Incident Log will be maintained and reviewed by the SCCMHA Compliance and Policy Team.
- SCCMHA will conduct periodic internal audits of system access and security controls. The HIPAA Security Officer will ensure that audit results are reviewed by executive management and that corrective actions are implemented promptly.
- SCCMHA will establish a breach detection and response plan that defines timeframes, roles, and notification procedures consistent with the HIPAA Breach Notification Rule (§164.400–414) and the 42 CFR Part 2 confidentiality standards.

E. Business Associate and Subcontractor Compliance:
- Contractual Requirements: Business Associates and subcontractors must adhere to SCCMHA's policies or develop their own, compliant with the HIPAA Security Rule. SCCMHA will review and ensure compliance with these requirements. SCCMHA will maintain a centralized Business Associate inventory and ensure all vendors with access to ePHI have executed current, compliant BAAs. BAAs will include provisions requiring subcontractors to adhere to equivalent safeguards and promptly report any security incident or breach within 24 hours of discovery.

Definitions:
See SCCMHA Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.308(a)(1)
- The HIPAA Security Rule §164.306(a)
- SCCMHA Policy Number 201 – Standards of Conduct
- SCCMHA Policy Number 205 – Corrective Action
- SCCMHA Policy Number 801 – Information Technology
- NIST SP 800-30

Procedure:

ACTION	RESPONSIBILITY
Identify Relevant Information Systems	
1. Identify all information systems that house EPHI, including hardware and software used to collect, store, process, or transmit EPHI.	1. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team
2. Analyze business functions and verify ownership and control of information system elements, as necessary.	2. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team
Conduct Risk Assessment	
3. An accurate and thorough SRA of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by SCCMHA and its Business Associates will be conducted periodically and as needed. a. Findings from each Security Risk Assessment will be reviewed by the HIPAA Security Officer, Compliance Officer, and Executive Management. Identified risks will be prioritized, documented, and addressed through a corrective action plan.	3. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team

Implement a Risk Management Program	
4. Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level (See Section 164.306(a) of the HIPAA Security Rule) will be implemented, inclusive of SCCMHA's Business Associates and Contract Providers.	4. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team Director of Human Resources
Develop and Implement a Sanction Policy	
5. Appropriate sanctions against workforce members who fail to comply with the security policies and procedures will be applied.	5. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team
Develop and Deploy the Information System Activity Review Process	
6. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 7. Implement and maintain an Incident Response and Breach Notification Procedure that outlines how to identify, document, mitigate, and report suspected or confirmed breaches of ePHI in compliance with HIPAA and 42 CFR Part 2. 8. Review and update this policy annually or as needed to reflect changes in regulations, guidance, or organizational structure.	6. HIPAA Security Officer Senior Database & Microsoft 365 Administrator IT/IS Team

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Assigned Security Responsibility</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.02</td></tr>
<tr><td>Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
8/31/22, 8/2/23, 9/9/24, 11/12/25
Supersedes:
08.06.06</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer & HIPAA Security Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer & HIPAA Security Officer

Additional Reviewers:
None</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.308(a)(2) – Assigned Security Responsibility, by defining the roles and responsibilities of individuals responsible for developing, implementing, and maintaining security policies and procedures at SCCMHA.

Policy:
SCCMHA will appoint a designated HIPAA Security Officer responsible for development, implementation, and enforcement of security policies and procedures required by the HIPAA Security Rule for SCCMHA. This individual will serve as the point contact for all HIPAA Security-related matters.

Application:
The HIPAA Security Rule and this Policy apply to all SCCMHA staff, contractors, interns, volunteers, business associates, and any subcontractor who create, access, maintain, or transmit PHI as part of behavioral health service delivery.
Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule.

Violations of this policy will result in appropriate disciplinary action up to and including termination of employment or contract. Non-compliance with HIPAA Security Rule requirements may also result in legal and regulatory consequences**.**

Standards:

A. Appointment and Responsibilities of the HIPAA Security Officer

- Designation**:** SCCMHA will appoint a HIPAA Security Officer who will be responsible for all aspects of HIPAA Security Rule compliance.
- Responsibilities: The identified SCCMHA HIPAA Security Officer will have responsibility for:
    1. Oversight & Development: Oversight, development, and communication of security policies and procedures.
    2. Communication: Ensure effective communication of security policies and procedures to all relevant staff and stakeholders.
    3. Risk Assessment: Conducting the risk assessment required under the HIPAA Security Rule §164.308(a)(1)(i).
    4. Security Evaluations: Reviewing the results of periodic security evaluations and continuous monitoring required under §164.308(a)(1)(ii)(D) and communicating those results to the SCCMHA Compliance and Policy Team.
    5. Addressing Security Concerns: Ensuring that security concerns have been appropriately addressed. Implementing corrective action and follow up to verify that issues have been resolved.
    6. Documentation: Maintain comprehensive records of all security activities, including risk assessments, security evaluations, incident reports, and corrective actions taken. All documentation required by the HIPAA Security Rule—including risk analyses, security evaluations, and incident response records—will be maintained for a minimum of six (6) years from the date of creation or last effective date, whichever is later.
- The HIPAA Security Officer shall coordinate with the HIPAA Privacy Officer to ensure that all security policies and procedures support timely, secure electronic access to PHI and align with the minimum necessary and disclosure requirements under the HIPAA Privacy Rule and 42 CFR Part 2.

B. Implementation and Monitoring:

- Policy Development: The HIPAA Security Officer will develop policies and procedures that meet the requirements of the HIPAA Security Rule, including those for:
    - Access Control: Policies for granting, modifying, and terminating access to PHI.
    - Data Protection: Procedures for safeguarding PHI against unauthorized access, use, and disclosure.
    - Incident Response: Protocols for responding to and managing security incidents and breaches.

- Training and Awareness: Programs for training staff on security policies and procedures and raising awareness about security risks. Monitoring & Enforcement: The HIPAA Security Officer will:
    - Continuous Monitor: Oversee continuous monitoring of security controls and systems to ensure ongoing compliance.
    - Periodic Reviews: Conduct periodic reviews and updates of security policies and procedures to address new threats, vulnerabilities, and changes in regulations.
    - Incident Management: Manage and coordinate responses to security incidents, including conducting investigations, documenting findings, and implementing corrective actions.
- SCCMHA will implement cybersecurity safeguards consistent with HHS Cybersecurity Performance Goals, including but not limited to multi-factor authentication, encryption of data at rest and in transit, endpoint protection, and regular patch management and system updates.

C. Reporting and Accountability:

- Reporting: the HIPAA Security Officer will report directly to the Chief Compliance Officer and SCCMHA Compliance and Policy Team to provide regular updates on the status of security policies, risk assessments, and security evaluations.
- Accountability: The HIPAA Security Officer is accountable for ensuring that all security measures are effectively implemented and adhered to. This includes holding relevant staff accountable for compliance with security policies and procedures.
- All suspected or confirmed security incidents must be reported immediately to the HIPAA Security Officer. The Officer shall document all incidents, risk assessments, mitigation steps, and notifications in accordance with SCCMHA's *08.05.03.03 - HITECH Breach Notification Protected Health Information* Policy.

D. Compliance and Training:

- Compliance: Ensure that SCCMHA's security policies and procedures comply with the HIPAA Security Rule and other applicable regulations.
- Training: Oversee the development and delivery of training programs to educate staff on security policies, procedures, and their roles in maintaining compliance.
- Training shall include role-specific content to ensure workforce members understand how their access level relates to security responsibilities, least-privilege principles, and behavioral-health-specific confidentiality requirements.

E. Business Associate and Subcontractor Oversight

- Monitoring: Monitor and ensure that business associates and subcontractors adhere to the security policies and procedures, either through direct oversight or through contractual requirements. Information regarding BAAs can be found in Policy 08.06.08.09: BAAs and other Arrangements.
- The HIPAA Security Officer shall periodically review Business Associate compliance through documented assessments, audits, or attestation of adherence to SCCMHA's security standards.
- Contractual Compliance**:** Ensure that business associate agreements and subcontractor contracts include provisions for compliance with HIPAA Security Rule requirements.

- For patient records subject to 42 CFR Part 2, the HIPAA Security Officer will ensure that electronic safeguards prevent unauthorized access, use, or redisclosure of substance use disorder information, and that all staff are trained on Part 2 requirements.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:
- The HIPAA Security Rule §164.308(a)(2)
- SCCMHA Policy 08.06.08.04 – HIPAA Security, Information Access Management
- SCCMHA Policy 08.06.08.06 – HIPAA Security, Security Incident Procedures
- SCCMHA Policy 08.05.03.03 – HITECH Breach Notification Protected Health Information
- SCCMHA Job Description – Chief Information Officer | Chief Quality and Compliance Officer

Procedure:

ACTION	RESPONSIBILITY
1. Identify the security official responsible for developing and implementing the policies and procedures required by the HIPAA Security Rule.	1. Chief Information Officer | Chief Quality and Compliance Officer
2. Document this assignment to one individual's responsibilities in a job description.	2. Chief Information Officer | Chief Quality and Compliance Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Workforce Security</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.03</td></tr>
<tr><td rowspan="2">Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/13/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers: Fred Stahl, Human Resources Director
Brett Lyon, Senior Applications, Information Security & BI Administrator
Ben Pelkki, Senior Database & Microsoft 365 Administrator
Matthew Devos, Senior Network Administrator, Mark Sauve, Senior Systems & Desktop Support Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Melissa Gutzwiller - Environmental Services, Customer Service, Security</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To assure compliance with the HIPAA Security Rule, §164.308(a)(3) – Workforce Security by establishing and maintaining policies and procedures that regulate workforce access to Electronic Protected Health Information (ePHI) and prevent unauthorized access.

Policy:

SCCMHA will implement comprehensive policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the HIPAA Privacy Rule, and to prevent those workforce members who do not have appropriate access under the HIPAA Privacy Rule from obtaining access to electronic protected health information. SCCMHA implements Zero Trust security principles and 42 CFR Part 2 safeguards to ensure confidentiality of behavioral-health and substance-use information.
For workforce members handling behavioral health or substance use disorder information, SCCMHA will implement heightened confidentiality safeguards consistent with 42 CFR Part 2, including access logging, redisclosure prohibitions, and specialized workforce training.

Application:
The HIPAA Security Rule, and this Policy, applies to SCCMHA, its business associates, and any subcontractor that is required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule.

Compliance with this policy is mandatory. Violations of the policy will result in disciplinary action, up to and including termination of employment or contract. Non-compliance may also lead to legal and regulatory consequences.

Standards:
Authorization and Supervision: Procedures will be developed and implemented for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed with be implemented.
The HIPAA Security Officer shall coordinate with the HIPAA Privacy Officer to ensure that workforce authorization, supervision, and access controls align with the Privacy Rule and 42 CFR Part 2 requirements, including the ‘minimum necessary’ and redisclosure limitations for behavioral health and substance use disorder information.

A. Access Authorization:
    - Access Request: All requests for access to EPHI must be documented and submitted through a formal process, including justification for access based on job role and responsibilities.
    - All access requests, modifications, and terminations will be documented and tracked through SCCMHA’s approved IT ticketing system to ensure accountability and auditability.
    - Role-Based Access: Access to EPHI will be granted based on the principle of least privilege, meaning access will be limited to the minimum necessary for the performance of job duties.
    - Authorization Review**:** Access requests will be reviewed and approved by designated managers or supervisors in coordination with the Security Officer. Access will only be granted after approval is obtained.

- User Authentication: All authorized workforce access to ePHI will require secure authentication methods such as multi-factor authentication (MFA). Access credentials must be unique and never shared. ePHI must be encrypted at rest and in transit consistent with SCCMHA technical safeguard standards.

B. Supervision:
- Monitoring Access: Workforce members who have access to EPHI will be subject to regular monitoring to ensure that access is appropriate and that no unauthorized activities occur.
- Training: All workforce members with access to EPHI will receive training in data protection policies, security protocols, and their responsibilities under the HIPAA Privacy and Security Rules. Role-based training requirements will be managed through SCCMHA's Learning Management System (LMS) and assigned automatically during onboarding or role change.

C. The Chief Information Officer retains authority to approve or deny any user account activation, modification, or deactivation when necessary to maintain system security or operational continuity.

Access Appropriateness: Procedures will be developed and implemented to determine that the access of a workforce member to EPHI is appropriate.

A. Periodic Review:
- Access Reviews: Access to EPHI will be reviewed periodically, at least annually, and upon any significant role, system, or employment status change to ensure that privileges remain appropriate. This review will be conducted by the IT Access & Identity Management Team and will include verifying that current access aligns with the individual's job role and responsibilities.
- Adjustments**:** Any changes in job roles, responsibilities, or employment status that affect access to EPHI will trigger a review of access privileges. Adjustments will be made as necessary to ensure compliance with the principle of least privilege.

B. Access Justification:
- Documentation: Each workforce member's access to EPHI will be documented, including the rationale for access and the specific EPHI accessed. Documentation will be maintained and available for audit purposes.
- Authorization Record: The Security Officer will maintain a record of all access authorizations, including approvals, modifications, and terminations.

Termination of Access: Procedures for terminating access to EPHI when the employment of, or other arrangement with, a workforce member ends.

A. Access Termination Procedures:
- Exit Process: When a workforce member's employment or other arrangement ends, their access to EPHI will be promptly terminated. This includes deactivating user accounts, retrieving access credentials,

and revoking physical access to areas where EPHI is stored or processed.

- Notification**:** The Security Officer and IT department will be notified immediately of any termination or changes in employment status to initiate the access termination process.

B. Access Revocation:

- Revocation Process: Procedures for revoking access will be in place to ensure that access rights are promptly adjusted or removed in response to role changes or termination. Access will be terminated within 24 hours of notification; for involuntary separations or security risks, termination will occur immediately.
- Audit and Verification: After access termination, the IT department will conduct an audit to verify that all access rights have been removed and that no unauthorized access has occurred.

Enforcement and Compliance:

A. Compliance Monitoring:

- Regular Audits: SCCMHA will conduct regular audits to ensure compliance with access control procedures and identify any potential gaps or issues in access management.
- Compliance Reports: Regular reports will be generated and reviewed by the SCCMHA Compliance and Policy Team to monitor compliance with access control policies and procedures.

B. Sanctions:

- Disciplinary Actions: Workforce members who fail to comply with access control policies and procedures will be subject to disciplinary actions as outlined in the SCCMHA Employee Handbook. This may include corrective actions, retraining, or termination of employment.
- Incident Reporting**:** Any suspected or actual unauthorized access to EPHI will be reported to the Security Officer and investigated. Appropriate actions will be taken to address and rectify the situation. Workforce members must immediately report any suspected unauthorized access, disclosure, or security incident to the HIPAA Security Officer. Reports shall be documented and investigated in accordance with SCCMHA's *08.05.03.03 – HITECH Breach Notification PHI* Policy.

C. Business Associate Oversight:

- Business Associates and subcontractors accessing SCCMHA systems must meet equivalent workforce-security standards. The HIPAA Security Officer will ensure verification through periodic compliance attestations or audits.

Documentation and Record Keeping:

A. Policy Documentation:

- Policy Access: All policies and procedures related to workforce security will be documented and made accessible to relevant staff.

- Record Maintenance**:** Documentation of access authorizations, changes, terminations, and periodic reviews will be maintained securely and retained for a minimum of six (6) years from the date of creation or last effective date, whichever is later or as required by applicable regulations.

Definitions:
See IT/IS Policy **08.06.00.01** which contains a comprehensive list of relevant words and terms used within the Policies of this section.

References:
- The HIPAA Security Rule §164.308(a)(3)
- The HIPAA Privacy Rule - 45 CFR Part 160 and Part 164, Subparts A and E
- SCCMHA Policy 08.04.02 - Electronic Health Record Identity and Access Management
- SCCMHA Procedure 09.07.01.16 – Activation-Deactivation-Change of Staff User Accounts
- SCCMHA Policy 08.06.08.09 – Business Associates Agreements

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Procedures for Authorization and/or Supervision	
1. Procedures will be developed and implemented for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.	Environmental Services, Customer Service, Security, HIPAA Security Officer, Senior Systems & Desktop Support Administrator, Senior Applications, Information Security & BI Administrator, Senior Database & Microsoft 365 Administrator
Establish Clear Job descriptions and Responsibilities	
2. Define roles and responsibilities for all job functions	Human Resources Director
3. Assign appropriate levels of security oversight, training, and access	IT Department Staff

4. Identify in writing who has the business need, and who has been granted permission, to view, alter, retrieve, and store EPHI, and at what times, under what circumstances, and for what purposes.	Human Resources Director
Establish Criteria and Procedures for Hiring and the Assignment of Tasks	
5. Ensure that members of the workforce have the necessary knowledge, skills, and abilities to fulfill roles, and that these requirements are included as part of the hiring process.	Human Resources Director
Establish a Workforce Clearance Procedure	
6. Implement procedures to determine that the access of a workforce member to EPHI is appropriate.	IT Department Staff HIPAA Security Officer, Senior Applications, Information Security & BI Administrator, Senior Database & Microsoft 365 Administrator
7. Implement a procedure for obtaining clearance from appropriate offices or individuals where access is provided or terminated.	Human Resources Director
Establish Termination Procedures	
8. Implement procedures for terminating access to EPHI when the employment of a workforce members ends or as required by determinations made as specified in the Policy.	Human Resources Director

9. Develop a standard set of procedures that should be followed to recover access to control devices, (identification [ID] badges, keys, access cards, etc.) when employment ends.	HIPAA Security Officer, Senior Applications, Information Security & BI Administrator, Senior Database & Microsoft 365 Administrator
10. Deactivate computer access accounts (e.g., disable user IDs and passwords).	Senior Systems & Desktop Support Administrator, Senior Applications, Information Security & BI Administrator, Senior Database & Microsoft 365 Administrator IT Department Staff

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Security: Information Access Management & Access Control	**Chapter**: 08 – Management of Information	**Subject No**: 08.06.08.04
Effective Date: October 01, 2020	**Date of Review/Revision**: 7/14/23, 8/4/23, 9/9/24, 11/12/25 **Supersedes**:	**Approved By**: Sandra M. Lindsey, CEO
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer **Reviewers**: Brett Lyon, Senior Applications, Information Security & BI Administrator Chad Brown, Senior Data Warehouse and Applications Administrator Ben Pelkki, Senior Database & Microsoft 365 Administrator David Wolfcale, Systems, Information Security & Microsoft 365 Administrator Matthew Devos, Senior Network Administrator

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.308(a)(4) – Information Access Management and to safeguard electronic protected health information (ePHI) against unauthorized access. This policy also supports compliance with the 2023–2025

proposed HIPAA Privacy Rule modernization efforts that strengthen individual access rights, business associate accountability, and role-based least privilege enforcement. SCCMHA's procedures ensure that access to ePHI is documented, auditable, and traceable across all systems, applications, and third-party integrations.

Policy:
SCCMHA is committed to implementing and maintaining robust policies and procedures for authorizing access to EPHI. These measures will align with the applicable requirements of the HIPAA Privacy Rule Subpart E (Privacy of Individually Identifiable Information) of CFR §164. SCCMHA will apply the "Zero Trust" security principle to access management—requiring continuous verification of user identity, device security, and contextual risk before granting or maintaining access to systems containing ePHI.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule.

Standards:

A. Access Authorization:
- SCCMHA will establish and enforce policies and procedures for granting, managing, and terminating access to EPHI. This includes controlling access to workstations, transactions, programs, processes, or other mechanisms used to handle PHI.
- Access will be granted based on the principles of least privilege, ensuring that individuals have the minimum necessary access required to perform their job functions.
- Access authorization decisions, including the role assigned, approval source, and justification, will be documented and retained for at least six (6) years in accordance with HIPAA §164.316(b)(2)(i).
- Temporary or emergency access accounts must be approved by IT leadership and automatically expire within 48 hours unless renewed.

B. Access Control Procedures:
- **Role-Based Access Control (RBAC):** Access to EPHI will be assigned based on job roles and responsibilities. Each role will have predefined access levels that reflect the need to know and perform job functions.
- **Authentication Mechanisms**: Access to systems containing EPHI will require strong authentication mechanisms, such as passwords and multi-factor authentication (MFA).
- **Access Reviews**: SCCMHA will conduct regular reviews and audits of user access rights to ensure that access is appropriate and reflects current job functions. Any unnecessary or outdated access rights will be promptly adjusted or revoked.

i. Each review will confirm alignment with current job responsibilities, least privilege principle, and behavioral health confidentiality rules (42 CFR Part 2).
ii. Access discrepancies discovered during review must be corrected within five (5) business days.
iii. Access reviews for privileged accounts (e.g., system administrators) will occur monthly.

- **Access Modifications**: Procedures for modifying access rights will be documented and enforced to ensure that changes in job roles, responsibilities, or employment status are reflected in access privileges in a timely manner.
- **Business Associate Access Controls:** Access for business associates and subcontractors to SCCMHA systems or shared drives must be time-bound, documented, and verified through an active Business Associate Agreement (BAA) in accordance with §164.314(a).

C. Security measures:

- **Physical Security**: Access to physical workstations and systems where EPHI is stored or processed will be secured against unauthorized access through measures such as locked facilities, secure rooms, and controlled access points.
- **Technical Safeguards**: Systems handling EPHI will have technical safeguards in place, including encryption, firewalls, and intrusion detection systems, to protect against unauthorized access and cyber threats.
- **Endpoint and Remote Access Controls**: All remote access to SCCMHA systems or ePHI (including VPNs, mobile devices, and telehealth systems) will use multifactor authentication (MFA) and device compliance checks prior to granting access.
- Data Loss Prevention (DLP) and audit logging tools must be enabled to detect and alert on unauthorized copying, downloading, or transmission of ePHI.
- **Training and Awareness**: All employees, business associates, and subcontractors will receive training on access management policies, the importance of safeguarding EPHI, and the procedures for reporting security incidents or breaches.

D. Sanctions and Enforcement:

- Violations of this policy, including unauthorized access, credential sharing, or failure to complete access reviews, will result in disciplinary action up to and including termination, consistent with SCCMHA's Sanctions Policy (§164.530(e)) and applicable labor agreements. Confirmed violations involving ePHI may also be reported to federal authorities as required under the HIPAA Breach Notification Rule (§164.404–§164.410).

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- HIPAA Privacy Rule Subpart E
- CFR §§164
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
- The HIPAA Security Rule §164.312(a) – Access Control
- The HIPAA Security Rule §164.312(d) – Person or Entity Authentication
- The HIPAA Security Rule §164.316 – Policies and Procedures and Documentation Requirements
- The HIPAA Privacy Rule §164.502(b) – Minimum Necessary Standard
- SCCMHA 08.06.12.04 – *HIPAA Security, Person, or Entity Authentication*
- SCMCHA PROPOSED – *Controlled Access & Least Privilege Access Policy*
- SCCMHA 08.06.08.09 – HIPAA Security, Business Associate Agreement (BAAs), and other Arrangements
- SCCMHA 08.06.16.01 – HIPAA Security, Policies, Procedures, and Documentation
- NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-63B – Digital Identity Guidelines
- SAMHSA Behavioral Health IT and 988 Data Protection Guidance (2023–2025 Updates)
- State of Michigan Department of Health and Human Services (MDHHS) HIPAA Implementation Guidance
- U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), Proposed Modifications to the HIPAA Privacy Rule (2024–2025)

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Implement Policies and Procedures for Authorizing Access	
1. Policies and Procedures for granting and restricting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism, will be implemented.	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer Senior Applications, Information Security & BI Administrator
2. Access control methods will be evaluated and applied (e.g., identity based, role-based, or other	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer,

reasonable and appropriate means of access.) a. Document each access authorization in the Access Request Form (Exhibit A) including role justification, system(s) requested, and date of approval.	Senior Applications, Information Security & BI Administrator
3. Determine when and if direct access to EPHI is appropriate for individuals' external to SCCMHA (e.g., Business Associates, Contract Providers, or person served seeking access to their own EPHI).	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer Senior Applications, Information Security & BI Administrator
Implement Policies and Procedures for Access Establishment and Modification	
4. Develop and implement procedures that, based upon SCCMHA's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program, or process. a. Maintain an Access Control Log (Exhibit B) to record access establishment, modification, and termination events. Logs will be reviewed quarterly by the IT Access & Identity Management Group (AIMG) and retained for a minimum of six (6) years.	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer Senior Applications, Information Security & BI Administrator
5. Formal authorization from the proper authority will be provided to an individual before that individual to granted access to EPHI.	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer Senior Applications, Information Security & BI Administrator

Evaluate Existing Security Measures Related to Access Controls	
6. The security features of access controls will be evaluated to determine if they are aligned with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.	HIPAA Security Officer and Chief Information Officer & Chief Quality and Compliance Officer Senior Applications, Information Security & BI Administrator

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Security Awareness and Training</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.05</td></tr>
<tr><td>Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/13/22, 8/4/23, 9/9/24, 11/12/25

Supersedes:
08.01.04
08.06.14
08.01.03</td><td>Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers:
Alecia Schabel, Continuing Education Supervisor
Kentera Patterson, Officer of Recipient Rights and Compliance & Privacy Officer
Matthew Devos, Senior Network Administrator,
David Wolfcale, Systems Information Security & Microsoft 365 Administrator
Chad Revell, Inventory Management and Mobile Device Specialist</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.308(a)(5) – Security Awareness Training, and to enhance the protection of electronic protected health information (ePHI) through comprehensive security awareness and training programs.

This policy also supports compliance with the HIPAA Privacy Rule, and 42 CFR Part 2 protection of behavioral health and substance use disorder information. The training program is delivered through SCCMHA's LMS and KnowBe4 platform, providing measurable, auditable training and phishing simulation tools to reinforce security awareness.

Policy:
SCCMHA is committed to implementing and maintaining robust security awareness and training programs for all members of its workforce, including management, to ensure effective safeguarding of PHI and to adhere to the HIPAA Security Rule requirements. The Security Awareness Training Program shall use the LMS and KnowBe4 to deliver phishing simulations, micro-modules, risk-based reinforcement exercises, as well as track assignments, documentation, and certifications of completion.

Application:
The HIPAA Security Rule, and this Policy, applies to SCCMHA, its business associates, and any subcontractor that is required to access or use PHI to complete its contracted duties.
Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule. Business associates and subcontractors must demonstrate proof of equivalent training (via LMS or KnowBe4) or adhere to SCCMHA's training modules. Failure to comply may result in contractual sanctions or termination of access.

Standards:

A. Security Awareness Training:

- **Mandatory Training**: All staff, including management, must complete Security Awareness Training upon hire and participate in ongoing monthly training sessions via KnowBe4.
    i. **Monthly Trainings** – users will receive a monthly notification of assigned trainings. These can be completed all at one time or separately on different dates/times. If user has not clicked on any "bad" links over the last 6 months (rolling), training will be reduced. These monthly training courses will consist of:
        1. A "game" to practice skills.
        2. Training session (sometimes interactive) or short phishing simulation/scenario
        3. Two IT or Security Policies to review.
    ii. **High-Risk User Monthly Trainings –** If a user's Phish prone score is over 10% (meaning 10% of "bad" links are clicked) they will be required to take additional courses.
        1. Clickers - 1 Failure in the past 6 months - 2 minutes
        2. Clickers - 2 Failure in the past 6 months - 4minutes
        3. Clickers - 3 Failure in the past 6 months - 10 minutes

4. Clickers – 4 or more Failures in the past 6 months - 20 minutes

iii. **Low-Reporter or Non-Reporter Monthly Trainings** – If a user is considered a low-reporter (haven't reported via the Phish Alert button at all in 1 month) or a non-reporter (haven't reported via the Phish Alert button at all in 6 months) they will be required to complete additional courses.

iv. **Occasional Trainings –** Required assessments to inform us on security standing and risk.

- **HIPAA Security Policy Review:** All staff must complete the monthly HIPAA Security Policy review assigned through KnowBe4.
- **Periodic Security Updates:** SCCMHA will provide updates on emerging security threats, regulatory changes, and policy modifications through multiple communication channels – including emails, Microsoft Teams channels, and internal broadcasts.
- **Notifications for Training, Reminders, and Past Due Notifications:**
  i. User will be notified when training is assigned. Typically, users have 4 weeks to complete training once assigned.
  ii. Users will be reminded of training every 5 days until it is completed.
  iii. If training becomes past due, users will be notified and every 6 days afterwards until completed.
  iv. Users will be notified when training is 14 days past due.
  v. User network accounts will be disabled when training is 15 days past due with no notification.
    1. Supervisors will need to coordinate with IT through the ticket system to follow the process in assisting users with completing training and obtaining network access.

B. Malicious Software Protections:

- Employees will receive training on identifying, preventing, reporting malicious software (malware), such as viruses, worms, and ransomware, phishing attacks, and other cybersecurity threats.
- Safe computer practices, including avoiding suspicious links, attachments, and downloads will be reinforced regularly.

C. Monitoring and Reporting:

- **Operations Team** will review reports on:
  i. The use of the Phish Alert button.
  ii. User's Phish-prone scores.
  iii. User's risk levels
  iv. Training completions
  v. High Risk User list.
  vi. Highest Risk User list
- **CEO/CIO** will review:
  i. Highest Risk Users list – Users and supervisors may be contacted directly by CEO or CIO for an in-person coaching session with all 4 participants.

D. IT Security personnel will monitor unauthorized or suspicious log-in attempts and access activities. **Password Management**:
    - Employees will receive training in password security best practices, including strong password creation, periodic updates, and safe storage of passwords.

E. Evaluation, Improvement, and Documentation:
    - The effectiveness of the security awareness training program will be assessments, feedback surveys, and analytics from the KnowBe4 platform. In addition to KnowBe4 metrics, completion data, quiz scores, and survey feedback will be reviewed quarterly by the HIPAA Security Officer and Compliance Team. Any user who fails training twice consecutively will be placed on a remediation plan and monitored more closely (e.g., monthly modules or in-person review). SCCMHA will use evaluation results to update and improve the training program as needed.
    - Training Records including completion dates, participants, and topics covered, will be maintained for compliance tracking. Records will be stored on KnowBe4 securely, retained for a minimum of six (6) years and accessible for audits.

F. Compliance Enforcement:
    - Supervisors are responsible for following up with employees who fall behind on their training requirements or are considered high-risk.
    - High-risk employees will receive a formal **compliance enforcement memo**, stating they have a specified number of days to correct deficiencies. The memo will be copied to the **chain of command**, ensuring accountability and proper documentation.
    - If compliance issues persist, employees may be required to complete **in-person training** with IT security personnel or designated training staff to reinforce security awareness and best practices.
    - Continued non-compliance may lead to further disciplinary action as per SCCMHA policies and procedures.

Role Responsibilities:

1. Supervisors play a key role in monitoring and enforcing compliance with security awareness training requirements. Using the **KnowBe4 Team Dashboard**, supervisors must:
    a. Track employee training progress and completion rates.
    b. Identify and address overdue training.
    c. Monitor high-risk users based on **Phishing Security Test (PST) results and Phish-prone percentage**.
    d. Encourage staff to participate in optional learning to enhance security awareness.
    e. Review team phishing test results, including failures and reported phishing attempts.
2. The **Chief Information Officer (CIO)** will provide **monthly reports** to the Leadership Team summarizing:

   a. Training completion and overdue status.
   b. High-risk users based on phishing test performance.
   c. Overall team risk scores and security awareness trends.
3. The HIPAA Security Officer will review LMS/KnowBe4 dashboard data monthly and present trends, high-risk users, and mitigation recommendations to Leadership.
4. IT Security staff will coordinate with KnowBe4 administrators to adjust phishing campaign difficulty and remedial modules based on observed behavior.

Definitions:
See I.T./I.S. Policy **08.06.00.01** which contains a comprehensive list of relevant words and terms used within the Policies of this section.

References:
- The HIPAA Security Rule §164.308(a)(5)
- • KnowBe4 Security Awareness Platform
- • NIST SP 800-50: Building IT Security Awareness and Training Programs
- • HIPAA Privacy Rule §164.530(b) – Training
- • 42 CFR Part 2 – Confidentiality of Substance Use Disorder Records
- • OCR Cybersecurity Alerts / Modernization Updates

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Conduct a Training Needs Assessment 1. Determine SCCMHA's training needs, related to HIPAA Security and EPHI.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Develop and Approve a Training Strategy and a Plan 2. Assess the specific HIPAA policies that require security awareness and training in the security awareness and training program.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor

3. Outline the security awareness and training program; the scope of the security awareness and training program; the goals and various target audiences of the security awareness and training program; the learning objectives, the deployment methods, evaluation, and measurement techniques and the frequency of the training.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Protection from Malicious Software; Log-in Monitoring; and password Management 4. Train members of the workforce using KnowBe4 on procedures for: • Guarding against, detecting, and reporting malicious software • Monitoring log-in attempts and reporting discrepancies. • Creating, changing, and safeguarding passwords	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Develop Appropriate Awareness and Training Content, materials, and methods. 5. Select topics that may need to be included in the training materials.	
6. Incorporate new information from email advisories, online IT security daily news Web sites, and periodicals, as is reasonable and appropriate.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Training Implementation 7. Schedule and conduct training outlined in the strategy and plan.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor

8. Implement reasonable techniques to disseminate security messages to the organization, including newsletters, email messages, teleconferencing sessions, staff meetings, and computer-based training including assignment of KnowBe4 modules/simulations.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Implement Security reminders. 9. Implement periodic security-reminder updates for staff, business associates, and contractors.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
10. Provide periodic security updates to staff, business associates, and contract providers.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
Supervisory Compliance Monitoring 11. Use KnowBe4 Team Dashboard to track training progress and overdue assignments. 12. Monitor high-risk users and take corrective action as needed.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, IT Department, Continuing Education Supervisor
13. Issue compliance enforcement memos for non-compliant employees with deadlines for completion. 14. Require in-person training for continued non-compliance. 15. Report training and security trends to Leadership Team.	Supervisors, HIPAA Security Officer, Chief Information Officer & Chief Quality & Compliance Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Security Incident Procedures</td><td>Chapter: 08 – Management of Information</td><td>Subject No: 08.06.08.06</td></tr>
<tr><td>Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/13/22, 8/4/23, 9/9/24, 11/12/25
Supersedes:</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers:
Compliance & Policy Team, Matthew Briggs – Chief of Network Business Operations,
Ben Pelkki – Senior Database & Microsoft 365 Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

To ensure compliance with the HIPAA Security Rule, §164.308(a)(6) – Security Incident Procedures by establishing procedures for identifying, responding to, and documenting security incidents involving Protected Health Information (PHI).

This policy also supports compliance with the HIPAA Privacy Rule, Breach Notification Rule (45 CFR §§164.400–414), and 42 CFR Part 2 requirements for confidentiality of substance use disorder records. SCCMHA recognizes the heightened sensitivity of behavioral health and substance use disorder information and ensures incidents are handled in accordance with these federal standards.

Policy:
SCCMHA will implement and maintain comprehensive policies and procedures to effectively address and manage security incidents, ensuring that appropriate actions are taken to mitigate harm and comply with HIPAA requirements. The policy includes specific response procedures for incidents involving electronic PHI (ePHI), paper PHI, and oral disclosures. SCCMHA will coordinate with the HIPAA Privacy Officer to ensure integrated handling of any breach that triggers both Privacy and Security Rule requirements. Security incident management will also include post-incident corrective actions, technical control adjustments, and retraining when human error is a factor.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule. Business Associates must notify SCCMHA of any actual or suspected security incident involving PHI within 24 hours of discovery, consistent with their Business Associate Agreement.

Standards:
A. Incident Identification and Reporting:

- Detection Mechanism: SCCMHA will employ monitoring tools and techniques to identify potential security incidents, including unauthorized access, data breaches, and system malfunctions.
- Reporting Protocols: staff must promptly report any suspected or known security incidents to the designated HIPAA Security Officer. Reports should include the nature of the incident, systems or data affected, when and how it was detected, and any immediate actions taken. All staff will receive refresher training through KnowBe4 to recognize and promptly report security incidents, phishing attempts, and unauthorized disclosures.

B. Incident Response and Management:

- Immediate Response: Upon identification of a security incident, SCCMHA will initiate an immediate response to contain and mitigate the incident, including isolating affected systems and preventing further unauthorized access.
- Assessment and Analysis: The Security Officer or designated response team will assess the scope and impact of the incident, determining the extent of damage and potential exposure of PHI. A preliminary Risk Assessment will be conducted following the NIST SP 800-61r2 and 800-30 frameworks to determine if the incident meets the definition of a breach under 45 CFR §164.402. If the event qualifies as a breach, the HIPAA Breach Notification Procedure will be activated. SCCMHA will preserve all relevant system logs, access reports, and evidence related to the incident for forensic review.
- Containment and Eradication: Steps will be taken to contain the incident, eradicate the root cause, and restore normal operations while ensuring that no further harm is caused to the system or data.

C. Mitigation of Harm:

- Impact Reduction: SCCMHA will implement measures to reduce the harmful effects of security incidents, such as notifying affected individuals, providing support, and offering credit monitoring services if necessary. In incidents involving 42 CFR Part 2-protected records, disclosures will only occur as authorized under Part 2 and in consultation with the Privacy Officer and Legal Counsel. Special care will be taken to avoid secondary disclosure of SUD treatment information. SCCMHA will coordinate with Human Resources for incidents arising from workforce actions, ensuring proper retraining or disciplinary measures where negligence or misconduct contributed to the event.
- Communication: The organization will communicate relevant information about the incident to affected parties, regulatory bodies, and other stakeholders as required by HIPAA and other applicable regulations.

D. Documentation and Reporting:

- Incident Documentation: Detailed records of each security incident, including the nature of the incident, response actions taken, and outcomes, will be maintained for minimum of six (6) years from the date of creation or last effective date, whichever is later.
- Outcome Analysis: Documentation will include an analysis of the incident's impact, lessons learned, and recommendations for improving security measures and incident response procedures.
- Compliance Reporting: SCCMHA will comply with HIPAA's reporting requirements by notifying the Department of Health and Human Services (HHS) and other regulatory agencies as required and providing breach notifications to affected individuals. SCCMHA will notify affected individuals without unreasonable delay and no later than 60 days following discovery of a breach, consistent with 45 CFR §164.404. For incidents affecting more than 500 individuals, HHS and local media will be notified in accordance with the Breach Notification Rule.

E. Review, Improvement & Training:

- Incident Review: Each incident will be reviewed to assess the effectiveness of the response and identify any areas for improvement in policies, procedures, or training. Results from incident reviews will be integrated into future KnowBe4 phishing campaigns, tabletop exercises, and staff training scenarios to prevent recurrence of similar issues.
- Policy Updates: Based on incident reviews and evolving security threats, SCCMHA will update security incident procedures and related policies as necessary to enhance response capabilities and safeguard PHI. The Security Officer and CIO will review Security Incident Procedures at least annually or following any significant incident, regulatory update, or technology change.
- Training: Regular training updates will be provided to ensure that all relevant parties are aware of current procedures and best practices for incident management.

Definitions:

See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.308(a)(6)
- 45 CFR §§164.400–414 – HIPAA Breach Notification Rule
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Records
- NIST SP 800-61r2 – Computer Security Incident Handling Guide
- NIST SP 800-30 – Risk Management Guide for Information Technology Systems
- OCR "Guidance on Ransomware and HIPAA" (2016, reaffirmed 2023)
- HIPAA Privacy Rule §164.530(d) – Mitigation and Sanctions

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Determine Goals of Incident Response Determine how SCCMHA will respond to a security incident and establish a reporting mechanism and a process to coordinate responses to the security incident.	HIPAA Security Officer Senior Database & Microsoft 365 Administrator
Provide direct technical assistance, advise vendors to address product-related problems, and provide liaisons to legal and criminal investigative groups as needed. Include criteria for escalating incidents to the Privacy Officer, CIO, or Legal Counsel, depending on potential breach classification or regulatory implications.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Chief of Network Business Operations, Senior Database & Microsoft 365 Administrator
Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism. Identify appropriate individuals to be a part of a formal incident response team.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Senior Database & Microsoft 365 Administrator

Develop and Implement Procedures to Respond to and Report Security Incidents.	
Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents known to SCCMHA; and document security incidents and their outcomes.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Senior Database & Microsoft 365 Administrator
Document incident response procedures provide a single point of reference to guide the day-to-day operations of the incident response team. Document step-by-step workflows for evidence preservation, internal communications, and activation of breach notification processes when warranted.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Senior Database & Microsoft 365 Administrator
Review incident response procedures with staff with roles and responsibilities related to incident response, solicit suggestions for improvements, and make changes to reflect input if reasonable and appropriate.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Senior Database & Microsoft 365 Administrator
Incorporate Post-incident Analysis into Updates and Revisions.	
Measure effectiveness and update security incident response procedures to reflect lessons learned and identify actions to take that will improve security controls after a security incident.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer, Senior Database & Microsoft 365 Administrator
Incorporate lessons learned into security training (via KnowBe4) and update incident response procedures to address recurring risks or vulnerabilities.	HIPAA Security Officer, Chief Information Officer & Chief Quality and Compliance Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Contingency Plan</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.07</td></tr>
<tr><td rowspan="2">Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/14/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers:
Matthew Devos - Senior Network & Information Security Administrator,
Benjamin Pelkki, Senior Database & Microsoft 365 Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Brett Lyon, Senior Applications, Information Security & BI Administrator</td></tr>
<tr><td>Supersedes:
08.06.23
08.06.24</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.308(a)(7) – Contingency Plan by establishing and implementing policies and procedures for responding to emergencies and other occurrences that could damage systems containing Electronic Protected Health Information (ePHI), ensuring the continuity and security of operations. This policy also supports compliance with **45 CFR §164.308(a)(1)(ii)(A)–(B)** by integrating contingency planning into the organization's risk analysis and risk management program, consistent with the 2024 NIST SP 800-66r2 guidance.

Policy:
SCCMHA will develop and maintain a comprehensive contingency plan to address emergencies and incidents such as fire, vandalism, system failures, and natural disasters that could impact systems containing ePHI. The contingency plan will include procedures for data recovery, emergency mode operations, alternate communications, and continuity of care, ensuring continued availability of behavioral health and clinical services even when standard systems are unavailable. This plan is designed to safeguard ePHI, maintain business operations, and facilitate recovery.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule.

Standards:
A. Data Backup & Retrieval:
- **Backup Procedures**: SCCMHA will establish and implement procedures to create and maintain retrievable exact copies of EPHI. Regular backups will be performed and securely stored to ensure data integrity and availability as stated in SCCMHA Policy 08.06.40: Data Backup & Storage.
- **Backup Storage**: Backup copies will be stored in a secure location, separate from the primary data source, to protect against data loss due to physical damage or theft.
- **Backup Encryption**: All backup copies of ePHI must be encrypted using current NIST-approved algorithms (e.g., AES-256) both in transit and at rest.
- **Backup Retention**: Backups will be retained for at least **six years** in accordance with §164.316(b)(2)(i), or longer if required by SCCMHA's records retention policy or contractual obligations.

B. Data Restoration:
- **Restoration Procedures**: SCCMHA will establish procedures for restoring ePHI following any data loss incident. These procedures will ensure that data can be quickly and accurately restored from backups to minimize downtime and disruption.
- **Restoration Testing**: Regular tests will be conducted to verify the effectiveness of data restoration procedures and to ensure that backup copies are complete and functional.
- **Restoration Documentation**: Test results and restoration validation records will be documented and maintained for a minimum of six years as required by §164.316(b)(2).

C. Emergency Mode Operations:

- **Critical Business Processes**: SCCMHA will establish procedures to enable continuation of critical business processes during emergencies or system failures. This includes implementing temporary measures to protect the security of ePHI and maintain essential operations.
- **Alternate Access Procedures**: SCCMHA will define procedures for secure remote access or temporary manual processes to continue essential clinical and administrative operations during system outages.
- **Behavioral Health Continuity**: Procedures must ensure protected behavioral health records remain accessible only to authorized staff and consistent with 42 CFR Part 2 confidentiality requirements during emergencies.

D. Testing & Revision:
- **Contingency Plan Testing**: SCCMHA will implement procedures for periodic testing of the contingency plan to ensure effectiveness and readiness. Testing will include simulations of various emergency scenarios and evaluation of response capabilities.
- **Testing Frequency:** Contingency plan testing will occur at least annually, or more frequently if significant system changes occur.
- **Cross-Department Coordination**: Testing will include participation from IT, Compliance, and the Management Team to validate operational readiness.
- **Plan Revisions:** The contingency plan will be reviewed and revised as needed based on test results, changes in business operations, technological advancements, and lessons learned from actual incidents.

E. Assessment of Criticality:
- **Application and Data Assessment**: SCCMHA will assess the criticality of specific applications and data to prioritize recovery efforts and resource allocation during an emergency. This assessment will guide the development and implementation of contingency plan components.
- **Impact Analysis**: An analysis of the potential impact of data loss or system failure on critical business functions will be conducted to inform contingency planning and risk management strategies.
- **Behavioral Health Systems Prioritization**: Applications supporting clinical documentation, medication management, crisis services, and electronic health record access will be classified as high-criticality systems for prioritized restoration.

F. Communication and Training:
- **Communication Plan**: A communication plan will be established to ensure that all relevant parties, including employees, business associates, and subcontractors, are informed of contingency procedures and their roles during an emergency.
- **Training**: Regular training sessions will be conducted to familiarize staff with the contingency plan and their responsibilities in executing it. This training will include response procedures, data protection measures, and emergency contact information.
- **Incident Notification Integration**: The communication plan must align with SCCMHA's 08.05.03.03 HITECH Breach Notification PHI and 08.06.08.06

HIPAA Security, Security Incident Response policies, ensuring timely coordination if an outage results in potential compromise of ePHI.

- **Workforce Acknowledgment**: All workforce members must acknowledge training completion annually and upon policy revision.

G. Contingency Plan Review and Documentation:

- **Annual Review**: The contingency plan will be reviewed annually by the Chief Information Officer| Chief Quality & Compliance Officer| HIPAA Security Officer to ensure continued compliance with HIPAA and NIST standards.
- **Documentation Retention**: All documentation of contingency planning, testing, revisions, and recovery activities will be retained for a minimum of six years from the date of creation or last in effect (§164.316(b)(2)).

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.308(a)(7)
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
- NIST SP 800-34 Rev.1 – Contingency Planning Guide for Federal Information Systems

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Develop Contingency Planning Policy	
1. Define SCCMHA's overall contingency objectives.	1. Information Security Team
2. Establish SCCMHA's framework, roles, and responsibilities for this area.	2. Information Security Team
3. Address scope, resource requirements, training, testing plan maintenance, and backup requirements.	3. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Conduct Applications and Data Criticality Analysis	

4. Assess the relative criticality of specific applications and data in support of other Contingency Plan components.	4. Information Security Team Chief Information Officer & Chief Quality and Compliance Officer Team
5. Identify the activities and material involving EPHI that are critical to business operations.	5. Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
6. Identify the critical services or operations, and the manual and automated processes that support them, involving EPHI.	6. Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
7. Determine the amount of time that SCCMHA can tolerate disruption to these operations, material, or services (e.g., due to power outages).	7. Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
8. Establish cost-effective strategies for recovering these critical services or processes.	8. Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Identify Preventive Measures	
9. Identify preventive measures for each defined scenario that could result in loss of a critical service operation involving the use of EPHI.	9. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
10. Ensure that preventive measures are practical and feasible in terms of their applicability in each environment.	10. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer Chief of Network Business Operations
Develop Recovery Strategy	
11. Finalize the set of contingency procedures that should be involved for all identified impacts, including emergency mode operations. The strategy must be adaptable to the existing operating	11. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer Compliance & Policy Team

environment and address allowable outage times and associated priorities identified above.	Chief of Network Business Operations
12. Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated.	12. Chief of Network Business Operations
Data Backup Plan and Disaster Recovery Plan	
13. Establish and implement procedures to create and maintain retrievable exact copies of EPHI.	13. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
14. Establish (and implement as needed) procedures to restore any loss of data.	14. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Develop and Implement an Emergency Mode Operation Plan	
15. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.	15. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Testing and revision Procedure	
16. Implement procedures for periodic testing and revision of contingency plans.	16. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
17. Test the contingency plan on a predefined cycle.	17. Senior Network & Information Security Administrator Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
18. Train those with a defined plan of responsibilities in their roles.	18. Senior Network & Information Security Administrator Information Security Team

19. **Maintain Documentation:** Maintain all contingency plan documentation, testing results, revisions, and communications for at least six years or longer in accordance with SCCMHA's data retention policy.	Chief Information Officer & Chief Quality and Compliance Officer 19. Chief Information Officer & Chief Quality and Compliance Officer /HIPAA Security Officer Senior Network & Information Security Administrator
20. **Annual Plan Review and Approval:** Conduct an annual review and approval of the contingency plan by the Chief Information Officer | Chief Quality & Compliance Officer. Update the plan as needed to reflect operational or technological changes.	20. Chief Information Officer & Chief Quality and Compliance Officer /HIPAA Security Officer Compliance & Policy Team

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Evaluation – Security Risk Assessment</td><td>Chapter: 08 – Management of Information</td><td>Subject No: 08.06.08.08</td></tr>
<tr><td>Effective Date: October 01, 2020</td><td>Date of Review/Revision: 9/14/22, 8/4/23, 9/9/24, 11/12/25
Supersedes: 08.06.27</td><td rowspan="2">Approved By: Sandra M. Lindsey, CEO

Responsible Director: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers: Ben Pelkki – Senior Database & Microsoft 365 Administrator
Matthew Devos, Senior Network Administrator
David Wolfcale- Systems, Information Security & Microsoft 365 Administrator</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

To ensure compliance with the HIPAA Security Rule, §164.308(a)(8) – Security Incident Procedures by establishing and implementing procedures for periodic technical and non-technical evaluations of security risks. This policy aims to assess the effectiveness of SCCMHA's security measures and policies in protecting Electronic Protected Health Information (ePHI) and to adapt to changes in the environment or operation that may impact security. It also supports SCCMHA's security governance framework by ensuring that risk assessments are integrated with incident response, audit controls, and change management. It further ensures that SCCMHA is prepared to adapt to evolving threats, technological changes, and regulatory updates (including anticipated OCR enhancements to risk evaluation requirements).

Policy:

SCCMHA will conduct regular and comprehensive security risk assessments, encompassing both technical and nontechnical aspects, to evaluate the effectiveness of security policies and procedures in protecting ePHI. SCCMHA will conduct risk assessments that include threat modeling, scenario-based simulations, and red-teaming or penetration testing when appropriate, to validate real-world resilience of safeguards. These assessments will be performed based initially upon the standards set forth by the HIPAA Security Rule and subsequently in response to environmental or operational changes affecting the security of EPHI.

Application:
The HIPAA Security Rule, and this Policy, applies to SCCMHA, its business associates, and any subcontractor that is required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policy and Procedure which complies with the applicable section of the HIPAA Security Rule. Business associates and subcontractors must provide SCCMHA with evidence or summary results of their risk assessments, including identified vulnerabilities and mitigation plans, upon request or as contractually required.

Standards:
A. Risk Assessment Schedule:
- **Initial Assessment**: SCCMHA will perform an initial risk assessment to evaluate the current security posture against the standards of the HIPAA Security Rule.
- **System Changes**: Risk assessments shall also be triggered by significant system changes (e.g., deployment of new EHR modules, integration with third-party APIs, telehealth expansions) and after any security incident.
- **Periodic Reviews**: Risk assessments will be conducted at least annually or more frequently if significant changes occur in the environment, operations, or security landscape.

B. Scope of Assessment:
- **Technical Evaluation**: This includes assessing the effectiveness of technical safeguards such as access controls, encryption, and system security configurations. Review of endpoints, mobile devices, APIs, cloud services (e.g., Microsoft 365, telehealth platforms) and assess vulnerabilities in recent technologies or integrations.
- **Non-Technical Evaluation**: This involves reviewing administrative and physical safeguards, such as policies, procedures, staff training, and facility security. In addition, analysis of organizational culture, workforce turnover, third-party vendor relationships, and physical environment risks (e.g., data center, remote clinics).

C. Assessment Methodology:
- **Risk Identification**: The assessment will identify potential security threats and vulnerabilities that could impact the confidentiality, integrity, or availability of EPHI.

- **Risk Analysis**: The likelihood and potential impact of identified risks will be analyzed to determine the level of risk and prioritize mitigation efforts.
- **Control Gap Analysis:** For each identified vulnerability, document existing compensating or interim controls and residual risk after applying controls.
- **Control Evaluation**: The effectiveness of existing security controls and measures will be evaluated to ensure they are adequate in addressing identified risks.

D. Response to Findings:
- **Mitigation Strategies**: Based on the assessment findings, SCCMHA will develop and implement strategies to mitigate identified risks and address any weaknesses in security controls. Mitigation plans must include realistic timelines (e.g., high-risk vulnerabilities resolved within 60 days, medium within 120 days) and responsible owners. These plans will be tracked and status reported quarterly to senior leadership.
- **Policy and Procedure Updates**: Security policies and procedures will be updated as necessary to reflect changes in risk levels, operational practices, and regulatory requirements.

E. Documentation and Reporting:
- **Assessment Documentation**: Detailed records of each risk assessment, including methodologies, findings, and actions taken, will be maintained. The documentation must include versioning (date/version), who conducted the assessment, tools used and change logs. Summary reports shall be presented annually to the SCCMHA Board and retained for a minimum of six (6) years.
- **Reporting**: Summary reports of risk assessments and remediation efforts will be provided to senior management and other relevant stakeholders as appropriate.

F. Continuous Improvement:
- **Feedback Mechanism**: Feedback from risk assessments and security incidents will be used to improve security measures and assessment processes.
- **Review and Update**: The risk assessment policy and procedures will be reviewed and updated regularly to ensure they remain effective and aligned with current security best practices and regulatory requirements. Lessons learned from assessment findings, audits, and actual security incidents shall be systematically incorporated into the risk assessment process and into policy updates.

Definitions:
See I.T./I.S. Policy **08.06.00.01** which contains a comprehensive list of relevant words and terms used within the Policies of this section.

References:
- The HIPAA Security Rule §164.308(a)(8)

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Determine Whether Internal or External Evaluation – Security Risk Assessment is Most Appropriate	
1. Decide whether the Evaluation – Security Risk Assessment will be conducted with internal staff resources or external consultants.	1. Chief Information Officer | Chief Quality and Compliance Officer
2. Engage external expertise to assist the internal Evaluation – Security Risk Assessment team where additional expertise to assist the internal Evaluation – Security Risk Assessment team where additional skills and expertise is determined to be reasonable and appropriate.	2. Chief Information Officer | Chief Quality and Compliance Officer
Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	
3. Use an Evaluation – Security Risk Assessment strategy and tool that considers all elements of the HIPAA Security Rule and can be tracked, such as a questionnaire or checklist.	3. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator Systems
4. Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard deployed to protect EPHI.	4. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator Systems
5. Leverage any existing reports or documentation that may already be prepared by SCCMHA that may already be prepared by SCCMHA addressing compliance, integration, or maturity of a	5. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator

particular security safeguard deployed to protect EPHI.	
Conduct Evaluation – Security Risk Assessment	
6. Determine, in advance, what departments and/or staff will participate in the Evaluation – Security Risk Assessment.	6. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator
7. Collect and document all needed information. Collection methods may include the use of interviews, surveys, and outputs of automated tools, such as access control auditing tools, system logs, and results of penetration testing.	7. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator
Documentation Results	
8. Document each Evaluation – Security Risk Assessment finding, remediation options and recommendations and remediation decisions.	8. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator
9. Document known gaps between identified risks and mitigating security controls, and any acceptance of risk, including justification.	9. Chief Information Officer | Chief Quality and Compliance Officer Systems, Information Security & Microsoft 365 Administrator Senior Network Administrator Systems
10. Develop security program priorities and establish targets for continuous improvement.	10. Chief Information Officer | Chief Quality and Compliance Officer
Repeat Evaluation – Security Risk Assessments Periodically	
11. Establish the frequency of Evaluation – Security Risk Assessments, considering the sensitivity of the EPHI controlled by SCCMHA.	11. Chief Information Officer | Chief Quality and Compliance Officer

12. In addition to periodic Evaluation – Security Risk Assessments, consider repeating Evaluation – Security Risk Assessments when environmental and operational changes are made.	12. Chief Information Officer | Chief Quality and Compliance Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Business Associate Agreements (BAAs) and Other Arrangements</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.08.09</td></tr>
<tr><td rowspan="2">Effective Date:
10/1/20</td><td>Date of Review/Revision:
10/1/20, 7/3/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Amy Lou Douglas - Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Amy Lou Douglas - Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers:
Matthew Briggs, Chief of Network Business Operations
Jennifer Keilitz – Director of Network Services, Public Policy & Continuing Ed</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.308(b) and §164.314(a)(1) – by establishing procedures for Business Associate Agreements (BAAs) and other Arrangements. This policy ensures that SCCMHA and its business associates adequately safeguard Electronic Protected Health Information (ePHI) and meet HIPAA requirements. This policy further supports compliance with OCR's proposed Security Rule enhancements (2024), which will impose more prescriptive vendor oversight, timely notification of contingency plan activations, and stronger downstream BAA obligations.

Policy:

SCCMHA will enter into Business Associate Agreements with any business associate before permitting them to create, receive, maintain, or transmit electronic protected health information on SCCMHA's behalf. SCCMHA must receive satisfactory assurances (documented through a written agreement or other arrangement referred to as a Business Associate Agreement) that the business associate will appropriately safeguard the information as required by §164.314. If SCCMHA subcontractors use vendors that require access to PHI or ePHI, they too need to enter into business associate agreements with their subcontractors. In accordance with HIPAA (45 CFR 164.502(e)(1)) a business associate agreement is not required and does not apply to disclosures by a covered entity (e.g., SCCMHA) to a health care provider for treatment purposes.

Application:
The HIPAA Security Rule, and this Policy, applies to SCCMHA, its business associates, and any subcontractor that is required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule.

Standards:

- Requirements for Business Associate Agreements:
    - **Satisfactory Assurances**: SCCMHA will only permit a Business Associate to handle ePHI if satisfactory assurances are obtained through a written Business Associate Agreement (BAA) that the business associate will appropriately safeguard the information in accordance with the **HIPAA Security Rule Exception**: SCCMHA is not required to enter into a BAA with a health care provider when the only PHI involved is in the context of treatment and no further disclosure or processing by the provider is required beyond treatment. In those cases, standard HIPAA treatment-sharing provisions apply. However, if the subcontractor performs functions beyond treatment (e.g., data aggregation, claims, analytics), then a BAA is required.
- Subcontractor Agreements:
    - **Assurances for Subcontractors**: A business associate may only allow a subcontractor to handle EPHI on its behalf only if the business associate obtains satisfactory assurances through a BAA with a subcontractor, in accordance with the HIPAA Security Rule §164.314(a).
- Documenting Assurances:
    - **Written Agreements**: The satisfactory assurances required must be documented through a written agreement or other arrangement with the business associate that meets the applicable requirements of the HIPAA Security Rule §164.314(a).

        i. The BAA must require the BA to return or destroy all PHI at termination, unless state law requires retention, and to certify the return or destruction.

ii. Require that the BA make available to SCCMHA its internal audit records, logs, and security documentation upon reasonable request for compliance and investigation purposes.
iii. The BAA should include a clause that subcontractors must notify upstream BAs or SCCMHA within 24 hours of activating their contingency plans (if the subcontractor's system is compromised or in emergency mode).
iv. The BAA must permit SCCMHA to perform audits or assessments (onsite or remote) to verify compliance, particularly for systems handling high-risk ePHI.
v. Incident Reporting: The BAA must include provisions requiring the business associate to report any security incident to SCCMHA, including breach of unsecured protected health information as required by §164.410.
vi. Subcontractor Requirements: The requirements of this policy also apply to the agreement or other arrangement between a business associate and a subcontractor consistent with HIPAA Security Rule § 164.308(b)(4).

- Indemnification and Governing Law:
  - **Indemnification**: SCCMHA requires that Business Associate Agreements (BAAs) include comprehensive indemnification provisions to protect SCCMHA from any losses, damage, penalties, costs, or expenses resulting from the business associate's acts, omissions, or breach of agreement. This indemnification shall include, but is not limited to, regulatory fines, investigation or enforcement costs, breach notification expenses, credit monitoring costs, and reasonable attorney's fees incurred by SCCMHA because of a business associate's noncompliance with HIPAA, the HITECH Act, or other applicable privacy and security laws.
  - **Liquidated Damages and Penalties:** SCCMHA reserves the right to include liquidated damages or penalty clauses in BAAs for willful, negligent, or repeated failure to safeguard PHI or ePHI. These provisions are designed to ensure accountability and promote prompt corrective action in the event of noncompliance or data breach.
  - **Insurance Requirements:** All business associates shall maintain adequate cyber liability or data breach insurance coverage sufficient to cover potential HIPAA violations and related privacy/security incidents. Proof of such coverage may be required prior to contract execution or renewal and upon request.
  - **Limitation of Liability:** SCCMHA does not accept contractual limitations of liability that reduce a business associate's responsibilities below what is required under HIPAA, the HITECH Act, or related federal and state privacy regulations. Any limitation of liability must be consistent with statutory and regulatory obligations.
  - **Governing Law**: Unless otherwise required by federal law, all Business Associate Agreements involving SCCMHA shall be governed by and construed in accordance with the laws of the State of Michigan. Authority

and venue for any disputes shall be within the appropriate courts of Michigan.

- Review & Monitoring:
  - **Regular Reviews**: SCCMHA will periodically review BAAs and relevant subcontractors to ensure compliance with HIPAA Privacy and Security Rule regulations. These reviews will assess and address any necessary updates due to changes in regulation or operations.
  - **Quarterly Compliance Reporting:** Business Associates shall submit quarterly written reports to SCCMHA summarizing:
    i. Security and privacy training completion rates.
    ii. Status of implemented safeguards.
    iii. Documented incidents or breaches (including near misses).
    iv. Results of internal or external vulnerability scans.
    v. Any changes in ownership, infrastructure, or subcontractors that may affect PHI security.
  - **Performance Metrics and Service-Level Expectations:** Business Associates shall comply with performance metrics defined by SCCMHA, including but not limited to:
    i. Notification of security incidents within **24 hours** of discovery.
    ii. Remediation of critical vulnerabilities within **15 calendar days** of identification.
    iii. Completion of corrective action plans within **30 calendar days** of issuance.
  - **Corrective Action and Escalation:** If audit findings or monitoring identify noncompliance, SCCMHA will require the Business Associate to submit a corrective action plan (CAP) with specific deliverables and deadlines. Failure to implement corrective actions may result in suspension, contract modification, or termination of the BAA.
  - **Continuous Oversight and Documentation:** The Compliance & Policy Team, in collaboration with the Chief Information Officer and Chief Quality and Compliance Officer, will maintain documentation of all audit results, compliance certifications, BA correspondence, and corrective action status reports for a minimum of **six (6) years** as required by 45 CFR §164.316(b)(2)(i).

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:
- The HIPAA Security Rule §164.308(a)(8)(b)
- The HIPAA Security Rule §164.314
- HIPAA Privacy Rule §164.502(e)(1)
- HIPAA Security Rule §164.314(a)
- HIPAA Breach Notification Rule §164.410

- HHS OCR Proposed Rule for HIPAA Security (2024)
- HIPAA Business Associate Agreement Best Practices (industry guidance)

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Identify Entities that Are Business Associates under the HIPAA Security Rule	
1. Identify the individual or department who will be responsible for coordinating the execution of business associate agreements or other arrangements. a. SCCMHA will maintain a vendor inventory/registry mapping which vendors handle ePHI, their roles, BAA status, and review dates.	Chief Information Officer | Chief Quality and Compliance Officer, Contracts Manager, Director of Network Services, Public Policy & Continuing Ed
2. Periodically, and as necessary, reevaluate the list of business associates to determine who has access to EPHI to assess whether the list is complete and current.	Contracts Manager
Written Contract or Other Arrangements	
3. Document the satisfactory assurances required by this Policy through a written agreement or other arrangement with the business associate that meets the applicable requirements of section 164.314(a).	Contracts Manager
4. Execute new or update existing agreements or arrangements as appropriate.	Contracts Manager

a. SCCMHA will ensure that when regulations change (e.g., new HIPAA or OCR laws), BAAs are reviewed and revised accordingly (e.g., by December 23, 2024, for 2024 HIPAA changes to reproductive health rules).	Contracts Manager
5. Include security requirements in business associate agreements to address confidentiality, integrity, and availability of EPHI.	Contracts Manager
6. Specify any training requirements associated with the agreement or other arrangement, if reasonable and appropriate.	Contracts Manager, Continuing Education Supervisor
Establish Process for Measuring Agreement Performance and Terminating the Agreement if Security Requirements are Not Being Met	Contracts Manager Security Officer, Contracts Manager, Director of Network Services, Public Policy & Continuing Ed
7. Maintain clear lines of communication with business associates.	Security Officer, Contracts Manager, Director of Network Services, Public Policy & Continuing Ed
8. Conduct periodic security reviews of business associates.	Security Officer, Contracts Manager, Contracts Manager
9. Establish criteria for measuring agreement performance of business associates.	Security Officer, Contracts Manager, Director of Network Services, Public Policy & Continuing Ed Security Officer, Contracts Manager
10. Agreements must ensure that Business Associates adequately protect EPHI.	Security Officer, Contracts Manager, Director of Network Services, Public Policy & Continuing Ed Security Officer, Contracts Manager
11. Agreements must provide that Business Associate's Agents adequately protect EPHI.	

12. Agreements must ensure that Business Associates will report security incidents. 13. Agreements must provide that Business Associates will authorize termination of the Agreement if it has been materially breached.	

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Facility Access Controls</td><td>Chapter: 08 – Management of Information</td><td>Subject No: 08.06.10.01</td></tr>
<tr><td rowspan="2">Effective Date: October 01, 2020</td><td>Date of Review/Revision: 9/15/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="2">Approved By: Sandra M. Lindsey, CEO</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td><td>Responsible Director: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers: Fred Stahl – Director of Human Resources / Transportation / Facilities, Melissa Gutzwiller, Director of Environmental Services, Customer Service and Security</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.310(a) – Facility Access Controls, and to protect the integrity and confidentiality of electronic information systems and facilities housing such systems. This policy also supports compliance with 45 CFR § 164.308(a)(1) (Risk Analysis and Management) and § 164.308(a)(5) (Security Awareness and Training), ensuring that physical access safeguards are aligned with SCCMHA's overall HIPAA Security and 42 CFR Part 2 obligations for behavioral health and substance use disorder information.

Policy:
SCCMHA will implement comprehensive policies and procedures to limit physical access to its electronic information systems and facilities, while ensuring that authorized access is granted according to established criteria. These procedures will protect against unauthorized access, tampering and theft. This policy will be reviewed and updated at least annually or following any significant facility, operational, or risk-assessment changes.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule. This policy applies to all physical locations, including leased sites, remote program offices, and off-site storage where electronic systems containing ePHI are located.

Standards:

A. Contingency Operations:
- **Disaster Recovery Access**: Establishment and implementation of procedures that allow facility access to restore lost data under the disaster recovery plan and emergency mode operations.
- **Emergency Contacts**: A list of authorized personnel who can access the facility during emergencies will be maintained, and SCCMHA will ensure the authorized personnel are trained in the emergency access procedures.
- **Annual Testing**: Periodic testing of facility access during disaster recovery and emergency-mode operations will be conducted at least annually.

B. Facility Security Plan:
- **Physical Security Measures**: Implementation and maintenance of security measures to safeguard the facility, including physical barriers (i.e., walls, doors, locks), surveillance systems (i.e., cameras), and alarm systems.
- All individuals must use their assigned access badge to enter secured areas within SCCMHA. Tailgating (where an unauthorized person follows an authorized person into a secure area) is prohibited and will be monitored to ensure compliance.
- **Access Controls**: Procedures will be developed and implemented for granting, modifying, and revoking physical access to the facility. Ensuring access is restricted to authorized personnel based on their roles and responsibilities.
    i. Areas that require restricted access controls:
        1. Server Rooms
        2. IT Offices & Areas
        3. Data Centers
- **Security Audits**: Regular security audits to identify vulnerabilities and ensure that physical security measures are effective.
- **Environmental Monitoring**: Critical areas such as server rooms and data centers shall maintain environmental controls (HVAC, fire suppression, temperature sensors) and alerts to prevent system damage.
- **Video Retention:** Surveillance recordings will be retained for a minimum of 90 days unless longer retention is required for investigations.

C. Badge Use & Requirements:
- All individuals must present their access badge at the door reader to gain entry.

- Badges must always be worn visibly while on SCCMHA premises.
- Lost or stolen badges must be reported immediately to Security or IT, and access credentials will be deactivated within 30 minutes of notification.

D. Access Control and Validation Procedures:
   - **Access Authorization:** Defined and implemented procedures for authorizing access to facilities based on role, function, and necessity. This includes a formal process for requesting and approving access.
   - Doors equipped with access control systems must be opened using the individual's access badge. The system will log each access attempt, including date, time, and badge ID.
   - **Visitor Management:** Implement visitor control procedures, including registration, identification, and escorting policies. Ensure visitors are only allowed access to areas necessary for their visit.
   - **Business Associate and Contractor Access**: Vendors requiring on-site work must be pre-approved by the CIO or Security Officer, logged at entry, and escorted in restricted areas.
   - **Access Logs Review**: Logs from badge readers and electronic door controls will be reviewed monthly by Security or IT for anomalies.
   - **Testing and Revision Access**: Control access to areas and systems used for testing and revisions. Ensure that such access is strictly managed and monitored.

E. Maintenance Records:
   - **Documentation**: Comprehensive policies and procedures to document repairs and modifications to the physical components of a facility which are related to security, including changes to physical components (for example, hardware, walls, doors, and locks) will be implemented. Maintenance and modification records shall be retained for a minimum of six years in accordance with HIPAA documentation requirements.

F. Access Control Monitoring:
   - **Access Logs**: Implement and maintain logs for all facility access, including entry and exit times, personnel involved, and reasons for access. Regularly review these logs to detect and respond to unauthorized access.
   - **Surveillance**: Use surveillance systems to monitor activity within and around the facility. Ensure that surveillance footage is stored securely and is accessible for review as needed by authorized personnel.
   - **Integration with Security Awareness Program:** Physical access logs and incident data will be incorporated into KnowBe4 awareness training to reinforce real-world examples.

G. Training and Awareness:
   - **Employee Training**: Provide regular training to employees on facility access procedures, security measures, and emergency protocols. Ensure that staff understand their roles and responsibilities in maintaining facility security. All training will be documented and tracked through SCCMHA's KnowBe4 Security Awareness Platform. Compliance and IT. will semi-annually review training completion reports.

- **Security Awareness**: Promote awareness of facility security policies and procedures among all personnel, emphasizing the importance of protecting EPHI and maintaining physical security. Training content will include facility-specific scenarios such as tailgating, visitor control, and emergency facility access.

H. Report & Incident Response:

- **Incident Management:** Develop and implement procedures for responding to security incidents related to facility access. This includes investigating, documenting, and addressing incidents of unauthorized access or tampering.
- **Special Access Areas**: To ensure the integrity and security of our facilities, it is crucial that access is strictly controlled and monitored. If an area that requires restricted access controls (i.e., Server Rooms, Data Centers, and IT areas) are found unattended or lacking an authorized individual, it constitutes a serious security violation. Such situations could potentially expose our sensitive systems and data to unauthorized access or tampering.
- **Reporting Security Violations**:
    i. If you observe any of the following scenarios, please report them to the CIO office immediately.
        - Unattended Server Room: The server room is found open or left unattended without an authorized IT staff member present.
        - Unauthorized Access: Individuals who are not authorized IT personnel are present in the server room without proper supervision or clearance.
        - Security Protocols Breach: Any breach in established security protocols regarding server room access and monitoring.
        - Tailgating: Staff should report any observed instances of tailgating to the HIPAA Security Officer.
- Timely reporting of such violations is critical in maintaining the security of our network and protecting our organizational assets.
- **Physical security incidents:** All physical security incidents will be logged in SCCMHA's Incident Management System, correlated with access-control and surveillance data, and reviewed quarterly by the CIO and HIPAA Security Officer.

Responsibilities

- **Security Personnel**: Monitor access control systems, investigate incidents of tailgating, and enforce policy compliance. Ensure surveillance and badge access logs are reviewed and retained according to this policy.
- **Employees and Contractors**: Adhere to badge usage requirements, report security incidents, and ensure compliance with access control procedures.
- **Management**: Support the implementation and enforcement of this policy and ensure all personnel receive proper training. Ensure all workforce members complete KnowBe4 physical-security modules monthly or quarterly.

Definitions:

See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.310(a)
- 45 CFR § 164.308(a)(1) – Risk Analysis and Management
- 45 CFR § 164.308(a)(5) – Security Awareness and Training
- 45 CFR § 164.316(b)(2)(i) – Documentation Retention
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Conduct an Analysis of Existing Physical Security Vulnerabilities	
1. Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities.	Director of Environmental Services, Customer Service and Security
2. Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed.	Director of Environmental Services, Customer Service and Security Chief Information Officer & Chief Quality and Compliance Officer
3. Determine which types of facilities require access controls to safeguard EPHI, such as: • Data Centers • Peripheral equipment locations • IT staff offices • Workstation locations	Director of Environmental Services, Customer Service and Security
Identify Corrective Measures	
4. Identify and assign responsibilities for the measures and activities necessary to correct deficiencies and ensure that proper access is allowed.	Director of Environmental Services, Customer Service and Security

5. Develop and deploy policies and procedures to ensure that repairs, upgrades, and/or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed.	Director of Environmental Services, Customer Service and Security
Developing a Facility Security Plan	
6. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Director of Environmental Services, Customer Service and Security
7. Implement appropriate measures to provide physical security protection for EPHI in SCCMHA's possession.	Director of Environmental Services, Customer Service and Security
8. Include documentation of the SCCMHA inventory, information about the physical maintenance records and the history of changes, upgrades, and other modifications.	Director of Environmental Services, Customer Service and Security
9. Identify points of access to the facility and existing security controls.	Director of Environmental Services, Customer Service and Security
Develop Access Control and Validation Procedures	
10. Implement procedures to control and validate a person's access to facilities based on their role or location, including visitor control, and control of access to software programs for testing and revision.	Director of Environmental Services, Customer Service and Security
11. Implement procedures to provide facility access to authorized personnel and visitors and exclude unauthorized persons.	Director of Environmental Services, Customer Service and Security

Establish Contingency Operations Procedures	
12. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.	Director of Environmental Services, Customer Service and Security
Maintain Maintenance Records	
13. Implement policies and procedures to document repairs and modifications to a facility's physical components related to security (for example, hardware, walls, doors, and locks). 14. Conduct an annual Facility Security Risk Assessment in coordination with the organizational HIPAA Security Risk Analysis, documenting any physical safeguard vulnerabilities and corrective actions.	Director of Environmental Services, Customer Service and Security

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Device and Media Transport & Disposal</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.10.04</td></tr>
<tr><td>Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/15/22, 8/4/23, 9/9/24, 11/12/25

Supersedes:
08.01.07
08.06.37
08.06.39</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer

Additional Reviewers:
Mark Suave, Senior Systems & Desktop Support Administrator
Chad Revell, Inventory Management and Mobile Device Specialist</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.310(d) – Workstation Use, and to protect electronic protected health information (EPHI), this policy governs the receipt, removal, and movement of hardware and electronic media containing EPHI within and outside SCCMHA facilities.

Policy:
SCCMHA will implement comprehensive policies and procedures that govern the inventory, movement, receipt, storage, transport, removal, and disposal of hardware and electronic media that contain electronic protected health information (ePHI). All activities involving these items will be tracked, logged, encrypted when in transport, and managed under chain-of-custody controls to ensure the confidentiality, integrity, availability, protection, and security of ePHI.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule.

Standards:

1. Tracking & Logging:
    - **Movement Tracking**: All movements of SCCMHA hardware, devices, and electronic media containing ePHI into, within, or out of its facilities must be tracked and logged. Logs must include chain-of-custody records, timestamps, device serial numbers, encryption status, and responsible personnel. Those responsible for such movement must take appropriate and reasonable actions to protect EPHI. This includes both EPHI received by SCCMHA and created within SCCMHA.

2. Authorization and Documentation:
    - **Authorization Requirement:** all uses or movement of information system or electronic media containing EPHI outside SCCMHA's premises must be authorized by appropriate SCCMHA management (Manager of Information Technology, CIO|CQCO). Such authorization must be tracked and logged.
    - **Documentation Details**: At a minimum, such tracking and logging must provide the following information:
        - Date and time of movement of system or media.
        - Device or media identifier (serial number)
        - Identity of individual moving the media
        - Destination and intended use.
        - Identity of approving authority
        - Encryption or security status during transport
        - Verification signature upon receipt

3. Protection and Responsibility:
    - **Employee Responsibility**: employees and associates must ensure that electronic media or information systems containing EPHI are protected against damage, theft, and unauthorized access during movement. This includes securing the items physically and logically (i.e., tamper-resistant containers, locked cases, or containers) or two-person handoff/transport. Lost or stolen media must be immediately reported and investigated under the Incident Response policy.

4. Data Backup and Storage:
    - **Pre-Movement Backup**: Before moving equipment containing PHI, ensure that a retrievable, exact copy of electronic protected health information will be created and stored securely.

- **Backup Validation**: Backup integrity must be assessed to confirm no corruption prior to movement.
- **Backup Security**: backups must be encrypted and stored in a secure, access-controlled location that meets SCCMHA's security requirements or encrypted cloud storage.

5. Disposal Procedures:
    - **Final Disposition**: Implementation of procedures for the secure disposal of ePHI and any hardware or electronic media that stored ePHI. This includes data wiping, physical destruction, or other secure methods of disposal. Dispose of hardware/media containing ePHI using methods that render data unrecoverable, such as DoD 5220.22-M wiping, degaussing (where applicable), or physical destruction (shredding, crushing).
    - **Certification**: The individual overseeing disposal must certify in writing that destruction or overwriting is complete and irrecoverable.
    - **Vendor Disposal:** When using a third-party disposal vendor, it requires a formal contract, proof-of-destruction, and chain-of-custody documentation. SCCMHA currently contracts with Shred Experts who are authorized to dispose of hardware/media through their contract.
    - **Documentation**: Document the disposal process, including details of the destruction and individual responsible for overseeing it.
6. Media Reuse:
    - **Data Removal**: Before electronic media is made available for reuse, ensure that EPHI is completely removed using approved methods such as data wiping or physical destruction. Acceptable methods include cryptographic wipe, secure erase commands, or multiple pass overwrites, depending on media type.
    - **Verification:** Verify that no recoverable EPHI remains in the media before it is repurposed.
    - **Logging**: Record reuse actions with who performed wipe, method, date/time, and verification results.
7. Encryption and Security Measures:
    - **Encryption Standards**: Implement encryption for EPHI stored on electronic media, both in transit and at rest, to protect against unauthorized access.
        i. All portable devices (e.g., laptops, USB drives, removable media) carrying ePHI must use full-disk encryption or file-level encryption.
        ii. Encrypt media prior to movement or transport.
        iii. Use secure transfer protocols (e.g., SFTP, TLS) if data is moved digitally via media.
        iv. Disable or physically block unused ports (USB, SD card slots) to reduce risk of unauthorized copying.
    - **Security Protocols**: Follow industry best practices for securing electronic media during transport and while stored.
8. Accountability and Record Keeping:

- **Movement Records**: A record will be maintained of the movements of hardware and electronic media and the identity of responsible individuals.
- **Access to Records**: Ensure that records are accessible to authorized personnel for review and auditing purposes.
- Retention: All logs and records related to media movement, reuse, disposal, and authorization must be retained for at least **six (6) years**, per HIPAA documentation requirements (45 CFR §164.316(b)(2)).
- Auditability: Logs must be tamper-resistant (write-once or cryptographically protected) and accessible only by designated personnel.

9. Training & Awareness:
    - **Employee Training:** Provide regular training to SCCMHA workforce members on the procedures for handling, moving, and disposing of EPHI-containing hardware and electronic media.
    - **Media Handling Module**: Training must include modules on device/media handling, disposal, encryption, chain-of-custody, and transport protocols.
    - **Awareness Programs**: Implement awareness programs to reinforce the importance of data protection and adherence to policies.
    - **Training Frequency**: At minimum, during onboarding and annually thereafter.
    - **Acknowledgment**: Workforce must sign an acknowledgment of understanding and compliance with this policy after each training.
10. Compliance Monitoring:
    - **Audits**: Conduct periodic audits to ensure compliance with this policy and identify any areas for improvement. Random audits or spot checks of device movement/disposal practices will be performed by CIO|CQCO or Manager of Information Technology to ensure compliance.
    - **Reporting**: Establish a reporting mechanism for any incidents or deviations from policy and address them promptly.

Responsibilities:

- **IT Department:** Oversees the implementation of encryption, backup procedures, logging, inventory registry, movement coordination, and secure storage.
- **Inventory Management & Mobile Device Specialist:** maintain registry, tag devices, coordinate transport/disposal.
- **HIPAA Security Officer:** Ensures oversight and adherence to HIPAA regulations and SCCMHA's policies. Reviews and validates logs and audits compliance.
- **Chief Information Officer (CIO)** – final approval authority for removal/transport, review of logs, oversight escalations
- **All Employees:** Follow procedures for handling, moving, and disposing of hardware and electronic media containing EPHI. Participate in training and adhere to security measures.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.310(d) - *Device and Media Controls*
- 45 CFR §164.310(b) – *Workstation Use*
- 45 CFR §164.312(a)–(e) – *Technical Safeguards*
- 45 CFR §164.316(b)(2) – *Documentation Retention*
- 45 CFR §164.308(a)(1) & (a)(3) – *Administrative Safeguards*
- NIST SP 800-111 – *Guide to Storage Encryption Technologies for End User Devices*
- NIST SP 800-88 Rev.1 – *Guidelines for Media Sanitization*
- NIST SP 800-53 Rev. 5 – *Security and Privacy Controls for Information Systems* (CM-8, MP-2, MP-4, MP-6)
- FIPS 140-3 – *Security Requirements for Cryptographic Modules*
- HITECH Act §13402 – *Breach Notification Requirements*
- SCCMHA Policy 08.06.08.06 – *HIPAA Security, Security Incident Procedures*
- SCCMHA Policy 08.05.03.03 – *HITECH Breach Notification PHI*
- SCCMHA 08.06.40 – *HIPAA Security, Data Backup and Storage*
- SCCMHA 08.06.08.05 – *HIPAA Security, Security Awareness & Training*
- SCCMHA 08.06.16.01 – *HIPAA Security, Policies, Procedures, and Documentation* SCCMHA 08.06.08.04 – *HIPAA Security, Information Access Management*
-

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Implement Methods for Final Disposal of EPHI	
1. Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist
2. Determine and document the appropriate methods to dispose of hardware, software, and the data itself.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist
3. Assure the EPHI is properly destroyed and cannot be recreated.	• Senior Systems and Applications Administrator & Inventory

Develop and Implement Procedures for Reuse of Electronic Media	Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
4. Implement procedures for removal of EPHI from electronic media before the media are made available for reuse.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist.
5. Ensure that EPHI previously stored on electronic media cannot be accessed and reused.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
6. Identify removable media and their use.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
7. Ensure that EPHI is removed from reusable media before they are used to record new information.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
Maintain Accountability for Hardware and Electronic Media	
8. Maintain an inventory and record of the movements of hardware and electronic media and any person responsible for such movement.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
9. Ensure that EPHI is not inadvertently released or shared with any unauthorized party.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
10. Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software which contains EPHI.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
Develop Data Backup and Storage Procedures	

11. Ensure that a retrievable exact copy of EPHI is created when needed before movement of equipment.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.
12. Ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of EPHI during equipment relocation.	• Senior Systems and Applications Administrator & Inventory Management and Mobile Device Specialist Help Desk, Network, Information and Desktop Support.

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security: Audit Controls</td><td>Chapter: 08 – Management of Information</td><td>Subject No:
08.06.12.02</td></tr>
<tr><td rowspan="2">Effective Date:
October 01, 2020</td><td>Date of Review/Revision:
9/15/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer; Security Officer

Additional Reviewers:
Brett Lyon, Senior Applications, Information Security & BI Administrator
Ben Pelkki, Senior Database & Microsoft 365 Administrator
Compliance & Policy Team
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Matthew Devos, Senior Network & Information Security Administrator</td></tr>
<tr><td>Supersedes:
08.06.46</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.312(b) – by establishing and implementing Audit Controls that record and examine activities within information systems containing or using Electronic Protected Health Information (ePHI). This policy supports SCCMHA's broader HIPAA compliance program by ensuring all audit controls

meet standards for integrity, confidentiality, and behavioral health record protection under 42 CFR Part 2 and HIPAA. This policy aims to protect ePHI by providing mechanisms to monitor, detect, and respond to security incidents and ensure proper handling of sensitive information.

Policy:
SCCMHA will implement and maintain hardware, software, and/or procedural mechanisms to record, monitor, and examine activity within information systems that contain or use electronic protected health information (ePHI). These audit controls will be designed to support the integrity, confidentiality, and availability of ePHI by providing detailed tracking and analysis capabilities.
Audit controls will be configured to generate alerts for suspicious or high-risk activity, including failed logins, data exports, access to multiple client records in a brief time, and privilege escalation attempts. SCCMHA will use automated monitoring tools where feasible to identify potential insider threats or unauthorized disclosures.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule.
This policy also applies to any vendor-provided platforms (e.g., Electronic Health Records, cloud-based storage, or external reporting systems) where ePHI resides or is transmitted. Audit access by business associates must be contractually guaranteed through Business Associate Agreements (BAAs).

Standards:
1. Scope of Audit Controls:
    - **Risk Assessment**: SCCMHA will determine the scope of audit controls required based on a comprehensive risk assessment. This assessment will consider the sensitivity of ePHI, potential threats, vulnerabilities, and an overall impact on information security. Risk assessments will be reviewed and updated annually or whenever major systems, applications, or data flows change.
    - **Organizational Factors**: The scope will also account for organizational factors, including system architecture, data flow, and compliance requirements.
2. Audit Mechanisms:
    - **Hardware & Software:** SCCMHA will deploy appropriate hardware and software solutions to facilitate recording and examination of activities related to ePHI. This includes implementing audit trails, logging mechanisms, and monitoring tools. SCCMHA will ensure audit logs are time-synchronized via secure time sources and retained for at least six (6) years in accordance with HIPAA documentation retention requirements. Logs will be encrypted both in transit and at rest.

- **Procedural Control:** In addition to technical measures, procedural controls will be established to ensure that audit data is reviewed regularly, anomalies are investigated, and appropriate responses are taken.

3. Responsibility and Management:

    - **Information Systems (IS) Department:** The SCCMHA Information Systems (I.S.) department is responsible for the installation, configuration, and maintenance of audit control mechanisms. This includes ensuring that hardware, software, and related services are properly implemented and functioning as intended.
    - **Regular Updates**: The I.S. department will ensure that audit controls are regularly updated to address evolving threats and changes in the information system environment.

4. Monitoring and Reporting:

    - **Activity Monitoring**: SCCMHA will continuously monitor activities within information systems to detect and respond to potential security incidents. This includes reviewing logs and audit trails for suspicious or unauthorized actions.
    - **Incident Reporting**: Any discrepancies, anomalies, or potential security incidents identified through audit controls will be reported to the appropriate personnel for investigation and remediation. Alerts related to potential privacy incidents or unauthorized access to client records will also be reported to SCCMHA's Privacy Officer in accordance with SCCMHA's *08.05.03.03 – HITECH Breach Notification PHI and 08.06.08.06 – HIPAA Security*, *Security Incident Response* policies.

5. Review and Compliance:

    - **Periodic Review:** Audit control mechanisms and their effectiveness will be reviewed periodically to ensure they remain effective and aligned with HIPAA requirements. This includes assessing the adequacy of logging, monitoring, and reporting practices. SCCMHA will document the date, participants, and outcomes of each audit control review, and will maintain a corrective action plan for any identified deficiencies.
    - **Compliance Checks**: SCCMHA will conduct regular compliance checks to verify that audit controls meet the standards set by the HIPAA Security Rule and other applicable regulations.

6. Training and Awareness:

    - **Staff Training**: All relevant staff will receive training on the importance of audit controls, how to interpret audit logs, and their role in maintaining the security of EPHI. Staff training will include awareness of audit monitoring, acceptable system use, and potential consequences for unauthorized access. SCCMHA's KnowBe4 training platform will be used to deliver and track completion of this mandatory education annually.

- **Ongoing Education**: Continuous education and updates will be provided to keep staff informed about new audit control technologies and practices.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:
- The HIPAA Security Rule §164.312(b)
- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
- NIST SP 800-66 Rev. 2 – Implementing the HIPAA Security Rule
- HHS Cybersecurity Performance Goals (CPG) – 2024–2025
- SCCMHA 08.06.08.06 - Incident Response
- SCCMHA 08.05.03.03 - HITECH Breach Notification PHI Policy
- SCCMHA HIPAA Security, Security Training and Awareness Policy

Exhibits:
Exhibit A: Audit Log Review Template
Exhibit B: Quarterly Audit Control Review Checklist
Exhibit C: Audit Finding and Corrective Action Log
Exhibit D: KnowBe4 Training Verification Record (for staff audit awareness)
Procedure:

ACTION	RESPONSIBILITY
Determine the Activities that Will Be Tracked or Audited	
1. Determine the appropriate scope of audit controls that will be necessary in information systems that contain or use EPHI based on SCCMHA's risk assessment and other organizational factors.	Chief Information Officer, Compliance & Policy Team
2. Determine what data needs to be captured. a. Determine and document the retention period, encryption method, and access control measures for audit logs to ensure they meet HIPAA and agency	Chief Information Officer, Compliance & Policy Team

data protection requirements.	
Selecting the Tools that Will Be Deployed for Auditing and System Activity Reviews	
3. Evaluate existing system capabilities and determine if any changes or upgrades are necessary.	Senior Applications, Information Security & BI Administrator Senior Database & Microsoft 365 Administrator
Develop and Deploy the Information System Activity Review/Audit Policy	
4. Document and communicate to the workforce the facts about the organization's decisions on audits and reviews.	Compliance & Policy Team Systems, Information Security & Microsoft 365 Administrator Chief Information Officer, Compliance & Policy Team
Implement the Audit/System Activity Review Process	
5. Activate the necessary audit system.	Senior Applications, Information Security & BI Administrator Senior Database & Microsoft 365 Administrator Compliance & Policy Team Systems, Information Security & Microsoft 365 Administrator
6. Perform logging and auditing procedures.	Senior Applications, Information Security & BI Administrator Senior Database & Microsoft 365 Administrator Compliance & Policy Team Systems, Information Security & Microsoft 365 Administrator Compliance & Policy Team
7. Conduct quarterly review and documentation of audit logs, with findings submitted to the CIO and CQCO for review and sign-off.	

Exhibit A: Audit Log Review Template

Policy Reference: HIPAA Security Rule §164.312(b) – Audit Controls
Purpose: To document the review of system audit logs and identify potential unauthorized access, anomalies, or policy violations related to ePHI.
Review Frequency: Ongoing/As performed.

Retention Period: 6 years

Audit Log Review Details

Field	Description / Entry
System or Application Reviewed:	e.g., Sentri EHR, Network File Share, Microsoft 365, etc.
Date Range of Logs Reviewed:	From ___ / ___ / ___ to ___ / ___ / ___
Reviewer Name & Title:	
Department:	
Date of Review:	
Review Type:	☐ Routine ☐ Targeted ☐ Incident Response
Review Source / Log Location:	e.g., SIEM system, server logs, application logs

Audit Findings

Finding Type	Description / Observation	Severity (L/M/H)	Corrective Action Taken / Planned	Date Completed
Unauthorized access attempt				
Multiple failed logins				
Large data export				
Elevated privileges used				
Other anomaly				

Reviewer Summary

- Were anomalies detected? ☐ Yes ☐ No
- If yes, were they reported to the Privacy Officer or CIO within 1 business day? ☐ Yes ☐ No
- Further investigation required? ☐ Yes ☐ No

Approvals

Name/Title	Signature	Date
Reviewer		
Chief Information Officer | Chief Quality & Compliance Officer		

Exhibit B: Quarterly Audit Control Review Checklist

Policy Reference: HIPAA Security Rule §164.312(b)
Purpose: To ensure that SCCMHA audit controls are functioning effectively and align with current HIPAA and agency requirements.
Review Frequency: Quarterly
Retention Period: 6 years

Quarter and Year: Q__ 20__
Review Date: ___ / ___ / ___
Conducted By: _____
Department: _____

Checklist

Control Area	Question	Compliant (Y/N)	Comments / Actions Required
System Coverage	Are all systems containing ePHI configured for logging and monitoring?		
Log Retention	Are logs retained at least six years and protected from alteration or deletion?		
Time Synchronization	Are all systems time-synchronized to a secure source?		
Access Control	Are only authorized users permitted to view audit logs?		
Review Frequency	Are reviews performed according to policy (quarterly or more frequently)?		
Incident Response	Are anomalies or alerts escalated within 1 business day?		
Training	Have reviewers completed KnowBe4 and audit review training this year?		
Documentation	Are findings, actions, and approvals documented and retained properly?		

Review Summary

☐ No compliance issues identified
☐ Minor issues identified and corrective action initiated
☐ Significant issues identified and reported to CIO/CQCO

Sign-Off

Name/Title	Signature	Date
Reviewer		
CIO| CQCO		

Exhibit C: Audit Finding & Corrective Action Log

Purpose: To document findings from audit reviews and track corrective actions through resolution to ensure compliance with HIPAA and agency policy.
Review Frequency: Continuously
Retention Period: 6 years post-closure

Audit Finding Record

Finding ID	Date Identified	Source (Audit, Alert, Report)	Description of Issue	Severity (L/M/H)

Corrective Action Tracking

Action Required	Responsible Party	Due Date	Status (Open/In Progress/Closed)	Completion Date	Verification by (CIO/CQCO)

Closure Summary

☐ Corrective action completed and verified
☐ Issue unresolved – escalated to CIO/CQCO
☐ Follow-up audit scheduled

Exhibit D: KnowBe4 Training Verification Record

Purpose: To verify staff completion of annual HIPAA Security and Audit Awareness Training via the KnowBe4 platform.
Review Frequency: Annually
Retention Period: 6 years

Employee Information

Employee Name:
Job Title:
Department:
Supervisor:
Email:

Training Details

Course Title	Delivery Method	Completion Date	Score / Status

Certification

- ☐ I acknowledge that I have completed the above-required HIPAA and Security Awareness Training modules and understand SCCMHA's expectations for safeguarding ePHI and monitoring activities.

Employee Signature: _____ Date: ___ / ___ / ___
Verified by: _____ Date: ___ / ____ / ___

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Security: Integrity	**Chapter**: 08 – Management of Information	**Subject No**: 08.06.12.03
Effective Date: October 01, 2020	**Date of Review/Revision**: 9/15/22, 8/4/23, 9/9/24, 11/12/25 **Supersedes**: 08.06.47	**Approved By**: Sandra M. Lindsey, CEO **Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer **Additional Reviewers**: Brett Lyon, Senior Applications, Information Security & BI Administrator Matthew Devos, Senior Network & Information Security Administrator David Wolfcale, Systems Information Security & Microsoft 365 Administrator
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		

Purpose:
To assure compliance with the HIPAA Security Rule, §164.312(c) – workstation use by establishing procedures to protect Electronic Protected Health Information (EPHI) from unauthorized alteration or destruction. This policy aims to maintain the integrity and confidentiality of EPHI in workstation environments. This policy also supports SCCMHA's obligations under proposed 45 CFR §164.308(a)(1)(ii)(A)–(E) and §164.308(a)(8) by ensuring that workstation environments undergo periodic evaluation and continuous monitoring, including remote and hybrid access points, to identify and mitigate new cybersecurity threats.

Policy:

SCCMHA will implement comprehensive procedures and technical controls to ensure protection of EPHI from unauthorized alteration or destruction at workstations. These measures will include electronic mechanisms and physical safeguards to maintain the integrity and security of ePHI. SCCMHA prohibits the use of unapproved personal devices, public workstations, or unsecured wireless networks to access ePHI unless specifically authorized and configured in accordance with SCCMHA's Remote Access Policy. All workstation configurations shall comply with minimum security baselines approved by the Chief Information Officer (CIO) and HIPAA Security Officer.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule. Business Associates and subcontractors must document and maintain workstation security and integrity controls that meet or exceed those of SCCMHA and provide annual attestations or audit summaries upon request.

Standards:

A. Electronic Mechanisms:
- **Access Controls**: Implement and maintain electronic access controls (e.g., unique user IDs, automatic logoff, multifactor authentication for remote access) to restrict access to workstations where ePHI is created, received, maintained, or transmitted. Access to these workstations will be limited to authorized personnel only.
- **Audit Trails**: Utilize audit trails and logging mechanisms to monitor and record activities related to EPHI. These logs will be regularly reviewed to detect any unauthorized access or alterations.
- **Data Integrity Checks**: Implement electronic mechanisms to verify the integrity of EPHI. This includes using hash functions or checksums to detect any unauthorized changes or corruption of data.
- **Configuration and Patch Management:** Workstations must be configured in accordance with SCCMHA's approved baseline security configuration and updated within 15 days of critical patch release to mitigate vulnerabilities affecting ePHI systems.

B. Physical Safeguards:
- **Workstation Security:** Ensure that physical workstations are secured to prevent unauthorized access. This includes locking devices when not in use and using secure locations for storing devices containing EPHI.
- **Person Served-Facing Workstations:** Devices used in clinical or shared spaces must employ privacy screens and automatic screen locks after five minutes of inactivity to prevent inadvertent viewing of behavioral health information.
- **Environmental Controls**: Protect workstations from environmental hazards that could impact EPHI, such as fire, water damage, or physical

tampering. Use physical barriers and environmental controls to mitigate these risks.

C. Procedural Controls:
- **User Training:** Provide training to all staff on the proper use of workstations and the importance of protecting EPHI. This includes instructions on how to handle and safeguard EPHI, as well as recognizing and reporting potential security incidents.
- **Cybersecurity Awareness and Phishing Prevention:** Annual and just-in-time training will include modules on identifying and reporting phishing attempts, ransomware indicators, and social engineering tactics targeting behavioral health organizations.
- **Incident Response:** Procedures must ensure all suspected or confirmed alterations, destruction, or corruption of ePHI are reported within 24 hours to the HIPAA Security Officer. All incidents must be logged, investigated, and remediated according to SCCMHA's 08.05.03.03 HITECH Breach Notification PHI and 08.06.08.06 HIPAA Security, Security Incident Procedures policies.

D. Monitoring and Compliance:
- **Regular Audits**: Conduct regular audits of workstation use and security measures to ensure compliance with this policy and HIPAA requirements. Audit findings will be used to enhance and improve security practices.
- **Compliance Checks**: Regularly verify that electronic and physical controls are functioning correctly and that procedures are being followed. Address any issues or deficiencies identified during these checks.
- **Continuous Monitoring and Evaluation:** SCCMHA will employ automated monitoring tools, such as endpoint detection and response (EDR) systems or integrity verification software, to identify unauthorized changes to EPHI or workstation configurations. The HIPAA Security Officer will review monitoring results at least quarterly.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:
- The HIPAA Security Rule §164.312(c)
- 45 CFR §164.308(a)(1), (a)(5), (a)(8), (b)(3)
- OCR Cybersecurity Guidance (2023, 2024)
- HIPAA Security Rule NPRM (Federal Register, March 2025)
- 42 CFR Part 2, §2.16 (Security for records)

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Identify All Users Who Have Been Authorized to Access EPHI	
1. Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
2. Address this identification in conjunction with the identification of unauthorized sources (see below) that may be able to intercept the information and modify it.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator
Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It	
3. Identify scenarios that may result in modification to the EPHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator
4. Conduct this activity as part of the risk analysis. a. Document workstation and endpoint configurations, including encryption status, patch level, and user access permissions, as part of the annual risk analysis. b. Validate that remote workstations comply with the same technical and procedural safeguards as onsite systems.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
Develop the Integrity Policy and Requirements	

5. Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
Implement Procedures to Address These Requirements	
6. Identify and implement methods that will be used to protect the information from modification.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
7. Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
Implement a Mechanism to Authenticate EPHI	
8. Implement electronic mechanisms to verify that EPHI has not been altered or destroyed unauthorizedly.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
9. Consider possible electronic mechanisms for authentication such as: • Error-correcting memory • Magnetic disk storage • Digital signatures • Check some technology.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
Establish a Monitoring Process to Assess How the Implemented Process Is Working	
10. Review existing processes to determine if objectives are being addressed.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator

11. Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.	HIPAA Security Officer Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
12. Maintain audit logs, integrity verification results, and monitoring records for a minimum of six (6) years in accordance with 45 CFR §164.316(b)(2).	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer
13. Submit annual compliance reports summarizing findings, corrective actions, and technology updates to the CIO and HIPAA Security Officer.	Senior Applications, Information Security & BI Administrator Senior Network & Information Security Administrator HIPAA Security Officer Chief Information Officer | Chief Quality & Compliance Officer

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Security: Person or Entity Authentication	**Chapter**: 08 – Management of Information	**Subject No**: 08.06.12.04
Effective Date: October 01, 2020	**Date of Review/Revision**: 9/15/22, 8/4/23, 9/9/24, 11/12/25 **Supersedes**: 08.06.49	**Approved By**: Sandra M. Lindsey, CEO **Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer **Additional Reviewers**: Matt Devos, Senior Network & Information Security Administrator Chad Revell, Inventory Management and Mobile Device Specialist Ben Pelkki, Senior Database & Microsoft 365 Administrator Brett Lyon, Senior Applications, Information Security & BI Administrator David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.312(d) – Person or Entity Authentication, 42 CFR Part 2 (§2.16 – Security for Records), and the HITECH Act (§13401), this policy establishes procedures to verify the identity of individuals and entities

seeking access to Electronic Protected Health Information (ePHI) or Part 2 data, ensuring safeguards against unauthorized access.

Policy:
SCCMHA will implement and maintain procedures to authenticate the identity of people or entities seeking access to EPHI. Authentication procedures apply to all access points, including on-premises systems, cloud-based applications (e.g., Microsoft 365), mobile access, and remote sessions. SCCMHA uses Azure Active Directory (AAD) with Conditional Access and audit logging to ensure identity verification and traceability of all authentication events.

Application:
The HIPAA Security Rule and this Policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA policy or develop their own policies and procedures which comply with the applicable section of the HIPAA Security Rule. All business associates and subcontractors with remote or cloud-based access to SCCMHA's systems must implement equivalent authentication safeguards, including MFA and unique credentialing. Business associate agreements (BAAs) must document these technical requirements and provide evidence of compliance upon request.

Standards:
A. Authentication Mechanisms: All users must authenticate using unique credentials before accessing systems.

- Username & Passwords: To log into any Information Systems that are managed and administered by SCCMHA's Information Technology Department, the following are required:
    - Unique username: Each user must be assigned a unique username to track and manage their access.
    - Password Complexity: Passwords must meet complex requirements, including a minimum length, the inclusion of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed regularly or immediately following any suspected compromise. Accounts will be locked after five unsuccessful login attempts and require IT verification before reactivation.

B. Multifactor Authentication (MFA): MFA must be integrated into the login process for accessing EPHI and other sensitive systems. MFA must be required for all remote access, administrative accounts, Microsoft 365 access, and any application that stores or transmits ePHI or Part 2 data. Credential Management:

- Prohibition of Sharing: Users will NEVER use another person's logon credentials. Everyone is responsible for their own credentials and must ensure they are not disclosed or used by unauthorized people. Shared or generic accounts are prohibited for all systems containing ePHI or Part 2 data. Credentials must never be stored in shared files, written notes, or unencrypted documents.

- Account Compromise: If a user's credentials are suspected to be compromised, the user's account will be disabled immediately, and the user's password will be reset. The IT department will investigate the compromise, and the user's account will only be re-enabled once the issue is resolved, and the user's identity is confirmed.

C. Provisioning and Deactivation:
    - Access Provisioning: User's will be provisioned based on Role-Based Access Control (RBAC), and system access credentials will be provided based on predefined roles that align with job functions by a member of the IT department when:
        - Human Resources notifies the IT department via Activation/Deactivation process of new hires, contractors, department changes, title changes, etc. for board-op staff.
        - Network Providers will notify the IT department via a Helpdesk ticket of new hires, department changes, title changes, etc.
        - After a Helpdesk ticket is created requesting activation to systems, the ticket will be forwarded to Department Supervisors, Directors, etc. requesting approval of access based on job functions.
        - Employees are restricted from accessing data beyond their job responsibilities unless otherwise approved by supervisors or director level with justification for access needed.
        - All required information must be submitted to establish and validate user access, including role and access level by IT.
        - Access Reviews will be conducted by the IT Access & Identity Management Group (AIMG) on a regular basis to ensure roles and access fall within the user's assigned job responsibilities.
    - Account Deactivation: Access rights will be promptly revoked for users who leave the organization or no longer require access.
        - Deactivation must occur within 24 hours of separation or role change notification. IT must document completion within the Helpdesk ticket system.
        - For Microsoft 365 and cloud-integrated applications, the user's Active Directory account will be disabled, and all associated tokens, shared links, and device connections will be revoked.
        - The IT department will manage deactivation in accordance with HR policies and procedures regarding termination or change of employment status.
        - Network providers will submit a Helpdesk ticket requesting a terminated user's account be deactivated.

D. Data Classification and Restrictions:
    - Persons served data is categorized based on sensitivity levels.
    - Extremely sensitive information is accessible only to authorized personnel. Access to extremely sensitive data, including Part 2 substance use disorder records, shall require elevated authentication controls and encryption in transit and at rest, in accordance with SCCMHA's Transmission Security Policy (08.06.12.05).

E. Authentication Policy Enforcement:
- Policy Adherence: Users must acknowledge and comply with authentication policies during onboarding and periodic security training. Non-compliance with authentication requirements may result in disciplinary action.
- Auditing and Monitoring: Authentication logs will be maintained and reviewed regularly to detect any unauthorized access attempts or anomalies.
- Authentication activity will be monitored using Microsoft 365 Defender and Azure AD audit logs. Any anomalies or failed MFA events will be automatically reported to the Information Security Officer and documented in the Security Incident Log.

F. Incident Management:
- Incident Reporting: Users must report any suspected or actual breaches of their authentication credentials immediately to the IT Department.
- Incident Investigation: The IT Department will investigate incidents of credential compromise, including determining the impact and taking appropriate corrective actions to prevent recurrence. All credential-related incidents involving ePHI or Part 2 data must be reported to the Privacy and Compliance Officers within 24 hours. If a breach is suspected, law enforcement delay protocols and breach notification procedures will be followed by SCCMHA's HIPAA Breach Notification Policy.

Responsibilities:
- **IT Department**: Responsible for implementing and managing authentication mechanisms, provisioning, and deactivating credentials, monitoring authentication logs, and investigating incidents.
- **Privacy Officer:** Ensures authentication mechanisms meet HIPAA and Part 2 confidentiality standards and reviews access exception reports.
- **Compliance Officer:** Oversees periodic authentication audits, reviews MFA compliance reports, and ensures policy adherence across departments.
- **Human Resources:** Responsible for notifying IT of new hires, terminations, and changes in employment status affecting access.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:
- The HIPAA Security Rule §164.312(d)
- • 45 CFR §164.308(a)(3), (a)(4), (a)(5), and (a)(6)
- • 42 CFR §2.16 and §2.53
- • HITECH Act §13401–13410
- • NIST SP 800-63B Digital Identity Guidelines
- • OCR Cybersecurity Proposed Rule (2024)

Exhibits:

None

Procedure:

ACTION	RESPONSIBILITY
Determine Authentication Applicability to Current Systems/Applications	
1. Identify methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed. (45 CFR § 164.304). Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems.	1. IT Department's Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Evaluate Authentication Options Available	
2. Weigh the relative advantages and disadvantages of commonly used authentication approaches. There are four commonly used authentication approaches available: • Something a person knows, such as a password, • Something a person has or is in possession of, such as a token (smart card, ATM card, etc.), • Some type of biometric identification a person provides, such as a fingerprint, or • A combination of two or more of the above approaches.	2. IT Department's Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Select and Implement Authentication Option	

3. Consider the results of the analysis conducted regarding the authentication options, select appropriate authentication methods, and implement the methods selected into SCCMHA's operations and activities.	3. IT Department's Information Security Team Chief Information Officer & Chief Quality and Compliance Officer
Network Access	
4. System Access will be granted upon proper approval process and the submission of a Helpdesk ticket. User credentials will be provided to that user and no others.	4. IT Department's Network & Helpdesk Teams
5. Passwords will be reset upon notice to the IT Helpdesk.	5. IT Department's Clinical Applications & Helpdesk Teams
Sentri EHR (Electronic Health Record)	
6. System Access will be granted upon proper approval process and the submission of a Helpdesk ticket. User credentials will be provided to that user and no others.	6. IT Department's Network & Helpdesk Teams
7. When Access has been granted, the IS staff will send an email to the staff with a cc: to the responsible HIPPA privacy officer, the user's supervisor, SCCMHA's training department, SCCMHA's auditing department and the staff that is requesting access.	7. IT Department's Network & Helpdesk Teams
8. The first logon will require the staff to change their password, no exception.	8. IT Department's Network & Helpdesk Teams
9. System Access will be granted upon proper approval process and the submission of a Helpdesk ticket. User credentials will be provided to that user and no others.	9. IT Department's Network & Helpdesk Teams

10. **Microsoft 365 Authentication:** For all users accessing Microsoft 365 services, authentication must occur through SCCMHA's Azure Active Directory with Conditional Access policies enforcing MFA, location-based restrictions, and session controls.	10. IT Department's Network Security & M365 Teams
11. **Periodic Review:** Authentication configurations and user credentials will be reviewed quarterly by the IT Access & Identity Management Group (AIMG) in coordination with the Privacy Officer to confirm that user identities remain valid, MFA enrollment is current, and inactive accounts are disabled.	11. IT Access & Identity Management Group (AIMG)

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Security: Transmission Security	**Chapter**: 08 – Management of Information	**Subject No**: 08.06.12.05
Effective Date: October 01, 2020	**Date of Review/Revision**: 9/20/22, 8/4/23, 5/23/24, 9/9/24, 11/12/25 **Supersedes**: 08.06.45	**Approved By**: Sandra M. Lindsey, CEO
SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY		**Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer **Authored By**: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer, Security Officer **Additional Reviewers**: Matt Devos, Network & Information Systems Administrator Brett Lyon, Senior Applications, Information Security & BI Administrator Ben Pelkki, Senior Database & Microsoft 365 Administrator David Wolfcale, Systems, Information Security & Microsoft 365 Administrator

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.312(e) – Transmission Security, by implementing measures to protect electronic protected health information (ePHI) during electronic transmission and safeguard against unauthorized access and modification. This policy also ensures compliance with the HIPAA 2024 Final Rule and proposed 2025 Cybersecurity Enhancements, emphasizing stronger protections for

electronic transmission of PHI, business associate oversight, and documentation of secure communication practices, including behavioral health confidentiality obligations under 42 CFR Part 2.

Policy:
SCCMHA will implement and maintain technical security measures to protect ePHI during electronic transmission over networks to prevent unauthorized access and ensure data integrity. SCCMHA will use multi-factor authentication (MFA) for all remote and network access involving ePHI transmission and will ensure that any automated transmission mechanisms are subject to periodic verification and security testing.

Application:
The HIPAA Security Rule and this policy apply to SCCMHA, its business associates, and any subcontractor required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may choose to adopt and comply with the relevant SCCMHA policy or develop their own policies and procedures which comply with the applicable section of the HIPAA Security Rule. Business associates and subcontractors transmitting SCCMHA ePHI must demonstrate encryption and transmission controls equivalent to SCCMHA standards and must provide documentation of annual security testing and workforce training related to secure data transmission.

Standards:
A. **Integrity Controls**: Security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of will be implemented.
    - **Data Integrity:** Implement mechanisms to ensure the integrity of ePHI is transmitted electronically. This includes using digital signatures to verify that the data has not been altered or corrupted during transmission.
    - **Validation and Verification**: Procedures must be in place to validate the authenticity of data received and confirm that it has not been improperly modified or tampered with during transmission.
    - **File Integrity Monitoring**: Implement automated integrity verification tools for systems transmitting ePHI, such as checksums or hash-based validation.
B. **Encryption:** A mechanism to encrypt EPHI whenever deemed appropriate will be implemented.
    - **Encryption Mechanisms:** Use encryption to protect EPHI during transmission over public and private networks. This includes the use of secure protocols (e.g., TLS/SSL for web traffic, S/MIME for email, and VPNs for remote access).
    - **Key Management:** Implement procedures for managing encryption keys, including key generation, distribution, storage, and retirement. Ensure that keys are kept secure and are accessible only to authorized personnel.
    - **Encryption Algorithm Standards**: Use NIST-approved encryption algorithms (e.g., AES-256) for transmission and storage, and review encryption configurations at least annually.
C. Access Controls:

- **Authentication:** Ensure that systems and applications involved in transmitting EPHI use strong authentication mechanisms to verify the identity of users and systems.
- **Authorization:** Implementation of access controls to restrict transmission of EPHI to authorized individuals and entities only. This includes role-based access controls and privilege principles.
- **Multi-Factor Authentication (MFA):** Require MFA for any system that facilitates remote transmission of ePHI, including VPN, secure email, or cloud platforms.

D. Transmission Security Measures:
- **Secure Channels:** Ensure that EPHI is transmitted over secure channels, such as SENTRI messaging, encrypted emails, or secure file transfer protocols (e.g., SFTP). Avoid using unencrypted or insecure methods for transmitting EPHI.
- **Network Security:** Protect the network infrastructure used for transmitting EPHI by implementing firewalls, intrusion detection/prevention systems, and network segmentation.
- **Third-Party Cloud & Messaging Platforms**: Conduct security reviews for any cloud or communication platforms used for transmitting ePHI to ensure compliance with encryption, audit logging, and data residency requirements.
- **Behavioral Health Data Sensitivity**: Transmission of 42 CFR Part 2 records must only occur through encrypted, access-restricted systems that prevent re-disclosure and include specific consent language.

E. Incident Management:
- **Incident Reporting:** Establish procedures for reporting and responding to incidents involving unauthorized access or modifications to EPHI during transmission. Users must report any suspicious activity or breaches immediately.
- **Incident Investigation:** The IT Department will investigate incidents involving the transmission of EPHI, determine the impact, and implement corrective actions to prevent recurrence.
- **Documentation**: All transmission-related security incidents, including phishing, man-in-the-middle attacks, or mis-sent encrypted emails, must be documented in the incident management system and retained for at least six years.

F. Monitoring and Auditing:
- **Activity Logging:** Implementation of logging and monitoring mechanisms to track the transmission of EPHI and detect any anomalies or unauthorized access attempts. Logs should be reviewed regularly to identify potential security issues.
- **Regular Audits:** Conduct periodic audits of transmission security controls to ensure they are effective and up to date with current security standards and compliance requirements.
- **Automated Alerts**: Implement automated alerting for failed or anomalous transmission attempts and review logs at least quarterly.
- **KnowBe4 Simulation Tracking**: Maintain records of employee performance in phishing and secure-email simulations to verify workforce awareness.

G. Training & Awareness:

- **Security Training:** Provide ongoing training for all workforce members on secure transmission practices, including the use of encryption, secure channels, and recognizing phishing or other attacks targeting transmission of EPHI.
- **Ongoing Reinforcement**: Training completion rates and test results from the KnowBe4 security awareness platform will be documented and reviewed during quarterly compliance meetings.
- **Role-Based Emphasis**: Behavioral health clinicians, administrative staff, and IT personnel will receive targeted modules addressing secure transmission of sensitive behavioral health and Part 2 records.

Responsibilities:

- **IT Department:** Responsible for implementing and managing encryption technologies, access controls, network security, and incident response related to transmission security.
- **Chief Information Officer:** Oversees security awareness and transmission-related phishing simulations, documents result and ensures remedial training for repeat vulnerabilities.
- **Compliance Officer:** Responsible for overseeing the policy's implementation, conducting audits, and ensuring compliance with HIPAA regulations.
- **Management:** Responsible for ensuring staff awareness and adherence to transmission security policies.
- **Users:** Responsible for following procedures for securely transmitting EPHI and reporting any security incidents promptly.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

- The HIPAA Security Rule §164.312(e)
- 45 CFR §164.308(a)(5), (a)(6), (a)(8)
- HHS OCR 2024 Final Rule (89 FR 30852)
- HHS Proposed Rule: *HIPAA Security Rule Enhancements and Cybersecurity Requirements* (anticipated 2025)
- NIST SP 800-66 Rev. 2 (2024)
- NIST SP 800-52 Rev. 2 (TLS Guidelines)
- 42 CFR Part 2 (2024 update)

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information	
1. Identify scenarios that may result in modification of the EPHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).	1. Information Security Team & HIPAA Security Officer
Develop and Implement Transmission Security Policy and Procedures	
2. Establish a formal (written) set of requirements for transmitting EPHI. a. Verify that all chosen methods and tools meet current NIST and HIPAA encryption standards and that MFA is enabled for all remote transmissions.	2. Information Security Team & HIPAA Security Officer
3. Identify methods of transmission that will be used to safeguard EPHI.	3. Information Security Team & HIPAA Security Officer
4. Identify tools and techniques that will be used to support the transmission security policy.	4. Information Security Team & HIPAA Security Officer
5. Implement procedures for transmitting EPHI using hardware and/or software, if needed. Conduct initial and annual testing of encrypted communication channels, including TLS configuration validation and email encryption testing logs.	5. Information Security Team & HIPAA Security Officer
Implement Integrity Controls	
6. Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.	6. Information Security Team & HIPAA Security Officer

Implement Encryption 7. Implement a mechanism to encrypt EPHI whenever deemed appropriate. 8. Document encryption configuration reviews, key management logs, and staff training completion records as part of the security management process.	7. Information Security Team & HIPAA Security Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Controlled Access & Least Privilege Access Policy</td><td>Chapter: Chapter section of SCCMHA policy & procedure manual - number & name</td><td>Subject No: 08.06.12.06</td></tr>
<tr><td rowspan="2">Effective Date:
11/12/2025</td><td>Date of Review/Revision:</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Chief Information Officer, Chief Quality and Compliance Officer

Authored By:
Christina Saunders, Administrative Assistant to CIO|CQCO

Additional Reviewers:
Kentera Patterson, Officer of Recipient Rights and Compliance</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
The purpose of this policy is to establish guidelines for controlled access and least privileged access to sensitive data and systems, ensuring SCCMHA employees have access only to the information and resources necessary for their job roles. This policy's goal is to minimize the risk of threats and accidental data exposure by enforcing strict access controls in compliance with regulatory requirements, such as HIPAA.
This policy also supports compliance with the HIPAA Privacy Rule, the HITECH Act breach notification requirements, and the 2023–2025 proposed HIPAA modifications emphasizing strengthened accountability for Business Associates and subcontractors.

Application:
This policy applies to all SCCMHA workforce members, including employees, interns, volunteers, and temporary staff who interact with Business Associates or subcontractors. SCCMHA departmental managers must ensure that business associates under their operational control comply with this policy.

Policy:
SCCMHA will implement controlled access measures and enforce principles of least privileges (PoLP) to safeguard people served information, prevent unauthorized access, and ensure compliance with regulatory requirements. SCCMHA will maintain a

centralized inventory of all active Business Associate Agreements and subcontractor agreements. This inventory will include the effective date, expiration date, contact information, data access level, and last review date. No data exchange involving ePHI may begin until the agreement is executed and recorded in this inventory.

Roles and Responsibilities:

1. **Chief Information Officer (CIO) | Chief Quality & Compliance Officer (CQCO)**
    1. Oversee the organization's information security strategy.
    2. Ensure that access control policies align with business and regulatory requirements.
    3. Work with security teams to implement necessary security controls.
    4. Review and approve changes to access control policies and procedures.
2. **Security Administrator**
    1. Implement and manage access control mechanisms.
    2. Ensure authentication and authorization controls are properly configured.
    3. Monitor system logs and investigates unauthorized access attempts.
    4. Conduct regular system security assessments and updates.
3. **Electronic Health Records (EHR) Coordinator**
    1. Enter and maintain accurate persons served data in the EHR system.
    2. Ensure data integrity and security within the system.
    3. Verify that only authorized individuals have access to persons served records.
    4. Report any inconsistencies or suspected unauthorized access to the Security Administrator.
4. **Supervisors & Directors**
    1. Request, review, and approve access requests for employees within their department.
    2. Report any discrepancies or unauthorized access to the Security Administrator or Compliance Officer.
5. **Employees & Contractors**
    1. Adhere to access control policies and procedures.
    2. Use only authorized credentials to access systems.
    3. Report any suspected security breaches or unauthorized access.
    4. Ensure secure handling of sensitive people served data.
6. **Compliance Officer**
    1. Monitor compliance with access policies and regulatory requirements.
    2. Conduct periodic audits of access control measures.
    3. Ensure corrective actions are taken in case of non-compliance.
    4. Provide training and awareness programs on security best practices.

Standards:

Controlled Access Measures:

1. **Authentication and Authorization:**
    - All users must authenticate using unique credentials before accessing systems.
    - Multi-factor authentication (MFA) is required for access to Sentri.

2. **Role-Based Access Control (RBAC):**
    - Access is granted based on predefined roles that align with job functions.
    - Employees are restricted from accessing data beyond their job responsibilities.
3. **Data Classification and Restrictions:**
    - Persons served data is categorized based on sensitivity levels.
    - Highly sensitive information is accessible only to authorized personnel.
4. **Physical and Logical Access Controls:**
    - Restricted physical access to areas where sensitive data is stored.
    - Secure workstations with automatic log-off and restricted removable media usage.

Least Privilege Access Measures:

1. **Need-to-Know Principle:**
    - Users receive the minimum necessary access to perform their duties.
    - Temporary access is granted only for specific tasks and revoked afterward.
2. **Regular Access Reviews:**
    - Periodic audits of user access levels.
    - Immediate revocation of access for employees who change roles or leave the organization, including disabling profiles, setting termination and hire dates, and ensuring that security roles assigned are applicable.
3. **Monitoring and Logging:**
    - All access activities are logged and reviewed regularly for suspicious activity.
    - Unauthorized access attempts trigger alerts and are subject to investigation.
4. **Incident Response and Reporting:**
    - Any suspected or confirmed unauthorized access must be reported immediately.
    - A response plan is in place to investigate and mitigate security breaches.

Requirements for Business Associate Agreements:

1. SCCMHA will only permit a Business Associate to handle ePHI if satisfactory assurances are obtained through a written Business Associate Agreement (BAA) that meets all applicable HIPAA Security and Privacy Rule requirements, including those related to minimum necessary access, data retention and destruction, security incident notification, and cooperation with breach investigations.
2. **Subcontractor Agreements**: Business Associates must ensure that their subcontractors apply the same or greater safeguards to ePHI as those required of the Business Associate under its agreement with SCCMHA. SCCMHA reserves the right to request documentation of subcontractor compliance, including audit results or training certifications, when appropriate.
3. **Documenting Assurances**: Business Associates must maintain written policies and procedures consistent with the HIPAA Security Rule and provide these upon request to SCCMHA for review or audit verification.
4. **Data Retention and Termination**: The BAA must include requirements for the secure return or destruction of ePHI upon termination of the agreement, in

compliance with §164.504(e)(2)(J), and must define the retention period for audit purposes.

5. **Breach Response Cooperation:** Business Associates must cooperate fully with SCCMHA during security incident and breach investigations, providing timely and complete responses as required under §164.410 and §164.412.
6. **Annual BAA Review**: The Compliance Department will perform an annual review of all BAAs to verify that agreements reflect current legal and operational standards.

Definitions:
See I.T./I.S. Policy 08.06.00.01, which contains a full list of relevant words and terms used in this section's Policies.

References:

Exhibits:
Exhibit A: System Access for New Employees or Contractors Questionnaire
Exhibit B: Access Provisioning Checklist
Exhibit C: Incident Categorization
Exhibit D: Sample Access Control Log

Procedure:

	ACTION	RESPONSIBILITY
I.	**Identify system access requirements for new employees or contractors.** **To determine system access requirements for new employees or contractors, see ***Exhibit A: System Access for New Employees or Contractors Questionnaire***	**Supervisors or Directors**
II.	**Submit access requests via the Helpdesk ticket system based on job role and function**, supervisors and employees are required to provide the following information to ensure accurate and secure access provisioning: see ***Exhibit B: Access Provisioning Checklist*** **a. Employee/Contractor Information** 1. Full Name 2. Job Title & Department 3. Employee/Contractor Status a) **Full-time -** Works a standard number of hours (e.g., 40 hours per week) b) **Part-time** – Works fewer hours than a full-time employee. c) **Temporary** - Hired for a specific period or project, often through a staffing agency.	**Supervisors and Employees**

d) **Intern** – A student or recent graduate, often working for experience rather than full wages.
e) **Contractor** - Provides specialized expertise on a contractual basis, either independently or through a firm.
f) **On-Call Employee** – Works only when needed, often with unpredictable hours.
g) **Casual Employee** - is employed on an irregular or as-needed basis, typically without a firm commitment from the employer regarding ongoing work.

4. Start Date & Expected End Date (if applicable)

b. <u>Access Requirements</u>

1. Specific systems, applications, or databases required (e.g., EHR, scheduling system, billing system)
2. Assign level of access needed.
   a) **Administrative** - Full system control, including user management, security settings, and system configurations.
      a. Example Roles: IT Administrators, System Administrators, Compliance Officers
   b) **Allied Health Professional** - Access to records necessary for treatment planning and documentation (e.g., therapy notes, imaging).
      a. Example Roles: Physical Therapists, Occupational Therapist, Pharmacists, Dietitians
   c) **Billing & Coding** - Access to patient billing records, insurance claims, and procedure codes, but no direct medical data.
      a. Example Roles: Medical Billers, Coders, Insurance Specialists
   d) **Emergency Access (Break the Glass)** - Temporary full access in emergency situations, with automatic logging for security.
      a. Example Roles: Crisis Teams, On-Call Crisis Specialists, MRSS
   e) **Front Desk/Reception** - Limited access for scheduling, demographic data, and insurance verification, but no clinical data.
      a. Example Roles: Receptionists, Patient Coordinators, Billing Staff
   f) **Nurse -** Access to patient records for administering treatments, updating vitals, and care notes.

a. Example Roles: Registered Nurses (RNs), Licensed Practical Nurses (LPNs), Medical Assistants

g) **Patient Access (via CEHR Patient Portal)** - Limited access to personal health records, appointment scheduling, and communication with providers.
   a. Example Roles: Patients, Guardians, Caregivers with Proxy Access

h) **Physician/Provider -** Full access to patient records, test results, prescriptions, and clinical documentation.
   a. Example Roles: Doctors, Nurse Practitioners, Physician Assistants

i) Read-only - Read-only access to certain patient information for audits, research, or compliance checks.
   a. Example Roles: Regulatory Auditors, Legal Teams, Researchers

j) **Superuser/Power User** - High-level access for troubleshooting, training, or overseeing workflows.
   a. Example Roles: Senior Medical Staff, EMR Trainers, Supervisors

3. Justification for access (why is access necessary for their role?)
4. Any restricted data they should *not* access

c. <u>Security & Compliance Measures</u>

1. Confirmation of completion of required security training (if applicable)
2. Multi-factor authentication (MFA) enrollment status (if required)
3. Location restrictions

a) Facility Based Access - Users can only access the EMR when physically present in the hospital, clinic, or healthcare facility. Prevents external access to protect sensitive patient data.

b) **IP Address Whitelisting -** Access is only allowed from specific, pre-approved IP addresses (e.g., hospital network, VPN). Blocks unauthorized remote access from unknown locations.

c) **Geofencing** - Uses GPS or network location to restrict access within a defined geographic area (e.g., within a specific city or state). Can block access from high-risk locations or foreign

countries. d) **Device-Based Location Control** - Restricts access to pre-approved or registered devices (e.g., hospital-issued computers, tablets). Prevents access from personal or untrusted devices, even if the location is permitted. e) **Role-Based Location** - Different roles have different location-based restrictions (e.g., doctors can access them remotely via VPN, but billing staff must be on-site). Ensures minimal necessary access based on job function. **d. <u>Approval & Authorization</u>** 1. Supervisor or Director approval 2. Access expiration date (for temporary roles)	
e. **<u>Business Associate Agreements (BAA)</u>** 1. SCCMHA will maintain a centralized BAA Inventory log (Excel or database) documenting the business associate's name, purpose, contact, agreement status, and next review date.	**Contracts & Procurement**
III. **Review and approve access requests**, the following should be completed to ensure secure and appropriate system access: **a. <u>Verify Employee/Contractor Information</u>** 1. Confirm that the individual requesting access is an active employee at SCCMHA or a contracted network provider or otherwise approved contractor. 2. Ensure the job title provided and department align with SCCMHA's Active Directory (AD) records.	**EHR Coordinator & Security Administrator**
b. <u>Validate Access Justification</u> 1. Review the access request form to ensure access is necessary for the employee's job function. 2. Confirm that the requested access level (e.g., read-only, data entry, administrative) matches their responsibilities. 3. Ensure the request complies with the **principle of least privilege (PoLP)** granting only the minimum necessary access.	**Security Administrator**
c. <u>Check System & Compliance Requirements</u> 1. verify that the requested access aligns with organizational policies and regulatory compliance (e.g., HIPAA, HITECH). 2. Ensure the individual has completed the required security and confidentiality training before granting access. 3. Determine whether additional security controls are required. 4. If remote access is requested, confirm that remote	**Access Management Group**

security protocols are in place.	
d. <u>Obtain Necessary Approvals</u> 1. Supervisor/Director approval for access. 2. Access Management Group (AMG) review and approval 3. CIO review and approval (if necessary for high-level access)	**Security Administrator**
e. <u>Document & Communicate Decision</u> **1.** Maintain Access Control Log (***Exhibit D: Sample Access Control Log)*** of all addition and terminations for audit and review processes. a. Record the approved or denied access request in an access control log. 2. Notify the employee/contractor and supervisor/director of the access decision. 3. If approved, provide login credentials or system access instructions. 4. If denied, provide a reason and alternative solutions (if applicable).	**EHR Coordinator**
f. <u>Assign Expiration & Review Date</u> 1. Set an access expiration date for temporary employees or contractors. 2. Schedule a follow-up review to reassess the necessity of the granted access.	**EHR Coordinator**
IV. **Configure and grant appropriate access levels**, the following should be completed to ensure secure and accurate system access provisioning:	
a. <u>Validate Approved Access Request</u> 1. Confirm that the access request has been fully reviewed and approved by the appropriate personnel (Supervisor/Director, AMG, Compliance Officer, Security Administrator, CIO). 2. Verify that the requested access level matches the employee's job function and role-based access controls (RBAC).	**Security Administrator**
b. <u>Configure System Access</u> 1. Create or modify the user account in the required system(s). 2. Assign the correct role and access level (e.g., read-only, data entry, administrative). 3. Restrict access to necessary data categories a. **Personal Identifiable Information (PII) or Personal Health Information (PHI)** – <u>*Restricted for Privacy Protection*</u> i. **Full Access:** Physicians, Nurses, Front Desk (for scheduling).	**EHR Coordinator**

ii. **Restricted Access:** Billing (partial data), Researchers (de-identified data).
iii. **Examples:**
1. **Names** - full, partial, initials, or aliases
2. **Dates** - birthdate, date of death, admission/discharge, appointment date
3. **Contact Numbers** - home, cell, work, emergency contacts, fax number
4. **Email Address** - personal or work
5. **Geographic Identifiers** - smaller than state – i.e. street address, city, county, zip code
6. **Full or Partial Identifiable Numbers –** medical transaction numbers, account numbers, Medical Record Number (MRN), Social Security Number (SSN), Insurance policy numbers, certificate/license numbers
7. **Vehicle Identifiers & Serial Numbers –** includes license plate numbers
8. **Device Identifiers & Serial Numbers –** Unique medical device IDs tied to an individual
9. **Web URLs & IP Addresses –** linking to individual healthcare information
10. **Biometric Identifiers –** fingerprints, retinal scans, voiceprints
11. **Full face photos or comparable images**
12. **Any other unique number, code, characteristic used to identify individuals.**

b. **Medical Records & Clinical Notes** – *Restricted by Role*
i. **Full Access:** Physicians, Nurses, Behavior Specialists.
ii. **Restricted Access:** Billing (procedure

codes only), Admin (limited access).
iii. **Examples:** Diagnoses, Progress Notes, Treatment Plans, Lab Results.

c. **Mental Health & Behavioral Records** – *Highly Restricted*
   i. **Full Access:** Psychiatrist, Licensed Mental Health Providers.
   ii. **Restricted Access:** Primary Care (limited view), ER (emergency-only).
   iii. **Examples:** Therapy Notes, Psychiatric Diagnoses, Substance Abuse Treatment Records.

d. **Prescription & Medication History** – *Restricted for Safety*
   i. **Full Access:** Physicians, Pharmacists, Nurses (for administration).
   ii. **Restricted Access:** Billing (medication codes only), Researchers (anonymized)
   iii. **Examples:** Current Medications, Dosages, Prescriber Information.

e. **Financial & Billing Information** – *No Clinical Data Access*
   i. **Full Access:** Billing & Coding Teams, Insurance Processors.
   ii. **Restricted Access:** Clinicians (cannot alter billing), Front Desk (limited view).
   iii. **Examples:** Payment History, Insurance Claims, Procedure Codes.

f. **Legal & Compliance Records** – *Strictly Controlled*
   i. **Full Access:** Compliance Officers, Legal Teams.
   ii. **Restricted Access:** Clinicians (unless legally required), Admin (limited).
   iii. **Examples:** Consent Forms, Subpoenas, Legal Disputes

g. **Research & De-Identified Data** – *Controlled & Anonymized*
   i. **Full Access:** Approved Researchers (with IRB approval).
   ii. **Restricted Access:** No identifiable patient information; only aggregated data.
   iii. **Examples:** Clinical Trial Data, Case

Studies, Population Health Analytics *h.* **Emergency "Break Glass" Access** – *Strict Logging & Justification* i. **Full Access (Temporary):** ER Physicians, Crisis Teams, MRSS ii. **Restricted Access:** Must justify and log access (audit trail required). **iii. Examples:** Crisis Intervention Services, Disaster Response	
c. Apply Security Controls 1. Implement location-based restrictions (e.g., on-site access only for certain systems). 2. Disable access to unnecessary applications or data repositories. 3. Log all access changes in the Access Control Log for audit tracking.	**Security Administrator**
d. Communication of Access Information 1. Notify the employee/contractor, supervisor/director that access has been granted. 2. Provide login credentials securely (never via email in plain text). 3. Share system usage guidelines, security policies, and best practices. 4. Ensure the employee completes any required security training before system use.	**EHR Coordinator**
e. Document Access Provisioning 1. Update the **Access Control Log** with details of granted access, including: a. Employee/contractor name and role b. System(s) accessed c. Level of access granted d. Approval records e. Expiration/review date for temporary access 2. Store documentation for compliance audits.	**EHR Coordinator**
f. Conduct a Post-Configuration Review 1. Verify that the user can log in and access only the authorized systems and data. 2. Test that MFA and other security measures are functioning correctly. 3. Confirm that unauthorized applications or data are inaccessible.	**Security Administrator**
V. **Conduct access training for new users.** a. **Develop Training Materials** 1. Create a presentation or handbook that covers the principles of controlled access and least privilege. 2. Include key topics such as:	**Security Administrator**

a. What does the least privileged principle mean? b. Why controlled access is important c. Examples of what constitutes excessive access d. How users can request or modify access levels e. The consequences of violating access policies	
b. **Schedule Training Sessions** 1. Schedule regular training sessions (e.g., bi-weekly or monthly) or create an on-demand online training module.	**EHR Coordinator or Security Administrator**
c. **Conduct Training for New Users** 1. Organize and deliver in-person or virtual training sessions for new users. 2. Ensure each new user understands the organization's access control policy, emphasizing the least privileged principle.	
d. **Test Understanding Through Knowledge Check** 1. Develop a quiz or knowledge check at the end of the session to assess users' understanding of the access policy. 2. Include practical scenarios where users need to identify appropriate access rights.	
e. **Provide Access Policy Documentation** 1. Ensure all new users have access to the company's access control and least privilege policies. 2. Offer easy-to-understand guides for users to refer to when they need to request or change access permissions.	**EHR Coordinator or Security Administrator**
f. **Track Training Completion** 1. Use an internal system or tool to track which users have completed the training. 2. Ensure that access to sensitive systems is restricted until training is completed.	
g. **Feedback Collection and Review** 1. Ask for feedback from users regarding the clarity and effectiveness of the training. 2. Use feedback to improve future training sessions and materials.	**Security Administrator**
h. **Follow-up and Ongoing Education** 1. Schedule regular refresher courses or updates on changes to the access policy. 2. Ensure users stay informed about any policy changes or new security practices.	
i. Perform periodic access reviews and audits. **1. Access Management Group (AMG):** **a.** Will meet monthly to review changes made to the Access Control Log, including but not limited to: i. Identification of active users and their assigned permissions ii. Verification that users only have the access they need to perform their job functions	**Compliance Officer & Security Administrator**

iii. Verification that terminated or inactive users have had their access revoked iv. Evaluation of any role changes that might necessitate adjusting access levels. 2. **Report on Audits at Compliance & Policy Team (CPT)** a. Prepare and deliver a summary report on changes to the Compliance & Policy Team highlighting key findings, changes made, and any ongoing concerns. b. Ensure that any significant access control issues are escalated as needed.	
j. **Monitor and Address Compliance Gaps** 1. Follow up on any access issues that were identified during the audit. 2. Implement corrective actions to address any gaps or weaknesses in access control processes. 3. Report any unauthorized access attempts. 4. Revoke access immediately for employees who change roles or leave the organization.	**Security Administrator**
k. Notify Security Administrator of Role Changes or Departures 1. Utilize the Activation-Deactivation sheet issued by HR to be aware of an employee's role change or planned departure.	**Human Resources, Supervisors/ Directors**
l. Review Access Rights for Role Changes 1. For employees changing roles, the supervisor, director, and Access Management Group should review the employee's current access and identify any permissions that are no longer needed. 2. Promptly update access rights to align with the new role, ensuring that the principle of least privilege is maintained.	**Supervisor, Director, Access Management Group**
m. Revoke Access for Departing Employees 1. Immediately upon receiving notification of an employee's departure, the Security Administrator should begin the process of revoking access. 2. Ensure that access to all systems, applications, and network resources is revoked. 3. Disable user accounts and change shared passwords (if applicable) that the employee may have access to.	**Security Administrator**
n. **Update Internal Access Logs and Documentation** 1. After revoking access, update internal documentation to reflect the employee's access changes. 2. Maintain an audit trail of when and how access was revoked, including any devices or credentials returned or deactivated.	**EHR Coordinator or Security Administrator**
o. **Monitor Systems for Any Unauthorized Access Post-Departure**	**Security Administrator**

1. Monitor systems for any suspicious or unauthorized activities related to departing employees, including any failed login attempts or access attempts using old credentials. 2. Set up alerts for any attempts to access systems beyond the employee's revocation date. 3. Monitor and log access activities for compliance.	
p. **Monitor Access Logs** 1. Set up real-time alerts for suspicious or unauthorized access activities, such as: i. Multiple failed login attempts ii. Access outside of normal working hours iii. Unauthorized access to sensitive systems or data iv. Elevated privileges being used without proper justification 2. Ensure logs are continuously monitored for potential security incidents. 3. Audit Access Logs for Compliance i. Regularly audit access logs to ensure they align with internal policies and regulatory requirements. ii. Verify that users' access aligns with the principle of least privilege, ensuring no unauthorized permissions or excessive access exist.	**Security Administrator**
q. **Investigate and Respond to Anomalies** 1. When anomalies or unauthorized access attempts are detected, initiate an investigation to understand the scope and cause of the event. 2. Follow an established incident response plan to address potential security breaches or policy violations.	**Access Management Group (AMG)**
r. **Investigate and respond to security incidents.** 1. **Identify and Classify Security Incidents** i. Assess and classify security incidents based on severity (e.g., low, medium, high). ii. Categorize incidents based on type and potential impact on the organization. See ***Exhibit D: Incident Categorization***	**Security Administrator, CIO, and Compliance Officer**
s. Gather Incident Details and Logs 1. Immediately gather relevant access logs, system logs, and network traffic data associated with the incident. 2. Ensure logs are protected from tampering and properly stored for future analysis, following best practices for log integrity.	**Security Administrator**
t. Initiate the Investigation Process 1. Initiate an investigation by identifying the source of the	**Compliance Officer and CIO**

incident, including identifying affected systems, users, and data. 2. Work with the CIO to determine the scope of the breach or security violation, assessing which resources have been accessed or compromised.	
u. <u>Contain the Incident and Limit Further Damage</u> 1. If the incident is ongoing, take immediate action to contain the threat. This may involve: a) Temporarily disabling user accounts or permissions associated with the incident. b) Isolating affected systems or networks to prevent further unauthorized access or data loss. c) Changing passwords or revoking access tokens for compromised users. d) Work with the CIO to ensure that containment actions align with overall business continuity plans.	
v. <u>Communicate Incident Details to Relevant Stakeholders</u> 1. Notify the CIO, senior management, and any other relevant stakeholders (e.g., legal, compliance) about the incident, providing a clear summary of the situation. 2. Ensure communication is clear and includes information on the nature of the incident, its impact, and the steps being taken to mitigate damage.	**CIO|CQCO**
w. <u>Coordinate with Legal and Compliance Teams</u> 1. Collaborate with legal and compliance teams to determine whether the incident requires external reporting (e.g., data breach notification under GDPR or other regulations). 2. Ensure that all actions taken during the investigation comply with legal and regulatory requirements.	**CIO|CQCO**
x. <u>Conduct a Root Cause Analysis</u> 1. Perform a thorough root cause analysis to understand how the incident occurred. 2. Investigate whether the incident was caused by a specific access control failure, human error, or a flaw in system configuration. 3. Document findings and identify any weaknesses in the access control or security policies that need to be addressed.	**CIO|CQCO**
y. <u>Implement Immediate Remediation Actions</u> 1. Based on the findings, implement remediation measures to address the vulnerabilities that allowed the incident to occur. 2. This may involve: a) Updating or reconfiguring access controls. b) Applying patches or system updates. c) Reviewing and strengthening user access policies, including adjusting access permissions or roles.	**CIO|CQCO**

z. **Monitor for Further Suspicious Activity** 1. After remediation, closely monitor systems, networks, and user activities for any signs of continued suspicious behavior or attempts to exploit the same vulnerability. 2. Set up alerts or triggers in relevant systems to identify any new incidents early.	**Security Administrator**
aa. **Document Incident Response and Findings** 1. Document all actions taken during the incident investigation and response, including: a) Incident timeline, severity, and impact. b) Actions taken to contain and mitigate the incident. c) Systems and users affected, as well as root cause analysis. 2. Maintain an audit trail for future reference and compliance reporting.	**Security Administrator**
bb. Conduct a Post-Incident Review 1. Once the incident is fully resolved, conduct a post-incident review with relevant stakeholders (e.g., Security Administrator, CIO, Compliance Officer). 2. Review the effectiveness of the incident response process, identifying any gaps or areas for improvement in response time, communication, or technical measures.	**Access Management Group**
cc. **Update Policies and Procedures** 1. Based on lessons learned from the incident, update the access control and security policies to prevent similar incidents in the future. 2. Adjust the least privilege access policy, logging practices, or user training programs as necessary.	**CIO|CQCO**
dd. **Communicate Incident Resolution to Employees** 1. If the incident impacted employees or required them to change behavior (e.g., password resets, access changes), communicate the incident resolution clearly. 2. Provide any necessary guidance or updates on what actions employees need to take to ensure ongoing security.	**CIO|CQCO**
ee. **Report to Regulatory Authorities (If Applicable)** 1. If required by law or regulatory standards (e.g., GDPR, HIPAA), report the incident to the relevant authorities within the mandated time frame. 2. Provide all necessary documentation and cooperate with any required investigations or audits.	**CIO|CQCO**
ff. **Review and Improve Training Based on Incident** 1. Use the insights gained from the incident to improve employee training programs. 2. Update training materials to address any specific issues highlighted by the incident, such as improper access management or security practices.	**CIO|CQCO**

gg. **Business Associate Agreements/Subcontrator Contract Termination:** 1. Upon termination of a Business Associate relationship, confirm that all ePHI is either securely destroyed or returned to SCCMHA, and document completion of this process. 2. Retain terminated BAA documentation for a minimum of six years per §164.316(b)(2)(i).	**Contracts & Procurement CIO|CQCO**

<u>Exhibit A:</u> System Access for New Employees or Contractors Questionnaire

Role & Job Functions:

a. What is the employee's or contractor's job title and role within the organization?

b. What specific tasks will they need to perform that require system access?

c. Will they need access to electronic health records (EHR), financial systems, or other sensitive data?

d. Do they require read-only access, data entry access, or administrative privileges?

System & Application Access:

e. What specific systems, applications, or databases do they need access to?

f. Are there any existing user roles or templates that align with their access needs?

g. Do they need access to internal communication platforms, email, or scheduling tools?

Data Sensitivity & Security:

h. Will they be handling protected health information (PHI) or personally identifiable information (PII)?

i. Do they need access to confidential substance use disorder (SUD) data?

j. Are there any restrictions on the data they should *not* access?

Security Measures & Compliance:

k. Does this role require enhanced security measures?

l. Should their access be limited to certain locations (e.g., on-site only vs. remote access)?

m. What level of training do they need before access is granted?

Access Duration & Review:

n. Is this a permanent or temporary role? If temporary, when should access be revoked?

Exhibit B: Access Provisioning Checklist

Step 1: Validate Approved Access Request

☐ Confirm that the request has been reviewed and approved by required personnel (Department Head, Compliance Officer, Security Administrator, CIO).

☐ Verify that the requested access level aligns with role-based access control (RBAC) policies.

Step 2: Configure System Access

☐ Create or modify the user account in the required system(s) (EHR, billing, scheduling, internal platforms).

☐ Assign the appropriate access level (Read-only, Data Entry, Administrative).

☐ Implement **multi-factor authentication (MFA)** if required.

☐ Restrict access to sensitive data based on **least privilege principle**.

Step 3: Apply Security Controls

☐ Enforce password policies (complexity, expiration rules).

☐ Implement location-based restrictions (on-site vs. remote access).

☐ Restrict access to unnecessary applications or data categories.

☐ Log all access changes in the **Access Management System** for tracking and audits.

Step 4: Communicate Access Information

☐ Securely provide login credentials and access details.

☐ Share system usage guidelines and security policies.

☐ Ensure the employee completes required security and compliance training before first login.

Step 5: Document Access Provisioning

☐ Update the **Access Control Log** with:

- Employee/contractor name and role
- System(s) accessed
- Level of access granted
- Approval records
- Expiration/review date (if temporary)

☐ Maintain documentation for compliance audits.

Step 6: Conduct Post-Configuration Review

☐ Verify successful login and system functionality.

☐ Confirm user access is limited to authorized systems and data.

☐ Test MFA and other security measures to ensure proper enforcement.

☐ Confirm unauthorized applications or data remain inaccessible.

Exhibit C: Incident Categorization

i. **Unauthorized Access – Potential High Impact** (Violates HIPAA, patient trust loss, legal penalties, and reputational damage) **Potential Medium Impact** (Requires investigation, employee sanction, and reporting)
   1. **Internal User Unauthorized Access** – A staff member accesses a patient's record without a valid reason.
   2. **External Unauthorized Access** – An outsider gains access to patient records (e.g., hacker breach).
   3. **Family/Friends Unauthorized Access** – A non-authorized individual accesses a patient's data.

ii. **Privilege Escalation - Potential High Impact** (Full system compromise, unauthorized data modification, regulatory violations) **Potential Medium Impact** (System integrity issues, audit failures, potential HIPAA violations)
   1. **Insider Threat –** An employee exploits a system flaw to gain elevated EMR access.
   2. **Misconfigured User Roles –** A front desk staff accidentally granted psychiatrist-level access.
   3. **Third-Party System Compromise –** A vendor with limited access exploits a vulnerability to gain admin control.

iii. **Data Exfiltration (Data Theft or Leakage) - Potential High Impact** (HIPAA breach, loss of patient confidentiality, regulatory fines, lawsuits) **Potential Medium Impact** (Partial data exposure requires disclosure and patient notification)
   1. **Malicious Insider Theft –** A disgruntled employee exports patient data for personal gain.
   2. **Phishing Attack –** An attacker gains EMR access through a phishing email and extracts data.
   3. **API Misuse –** A poorly secured API allows unauthorized bulk data extraction.

iv. **Ransomware & Malware Attacks - Potential High Impact** (Service downtime, financial loss, HIPAA penalties, patient safety risks) **Potential Medium Impact** (System recovery costs, potential temporary data loss)
   1. **Ransomware Infection –** Encrypts EMR data, making it inaccessible until ransom is paid.
   2. **Trojan/Spyware Attack –** Malicious software captures login credentials and patient data.
   3. **Worm or Virus Spread –** Infects multiple workstations, causing downtime.

v. **System Misconfigurations & Human Errors - Potential Medium Impact** (Regulatory compliance issue, requires breach notification.) **Potential Low Impact** (Correctable through security patches and audits.)
   1. **Incorrect Role Assignments –** Staff accidentally given too much access.
   2. **Accidental Patient Data Exposure –** Wrong patient file sent to another provider or emailed insecurely.
   3. **Open Database or Unsecured Cloud Storage –** EMR records exposed due to improper security settings.

vi. **Insider Threats & Employee Misuse - Potential High Impact** (Direct HIPAA violation, possible termination and legal actions.) **Potential Medium Impact** (HR investigation, disciplinary action required.)

1. **Curious Employee Browsing –** Staff accesses celebrity or personal acquaintance records without permission.
2. **Data Manipulation –** Altering patient notes or prescriptions without authorization.
3. **Printing or Copying Sensitive Data –** Downloading records onto USB or personal devices.

vii. **Third-Party & Vendor Security Breaches – Potential High Impact** (Large-scale patient data breach, lawsuits, regulatory actions.) **Potential Medium Impact** (Partial compromise, requiring extensive security review.)

1. **EHR Vendor Compromise –** Cloud-based EMR provider suffers a breach.
2. **Billing or Telehealth Vendor Hack –** Third-party billing or telehealth system exposes patient data.
3. **Supply Chain Attack –** Malicious code introduced via a vendor software update.

viii. **Denial-of-Service (DoS) & System Disruptions - Potential High Impact** (Full EMR compromise, patient data theft, HIPAA fines.) **Potential Medium Impact** (Partial account compromise, requiring password resets.)

1. **DDoS Attack –** Attackers flood the network, making the EMR system unavailable.
2. **Hardware or Network Failure –** Data center outage affects EMR availability.
3. **Cloud Service Downtime –** The EMR provider experiences downtime, halting patient care.

ix. **Social Engineering & Credential Theft - Potential High Impact** (Patient care delays, financial loss, emergency cases at risk.) **Potential Medium Impact** (Temporary system outages, requiring backup activation.)

1. **Phishing Emails –** Employees tricked into revealing login credentials.
2. **Pretexting or Impersonation –** Attacker pretends to be IT support to gain access.
3. **Weak Password Exploits –** Default or easy passwords used to access EMR.

x. **Physical Security Incidents - Potential High Impact** (Large-scale data exposure, regulatory violations.) **Potential Medium Impact** (Localized breach, requiring policy updates and training.)

1. **Stolen Devices –** Laptops or tablets with unencrypted patient data are lost.
2. **Unauthorized Facility Access –** An intruder gains physical access to EMR workstations.
3. **Improper Document Disposal –** Printed patient records discarded without shredding.

Exhibit D: Sample Access Control Log

Date of Access Change	System, Application, or Database Access Requested - (i.e. Sentri or Microsoft)	Last Name, First Name	Email Address	Employment Status (full-time, part-time, temporary, intern, contractor)	Organization (SCCMHA or Name of Network Provider affiliate)	Start Date	Termination Date	Department	Job Title	Access Type (read-only, data entry, administrative, full edit access)	Access Level Granted	Justification for Access requested above PoLP	Training Completed?	MFA Enrollment Completed?	Supervisor or Director Approval Acquired?	AMG Review Completed?	High-Level Access Approval by CIO (if applicable)	Approve or Denied Access Control Request
3/1/2025	*Sentri*	*Doe, Jane*	*jane.doe@sccmha.org*	*Full-Time*	*SCCMHA*	*3/5/2025*		*Support Coordination Services (SCS 1) - IDD*	*Support Coordinator - IDD (SCS 1)*	*Data Entry*	*Primary Case Holder, MichiCANS Read/Write, SCCMHA and Primary Teams, Saginaw Clinician, Two Factor Mandatory*		*X*	*X*	*K. Feltman*			

Exhibit E: Sample Business Associate Agreement (BAA) Clauses

The following language may be included or referenced in SCCMHA's Business Associate Agreements to ensure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

- **Purpose:** This Agreement establishes the responsibilities of the Business Associate ("BA") to appropriately safeguard Protected Health Information ("PHI") and Electronic Protected Health Information ("ePHI") received, maintained, or transmitted on behalf of SCCMHA ("Covered Entity").
- **Permitted Uses and Disclosures**
  - The Business Associate may use or disclose PHI only:
    - To perform services as described in the main contract or scope of work.
    - As required by law; and
    - As permitted by the HIPAA Privacy and Security Rules, limited to the minimum necessary amount of PHI.
- **Safeguards**
  - The Business Associate must:
    - Implement administrative, physical, and technical safeguards that meet or exceed those required by 45 CFR §164.308, §164.310, and §164.312.
    - Restrict access to PHI to only those personnel who require it to perform duties under this Agreement.
    - Encrypt all ePHI in transit and rest using current industry standards (NIST FIPS 140-2 validated encryption).
    - Report any security incident or unauthorized use/disclosure of PHI to SCCMHA within five (5) business days of discovery.
- **Subcontractors**
  - If the Business Associate uses a subcontractor that creates, receives, maintains, or transmits PHI, the Business Associate must:
    - Obtain written satisfactory assurances (via BAA) that the subcontractor will comply with the same restrictions and conditions required of the Business Associate.
    - Provide documentation of subcontractor compliance to SCCMHA upon request.
- **Breach Notification**
  - In the event of a breach of unsecured PHI:
    - The Business Associate shall notify SCCMHA's Privacy Officer without unreasonable delay, and no later than **five (5) calendar days** after discovery.
    - Notification must include the nature of the breach, the types of PHI involved, the number of affected individuals, and mitigation steps taken.
    - The Business Associate shall cooperate fully with SCCMHA during investigation and remediation.
- **Data Retention and Destruction**
  - Upon termination of the Agreement:
    - The Business Associate must return or securely destroy all PHI and ePHI received from SCCMHA.

    - If destruction is not feasible, the Business Associate must explain the reason in writing and continue to safeguard the information under this Agreement's terms.
    - Retention for audit or legal purposes must comply with SCCMHA's record retention schedule and HIPAA §164.530(j).
- **Indemnification**
    - The Business Associate agrees to indemnify and hold harmless SCCMHA from any loss, cost, damage, or liability resulting from its breach of this Agreement or violation of HIPAA regulations.
- **Termination**
    - SCCMHA may terminate this Agreement immediately if it determines that the Business Associate has violated a material term. SCCMHA shall provide written notice specifying the violation and effective termination date.
- **Governing Law**
    - This Agreement shall be governed by and construed in accordance with the laws of the **State of Michigan** and applicable federal law.

Exhibit F: Business Associate Agreement Inventory Log Template

Business Associate Name	Contact Person	Department / Contract Owner	Purpose / Services Provided	Access Type (PHI/ePHI)	Date Executed	Renewal / Expiration Date	Last Review Date	Compliance Verification Date	Subcontractors Identified	Notes / Follow-Up
Example: HealthData Analytics	John Doe	Information Systems	Data analysis using PHI extracts	ePHI (read-only)	1/15/2024	1/15/2027	7/1/2025	7/1/2025	None	BAA renewed; encryption verified

Maintenance Responsibility:
The Compliance & Policy Team, in coordination with the Chief Information Officer, will maintain and review this log quarterly.

Exhibit G: Annual BAA Review Checklist

Purpose: To ensure that all Business Associate Agreements remain compliant with HIPAA requirements and organizational expectations.

Review Item	Requirement / Verification	Status (Y/N)	Notes / Action Items
1. BAA is active and signed by both parties	Verify document signatures and effective dates		
2. Agreement includes breach notification clause (≤5 days reporting)	45 CFR §164.410		
3. Agreement includes minimum necessary and data security safeguards	45 CFR §164.502(b), §164.308		
4. Agreement includes subcontractor flow-down requirement	45 CFR §164.314(a)(1)		
5. Agreement includes termination and data destruction terms	45 CFR §164.504(e)(2)(J)		
6. Encryption, access controls, and audit logging are documented	NIST SP 800-66r2 §4.1		
7. Security incident cooperation clause present	Strongly recommended (OCR 2023 guidance)		
8. Indemnification and governing law specified	Organizational standard		
9. Business Associate's most recent security assessment or attestation on file	SOC 2, HITRUST, or internal audit accepted		
10. Subcontractor list reviewed and up to date	45 CFR §164.314(a)(2)		

Reviewer: _____
Date of Review: _____
Next Scheduled Review: _____

Exhibit H: Business Associate Risk Assessment Template

Purpose: To evaluate the potential risks and vulnerabilities associated with granting a Business Associate access to PHI or ePHI.

Category	Assessment Question	Risk Level (Low/Med/High)	Mitigation or Control	Responsible Party
Data Sensitivity	What types of PHI/ePHI will the BA access (e.g., demographics, diagnoses, medications)?			
Data Volume	How much PHI will be shared or stored?			
System Access	Will the BA have remote, on-site, or API access to SCCMHA systems?			
Security Posture	Does the BA have documented security policies consistent with NIST and HIPAA standards?			
Encryption Controls	Is ePHI encrypted in transit and at rest using FIPS 140-2 or equivalent?			
Incident Response	Does the BA have a documented incident response plan?			
Subcontractors	Will the BA use subcontractors to process PHI? If yes, are they covered by BAAs?			
Retention & Disposal	How will ePHI be securely destroyed or returned at the end of engagement?			
Compliance History	Has the BA had prior security incidents or OCR enforcement actions?			
Insurance Coverage	Does the BA carry cyber liability or data breach insurance?			

Assessment Completed By: _____

Department: _____

Date: _____

Review Frequency: Annual or upon contract renewal

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: Guest User Access Policy</td><td>Chapter: Chapter section of SCCMHA policy & procedure manual - number & name</td><td>Subject No: 08.06.12.07</td></tr>
<tr><td rowspan="2">Effective Date:
10.13.2025</td><td>Date of Review/Revision:</td><td rowspan="2">Approved By:
Sandra M. Lindsey, CEO</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td><td>Responsible Director:
Chief Information Officer, Chief Quality & Compliance Officer

Authored By:
Christina Saunders, Administrative Assistant to CIO|CQCO

Additional Reviewers:
Chris Hermanns, Manager of Information Technology</td></tr>
</table>

Purpose:
To define a standardized and secure method for onboarding, managing, and auditing guest users in Microsoft Azure and Microsoft Teams, ensuring adherence to least privilege principles and regulatory compliance.

Application:
This policy applies to all employees, network providers, contractors, and third-party collaborators who request or sponsor external (guest) access to SCCMHA's Microsoft 365 environment, including Teams, SharePoint, OneDrive, and other integrated apps.

Policy:
This policy governs the onboarding, access control, and lifecycle management of guest users within the organization's Microsoft Azure and Microsoft 365 environments. The primary objective is to ensure that external collaborators (e.g., vendors, partners, contractors, network providers) are granted access only to the resources necessary for their roles, in alignment with security, compliance, and auditing standards.

This process should be utilized for any external collaborators that do not require a SCCMHA network connected device. Guest Access will provide users with access to Teams meetings, shared reports, collaborative documentation, and communications via Microsoft Teams.

Standards:

A. Guest Invitation & Onboarding

a. **Controlled Onboarding**: All guest accounts must be requested via the Helpdesk Ticket Portal under the External Provider Support tab, "External Provider Microsoft Guest User Access Request."
b. Guest User will receive an email notification of being added to Team/Channel sent by Microsoft. This email will provide instructions on how to set up or log into Microsoft account for the email address provided to SCCMHA for guest account.
c. Guests will have access to instructional documentation on Teams to help navigate the different utilization of their guest account.

B. Access Scope

a. Guests must be assigned to predefined security or Microsoft 365 groups that correspond to specific access roles and resources (e.g., Teams, SharePoint sites). Guest Accounts can access:
    i. Access to Teams and Channels assigned
    ii. Microsoft Teams meetings via invitations
    iii. Office Online (web version only, no desktop apps)
    iv. SharePoint Online (access to files/collaboration sites
b. No guest should receive access beyond their scope of work.

C. Least Privilege Enforcement

a. Guest access is restricted to the minimum level necessary for collaboration.

D. Lifecycle Management

a. All guest access must have defined expiration dates and undergo regular access reviews to validate continued need.
b. Access Reviews must be conducted regularly via Azure AD for all guest groups.
c. Default access expiration of 30-90 days must be set for all guest accounts.
d. Expired or inactive accounts will be automatically disabled and reviewed for deletion.

E. Auditing/Monitoring

a. All guest activity is logged and monitored via Azure AD sign-in and audit logs, with alerting configured for suspicious or anomalous behavior.
b. IT Security will review access patterns and exceptions monthly.
c. Any unauthorized guest access will be escalated and reported by incident response procedures.

F. **Responsibilities**

a. IT Security/Access & Identity Management Team – Enforce policies, monitor logs, manage access packages, perform reviews.
b. Team Owners – Sponsor and justify guest accounts, participate in access reviews.
c. Employees/Requestors – Submit guest requests via the Helpdesk Ticket Portal, to ensure legitimate business need.

G. **Exceptions**

a. All exceptions must be documented and approved by the CIO with time-bound justifications.

Definitions:

- **Guest User:** An external user (non-employee) invited to collaborate with Microsoft 365.
- **Access Package:** A bundle of resources and permissions provisioned through Azure.
- **Conditional Access:** A set of policies that apply security requirements based on context (user, device, location).
- **Least Privilege:** Providing only the access necessary for a user to perform their tasks.

References:

1. Microsoft Azure AD B2B Documentation
2. NIST 800-53 Access Control Guidelines
3. Microsoft 365 Compliance Center
4. SCCMHA Knowledge Base Articles – Microsoft Support

Exhibits:

A. Guest Account Access Request Required Fields & Descriptions

Procedure:

ACTION	RESPONSIBILITY
1. Helpdesk Ticket entered for Guest User Access with required fields (see Exhibit A for complete list).	1. Sponsor Department
2. Users will be added to the Team and channels noted within the Helpdesk ticket.	2. Microsoft Teams Administrator
3. If new Team or Channel needs to be created for external user collaboration, one will be created.	3. Microsoft Teams Administrator
4. Guest User will receive an email notification of being added to Team/Channel sent by Microsoft.	4. Guest User
5. Guest will see the Team and all files/folders in their agency's shared channel. The user will be able to add, modify and delete files/folders.	5. Guest User
6. Modifications to guest user accounts can be requested via the Helpdesk Ticket portal – including additional access, revocation of access, and individual role changes.	6. Guest User

7. Regular audits will be conducted to ensure Least Privilege Principle and Role Based Security policies are being followed.	7. Access & Identity Management Team/ Network Services Department/ Network Providers

EXHIBIT A: Guest Account Access Request Required Fields & Descriptions

This form should only be used for individuals who need access to Microsoft Teams but DO NOT need an SCCMHA device.

1. **Requestor Name & Department** – individual who is sponsoring the guest and what team they belong to
2. **Guest Full Name** – Legal name for external user
3. **Guest Email address** – Business email used for Azure B2B invitation
4. **Guest Organization Name** – external organization or agency the guest user works for
5. **Reason for Access** – A brief description of why the guest needs access (project name, task, Power BI access, etc.)
6. **Resources Requested** – Teams, SharePoint, apps, documents the guest will access, etc.
7. **Level of Access Required** – Read-only, edit, contributor, or specific Azure role (if applicable)
8. **Access Start Date** – when access should be granted
9. **Access End Date** – when access should be revoked (default 90 days unless specified)
10. **Sensitivity of Data Accessed** – Whether guest access will be sensitive, confidential, or regulated data
11. **Manager or Director Approval** – signoff required by set individuals for ticket routing (example CIO|CQCO)

Policy and Procedure Manual Saginaw County Community Mental Health Authority		
Subject: HIPAA Security: Policies, Procedures, and Documentation	**Chapter**: 08 – Management of Information	**Subject No**: 08.06.16.01
Effective Date: October 01, 2020	**Date of Review/Revision**: 9/20/22, 6/28/23, 9/9/24, 11/12/25 **Supersedes**:	**Approved By**: Sandra M. Lindsey, CEO
		**Responsible Director:** AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer & HIPAA Security Officer **Authored By**: AmyLou Douglas, Chief Information Officer | Chief Quality and Compliance Officer & HIPAA Security Officer **Additional Reviewers**: Jennifer Keilitz, Director of Network Services, Public Policy, and Continuing Ed and Kentera Patterson, Officer of Recipient Rights and Compliance & Privacy Officer

Purpose:
To ensure compliance with the HIPAA Security Rule, §164.316 – Policies and Procedures and Documentation Requirements, by establishing comprehensive policies and procedures for maintaining, reviewing, and managing documentation related to electronic protected health information (ePHI) and security practices. This policy also ensures alignment with the HIPAA 2024 Final Rule and proposed 2025 Cybersecurity Enhancements, including strengthened safeguards for third-party access, employee awareness, and cybersecurity incident preparedness consistent with §164.308 and §164.316.

Policy:

SCCMHA will implement and maintain policies and procedures to comply with the HIPAA Security Rule. All actions, activities, and assessments required by the HIPAA Security Rule will be documented in written form (which may be electronic), and these records will be maintained according to the established standards. SCCMHA will document evidence of employee training, phishing simulation, and awareness activities conducted through platforms such as **KnowBe4**, as part of its ongoing security and compliance monitoring program. Documentation will also include the results of periodic evaluations of technical and administrative safeguards.

Application:
The HIPAA Security Rule, and this Policy, applies to SCCMHA, its business associates, and any subcontractor that are required to access or use PHI to complete its contracted duties. Business Associates and subcontractors may elect to adopt and comply with the relevant SCCMHA Policy or develop their own Policies and Procedures which comply with the applicable section of the HIPAA Security Rule.
Designated individuals or teams responsible for managing documentation, conducting reviews, and implementing updates to ensure accountability and adherence to this policy. Business Associates and subcontractors must also maintain auditable documentation of their own security training, incident response readiness, and any subcontracted vendor management processes that involve SCCMHA's ePHI. Documentation of these assurances must be retained by SCCMHA for monitoring and compliance review.

Standards:
1. Documentation and Assurance for Business Associates:
    - Business Associate Agreements: Before permitting a Business Associate to create, receive, maintain, or transmit EPHI on behalf of SCCMHA, satisfactory assurances must be obtained that the business associate will appropriately safeguard the information. This assurance is formalized through Business Associate Agreements (BAAs) that specify security and privacy obligations, in accordance with the HIPAA Security Rule and according to Policy 08.06.08.09: HIPAA Security – BAAs and Other Arrangements.
    - Document Retention: Any documentation related to BAAs and assurances must be retained for 6 years from the date of creation or from the date when the document was last was in effect, whichever is later.
    - Security Review Documentation: Maintain records of periodic reviews and risk analysis of business associate security controls, including verification of incident response procedures and breach notification readiness.
2. Availability of Documentation:
    - Accessibility: documentation will be made readily available to personnel responsible for implementing and enforcing the applicable policy or procedures. This includes making sure that all relevant staff have access to the documents necessary for their roles.
    - Access Control: Documentation repositories (electronic or physical) must be access-restricted based on least privilege and monitored via audit logs.
3. Periodic Review & Updates:

- Regular Reviews: The documentation will be reviewed periodically, and updated as needed, to ensure its continued effectiveness and relevance. This includes assessing the adequacy of documentation considering environmental or operational changes that may impact the security of electronic protected health information.
- Security Event Documentation: Results of vulnerability scans, phishing tests, and any KnowBe4 campaign summaries must be documented and retained as part of the security evaluation record.
- Updates & Revisions: Documentation will be updated as needed to reflect changes in regulations, organizational practices, and results of security assessments. Changes will be documented, and previous versions will be archived according to retention policies.

4. Documentation of Actions & Assessments:
    - Record Maintenance: Maintain comprehensive records of all actions, activities, and assessments related to the implementation and enforcement of security policies. This includes risk assessments, security evaluations, training records, and incident response activities.
    - Audit Trail: Ensure that an audit trail is maintained for all significant actions, changes, and updates to policies and procedures. This includes documenting who made changes, the nature of the changes, and the rationale for such changes.
    - Incident Documentation: Maintain detailed incident response documentation including time of discovery, containment, mitigation, and notification steps.
    - Breach Documentation: Include law enforcement delay requests, breach determinations, and notices as required by §164.414(b).
    - Compliance Monitoring: Regular audits will be conducted to ensure compliance with the policies and procedures. Non-compliance will be addressed through corrective actions and disciplinary measures as appropriate.
5. Documentation Storage and Security:
    - Secure Storage: All documentation, including electronic records, will be stored securely to protect against unauthorized access, alteration, or destruction. Access to documentation will be conducted based on roles and responsibilities.
    - Backup and Recovery: Maintain secure, encrypted backups of all documentation, with tested recovery procedures, to ensure continuity and integrity.

Responsibilities:

- **HIPAA Privacy & HIPAA Security Officers:** Oversees the implementation and enforcement of this policy, including ensuring that documentation is maintained and reviewed in accordance with HIPAA requirements.
- **IT Department:** Responsible for secure storage and management of electronic documentation and for implementing technical controls to protect electronic records.

- NOT SURE WHO IT WOULD BE: Oversees implementation and documentation of ongoing workforce security training, phishing simulations, and awareness campaigns.
- **Management:** Ensures that all staff are aware of and comply with the documentation requirements and participate in periodic reviews and updates.
- **All Employees:** Responsible for adhering to the policies and procedures outlined, participating in training, and reporting any issues related to documentation or policy compliance.

Definitions:
See I.T./I.S. Policy **08.06.00.01** which contains a comprehensive list of relevant words and terms used within the Policies of this section.

References:

-
- 45 CFR §164.308, §164.312, §164.316
- HHS OCR HIPAA 2024 Final Rule (89 FR 30852, April 2024)
- NIST SP 800-66 Rev.2, *Implementing the HIPAA Security Rule* (2024)
- 42 CFR Part 2 (2024 updates)
- HHS Proposed Rule: *HIPAA Security Rule Enhancements and Cybersecurity Requirements* (expected 2025)
-

Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
Create and Deploy Policies and Procedures	
1. Implement reasonable and appropriate procedures to comply with the HIPAA Security Rule.	HIPAA Security Officer & HIPAA Privacy Officer
2. Periodically evaluate written policies and procedures to verify that: a) Policies and procedures are sufficient to address the standards, implementation specifications, and other requirements of the HIPAA Security Rule.	HIPAA Security Officer & HIPAA Privacy Officer

b) Policies and procedures accurately reflect the actual activities and practices exhibited by SCCMHA, its workforce, its systems, and its business associates. c) Documentation includes workforce cybersecurity awareness activities, KnowBe4 training completion reports, and periodic phishing assessments.	
Update Documentation of Policy and Procedures 3. Change policies and procedures as is reasonable and appropriate, at any time, provided that the changes are documented and implemented in accordance with the requirements of the HIPAA Security Rule.	HIPAA Security Officer & HIPAA Privacy Officer
Draft, maintain and Update Required Documentation 4. Written documentation may be incorporated into existing manuals, policies, and other documents, or may be created specifically for the purpose of demonstrating compliance with the HIPAA Security Rule. All documentation systems must ensure version control, date/time stamping, and restricted access in compliance with SCCMHA's records management and retention schedule.	HIPAA Security Officer & HIPAA Privacy Officer
Retain Documentation for at Least Six Years 5. Retain required documentation of policies, procedures, actions,	HIPAA Security Officer & HIPAA Privacy Officer Director of Network Services, Public Policy

activities, or assessments required by the HIPAA Security Rule for six years from the date of its creation or the date when it last was in effect, whichever is later.	
Assure that Documentation is Available to those Responsible for Implementation 6. Make documentation available to those people by implementing the procedures to which the documentation pertains.	HIPAA Security Officer & HIPAA Privacy Officer Director of Network Services, Public Policy
Update Documentation as Required 7. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI. The Security Officer will also review training and incident documentation to identify trends, recurring risks, or compliance gaps and include these findings in the annual Security Risk Assessment report.	HIPAA Security Officer & HIPAA Privacy Officer

<table>
<tr><td colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: HIPAA Security - Data Backup and Storage</td><td>Chapter: 08 - Management of Information</td><td>Subject No: 08.06.40</td></tr>
<tr><td rowspan="2">Effective Date:
June 7, 2004</td><td>Date of Review/Revision:
3/25/04, 7/11/07, 9/12/17, 11/14/18, 9/14/22, 8/4/23, 9/9/24, 11/12/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Amy Lou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Authored By:
Amy Lou Douglas, Chief Information Officer | Chief Quality and Compliance Officer

Additional Reviewers:
Matthew Devos - Senior Network & Information Security Administrator,
Benjamin Pelkki Senior Database & Microsoft 365 Administrator
David Wolfcale, Systems, Information Security & Microsoft 365 Administrator
Brett Lyon – Senior Applications, Information Security & BI Administrator</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:

To ensure that SCCMHA's data on its information systems and electronic media is backed up regularly, securely stored, and recoverable, thereby supporting data integrity and availability in alignment with industry standards and compliance requirement.

This policy also supports compliance with 45 CFR §164.308(a)(7) – Contingency Plan and aligns with the 2023–2025 HHS Cybersecurity Performance Goals emphasizing resilient data recovery capabilities. It applies to all systems containing Electronic Protected Health Information (ePHI), including behavioral-health-specific systems subject to 42 CFR Part 2 confidentiality requirements.

Policy:
All data on SCCMHA's information systems and electronic media must be regularly backed up, securely stored, and tested for restoration. This policy ensures data protection against loss, damage, and unauthorized access through comprehensive backup and recovery procedures. SCCMHA will maintain documented evidence of all backups, restoration, and verification activities for at least six (6) years, as required under §164.316(b)(2)(i). All contingency operations shall ensure data availability while preventing unauthorized access during emergency mode operations (§164.308(a)(7)(ii)(C)).

Application:
This policy applies to all data residing on SCCMHA-owned components of the Management Information System, including data stored on servers, workstations, and other electronic media. It excludes SCCMHA data located offsite which has been entrusted to a third party via a contractual agreement but includes oversight and coordination with such third parties where applicable.
When SCCMHA data is hosted or backed up by third-party or cloud providers, Business Associate Agreements (BAAs) must specifically address backup frequency, encryption, data-residency, incident response, and recovery time objectives. SCCMHA will periodically verify that the provider's controls meet or exceed HIPAA and HHS Cybersecurity Performance Goals (§164.314(a)).

Standards:
1. Backup Frequency & Scope:

    - Daily Backup: Backup copies of all data on SCCMHA electronic media and information systems must be made each business day. This includes both data received by SCCMHA and data created within SCCMHA.

    - Comprehensive Coverage: Backups must cover all data across SCCMHA's servers, workstations, and other relevant information systems, ensuring no critical data is excluded.

    - Backups must include system configuration data and audit logs necessary to reconstruct security events or incidents.

2. Backup Systems & Testing:

    - Adequate Backup Systems: SCCMHA must have adequate backup systems that ensure that all data can be recovered following a disaster or media failure. These systems must be evaluated and regularly tested to ensure their effectiveness.

    - Testing Schedule: Backup and restoration procedures must be tested at least semi-annually. Tests should simulate actual disaster scenarios and recovery processes to validate system reliability and performance.

- Testing Results: Results of all restoration tests will be documented and reviewed by the HIPAA Security Officer and CIO. Any identified deficiencies will be tracked through corrective-action plans.

- Restoration of ePHI integrity: Testing will also verify restoration of ePHI integrity (e.g., checksums or hash validation) to confirm that no unauthorized modification occurred.

3. Storage and Security of Backup Data:

    - Secure Remote Storage: Backup of data on SCCMHA information systems and electronic media, together with accurate and complete records of the backup copies and documented restoration procedures, must be stored in a secure remote location, at a sufficient distance from SCCMHA facilities to escape damage from a disaster at SCCMHA. (*See SCCMHA I.S. Departmental procedures 09.07.01.05 – Backup procedure, 09.07.01.10 – Restore Procedure and SCCMHA's DRP plan for full server restore procedure*).

    - Physical & Environmental Protections: The backup media containing SCCMHA's data at the remote backup storage site must be given an appropriate level of physical and environmental protection consistent with the standards applied to data physically at SCCMHA.

    - Encryption: All backup media, whether physical or cloud-based, must be encrypted using FIPS 140-2 or higher validated cryptographic modules. Encryption keys must be stored in a separate secure management system with role-based access control.

    - Quarterly Review: Access logs for backup repositories must be retained and reviewed quarterly for unauthorized attempts or anomalies.

4. Access & Retrieval: Backup copies of data stored at secure remote locations must be accessible to authorized SCCMHA employees or delegated contractors for timely retrieval of the information. Retrieval procedures must include verification of requester identity and authorization prior to restoration or data release, consistent with the minimum necessary principle (§164.514(d)).

5. Data Encryption Standards: Backup data must be encrypted both in transit and at rest to protect against unauthorized access and data breaches. Encryption keys must be managed securely and separately from the encrypted data. Encryption key rotation and lifecycle management must follow NIST SP 800-57 guidance, and all key access or use must be logged.

6. Retention and Archival:
    - Retention Period: The retention period for backup of Electronic Protected Health Information (EPHI) on SCCMHA information systems and electronic

media and any requirements for archive copies to be permanently retained must be defined and documented.

- Archival Requirements: Specify any requirements for archive copies that need to be permanently retained. Documentation of archival procedures should detail the process for managing long-term data storage. Archival backups containing ePHI must be reviewed periodically to determine ongoing business or legal necessity. When no longer required, secure destruction must follow NIST SP 800-88 Rev 1 sanitization standards.

7. Cloud-Based Backups:
    - Integrations: In addition to all prem backups, the servers must also be backed up to a cloud-based service. Ensure that the cloud backup solution meets SCCMHA's security and compliance standards.
    - Management: Regularly review and update cloud backup configurations and contracts to ensure they align with SCCMHA's backup policies and security requirements.
    - Cloud backup solutions must provide audit logs, encryption at rest/in transit, data-location transparency, and support for SCCMHA's recovery-time objectives (RTO) and recovery-point objectives (RPO).
    - SCCMHA will document annual reviews of cloud vendor SOC 2 or equivalent security reports.
8. Accountability and Documentation:
    - Documentation and Reporting**:** The IT Department will maintain a centralized Backup and Recovery Log documenting schedules, locations, test results, encryption verification, and responsible personnel. The HIPAA Security Officer will review this log quarterly.

Responsibilities:

- **IT Department:** Implements, monitors, and tests backup systems; documents backup and restoration activities; maintain encryption and access logs; and coordinates offsite or cloud storage arrangements.
- **HIPAA Security Officer/Chief Information Officer (CIO):** Oversees compliance with this policy, reviews test results, and approves corrective-action plans.
- **Department Supervisors and Directors:** Ensure critical data within their programs is properly designated for inclusion in scheduled backups.
- **All Employees:** Must store agency data on approved systems subject to backup and avoid saving PHI to unencrypted or non-network drives.

Definitions:

See I.T./I.S. Policy **08.06.00.01** which contains a comprehensive list of relevant words and terms used within the Policies of this section.

References:

45 CFR §164.308(a)(7) – Contingency Plan
45 CFR §164.310(d)(2) – Device and Media Controls
45 CFR §164.316(b)(2)(i) – Documentation Retention
42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
HHS Cybersecurity Performance Goals (2023)
NIST SP 800-34 Rev 1 – Contingency Planning Guide
NIST SP 800-88 Rev 1 – Media Sanitization
NIST SP 800-57 – Key Management

Exhibits:
None

Procedure:
None

Tab 7

Claims Processing

<table>
<tr><th colspan="3">Policy and Procedure Manual
Saginaw County Community Mental Health Authority</th></tr>
<tr><td>Subject:
Financial Liability for Mental Health Services</td><td>Chapter: 05 - Organizational Management</td><td>Subject No: 05.02.06</td></tr>
<tr><td rowspan="2">Effective Date:
October 1, 2002</td><td>Date of Review/Revision:
9/30/02, 6/1/07, 6/2/14, 8/3/16, 7/31/17, 5/2/18, 2/12/19, 1/1/20, 12/31/20, 1/10/22, 1/10/23,11/1/24, 11/1/25</td><td rowspan="3">Approved By:
Sandra M. Lindsey, CEO

Responsible Director:
Chief Financial Officer

Authored By:
Chief Financial Officer

Additional Reviewers:
Finance Manager</td></tr>
<tr><td>Supersedes:</td></tr>
<tr><td colspan="2">SAGINAW COUNTY COMMUNITY MENTAL HEALTH AUTHORITY</td></tr>
</table>

Purpose:
In order to ensure that when a person served is covered, in part or in whole, under any type of insurance coverage, private or public, for services provided directly or by contract with SCCMHA, the benefits from that insurance coverage(s) is considered to be available to pay the consumer's financial liability, in addition to the person served calculated ability to pay, notwithstanding that the insurance contract was entered into by a person other than the consumer or that the insurance coverage was paid for by a person other than the person served. Additionally, the insurance coverage is considered available to pay for the person served financial liability for services provided by SCCMHA or its contracted providers in the amount and to the same extent that coverage would be available to cover the cost of services if the person served had received the services from a health care provider other than SCCMHA or it's contracted providers.

Application:
All the following functions within the SCCMHA Provider Network, but not limited to:

- Customer Service Department
- Finance Department
- Care Management Department
- Network Services Department
- Network Services Providers
- All SCCMHA staff

Policy:

It is the policy of SCCMHA to properly bill all responsible parties who are financially liable for the cost of services provided to a person served either directly or by contract with SCCMHA, and to coordinate the benefits related to the services received.

Standards:
When a responsible party is financially liable for the cost of services provided to the consumer directly by or by contract with SCCMHA:

1. SCCMHA shall charge responsible parties for that portion of the financial liability that is not met by insurance coverage. The amount of the charge shall be the least of the following:
    a. Ability to pay (ATP) determined rules and guidelines of the Mental Health Code
    b. Cost of Services as defined in Section 800 of the Mental Health Code.
    c. The amount of coinsurance and deductible in accordance with the terms of participation with a payer or payer group.

2. SCCMHA shall waive payment of that part of a charge determined to exceed financial liability, and shall not impose charges in excess of ability to pay.

3. If the consumer is single, insurance coverage and ATP shall first be determined for the consumer. If the person served is an unmarried minor and the consumer's insurance coverage and ATP are less than the cost of the services, insurance coverage and the ATP shall be determined for the parents. If the person served is married, insurance coverage and ATP shall be determined jointly for the person served and the spouse.

4. The total combined financial liability of the responsible parties shall not exceed the cost of the services.

5. A person served shall not be denied properly approved and eligible services because of the inability of responsible parties to pay for the services.

6. If a responsible party willfully fails to apply to have insurance benefits that cover the cost of services provided to the person served, the responsible party's ATP shall be determined to include the amount of insurance benefits that would be available. If the amount of insurance benefits is not known, the responsible party's ATP shall be determined to be the full cost of services.

7. Willful failure to provide the relevant financial information by a responsible party may result in a determination of ATP up to the full cost of services received by a person served.

8. Person(s) served who receive services will receive a determination of the responsible parties' insurance coverage and ATP as soon as practical after the start of services.

9. No determination of ATP made by SCCMHA shall impose an undue financial burden for the person served or person served family members.

10. SCCMHA shall annually determine the insurance coverage and ATP of each person served who continues to receive services and of each additional responsible party, if applicable.

11. A responsible party may request SCCMHA to make a new determination of ATP, if they believe it does not appropriately reflect their ATP. The responsible party has a right to contest an ATP, by means of an administrative hearing.

12. In no instance shall the request for a redetermination of ATP result in an amount greater than the original determination.

Definitions:
Ability to Pay (ATP) - the ability of a responsible party to pay for the cost of services, as determined under sections 818 and 819 of the Mental Health Code

Coordination of Benefits (COB) – The coordination of billing priority when a person served is covered, in part or in whole, under any type of insurance coverage, private or public, for services provided directly or by contract with SCCMHA.

Cost of Services – The total operating and capital costs incurred by SCCMHA with respect to, or on behalf of, a person served. Cost of services does not include the costs of research programs or expenses unrelated to the provision of mental health services. Section 800 of the Mental Health Code

Person Served– The minor or adult who receives services from SCCMHA or one of its contracted providers.

Insurance Benefits – Payments made in accordance with insurance coverage for the cost of health care services provided to an consumer.

Insurance Coverage – Any policy, plan, program, or fund established or maintained for the purpose of providing for its participants or their dependents medical, surgical, or hospital benefits. Insurance coverage includes, but is not limited to, Medicaid or Medicare; policies, plans, programs, or funds maintained by nonprofit hospital services and medical care corporations, health maintenance organizations, and prudent purchaser organizations, and commercial, union, association, self-funded and administrative service policies, plans, program and funds.

Responsible Party – The person financially liable for services furnished, which includes the person served and, as applicable, the person served spouse and parent or parents of minor.

References:
Michigan Mental Health Code – Act 258 of 1974, Chapter #8 , Section – 330-1800 - 330.1844
SCCMHA Procedure 09.02.03.01 Ability to Pay Determination Process
SCCMHA Procedure 09.02.03.02 Person(s) Served Finance Information Sheet - Instructions for Completion of Form
SCCMHA Procedure 09.02.08.04.01 Self Pay Billing Procedure

Exhibits:
None

Procedures:

	ACTIONS	RESPONSIBLE
1.	A financial billing system is set up and maintained to ensure that timely billing of services can be achieved.	Chief Executive Officer
2.	Ensure that responsible parties who are financially liable for cost of services are properly billed for services.	Chief Financial Officer Finance Department Billing Staff
3.	When a person served is covered, in part or in whole, under any type of insurance coverage, private or public, for services provided directly by or by contract with SCCMHA, the benefits from that insurance(s) become a significant part of the coordination of benefits for service.	Chief Financial Officer Finance Department Billing Staff
4.	A determination of the responsible parties and person served ability to pay (ATP) is completed as soon as practical after the start of services.	Clinical Supervisors Primary Case Holder Finance Department Entitlement & Billing Staff
5.	Annual re-determinations of ability to pay is completed.	Primary Case Holder Finance Department Entitlement & Billing Staff
6.	Re-determination of ATP will be completed when requests are received from responsible parties.	Primary Case Holder Finance Department Entitlement & Billing Staff
7.	Communication to responsible party that they have a right to administrative hearing to contest an ability to pay determination.	Customer Service Department

Finance Department Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Contracted Network Provider Claims Submission	**Chapter**: 09.10.01 - Claims	**Subject No:** 09.10.01.01
		
Effective Date: September 14, 2000	**Date of Review/Revision**: 3/18/02, 10/1/02, 4/1/03, 10/1/03, 10/1/06, 2/7/07, 7/1/10, 9/1/10, 11/10/11, 6/15/12, 6/2/14, 5/4/16, 7/21/17, 6/20/18, 6/14/19, 1/27/20, 3/31/20, 12/28/23, 12/30/25 **Supersedes**:	**Approved By**: Chief of Network Business Operations **Authored By**: Chief of Network Business Operations **Reviewed By**: Claims Processors:

Purpose:
In order to ensure accurate and timely payment of claims, the following specific claims related guidelines have been issued.

Application:
SCCMHA Claims Processors
SCCMHA Chief of Network Business Operations
SCCMHA Contracted Network Service Providers

Policy:
None

Standards:
None

Definitions:
Clean Claim: A clean claim is defined as having all claims criteria accurately supplied and free of all error messages.

References:
SCCMHA Financial Liability for Mental Health Services Policy - 05.02.06
UB04 (CMS-1450) Uniform Billing Form Instructions - 09.10.01.01.05
Sentri Claims Adjudication Reason Codes - 09.10.01.01.02

Non Panel– Non Contract Provider Authorizations and Claims Submission Procedures - 09.10.01.01.09
Sentri Claims Processing and Reimbursement Procedures - 09.10.01.01

Exhibits:
None

Procedure:
- Claims Submission:

The provider shall submit to SCCMHA claims for payment of authorized covered services. There are three types of submission:

1. Claims prepared on either a form CMS-1500 for Professional Charges or UB04 (CMS-1450) for Institutional charges for Inpatient Stays as described in the Service Provider Manual and mailed to SCCMHA claims department.
2. Online data entered directly into the SCCMHA E.H.R. software "Sentri". Provider setup specific login must be obtained by SCCMHA IS Department individually specific to each provider's setup(s) for each billing clerk as described in the Service Provider Manual.
3. Electronic data transmission approved through SCCMHA 837p or 837i file.

The provider shall submit clean claims within ninety (90) calendar days of service and not to exceed forty-five (45) days from end of each fiscal year ending September 30th, or within thirty (30) calendar days of receipt of remittance advice from payors precedent to SCCMHA, not to exceed a year from date of service.

To prevent delay in processing of claims, all paper claims should be mailed to:

SCCMHA
Attn: Claims Processing Department
500 Hancock
Saginaw, MI 48602

Claims may also be dropped off at 500 Hancock exterior drop box located near canopy entrance or the Customer Services window at 500 Hancock, addressed to the attention of Claims Processing.

- Claims Criteria:

All claims must be submitted in a HIPAA 837 compliant format, with all critical information provided without errors in order to be considered a clean claim.

The letter(s) of authorization available by SCCMHA E.H.R. Sentri will provide current claims information. Every claim must contain this authorization number in order to be

considered a clean claim. **Claim Processers do not approve nor create service authorization numbers**.

- Claims Processing:

The Provider must adjudicate the claim batch and review for errors. The errors should be corrected and the claim batch should be re-adjudicated by the Provider prior to the submission. This above statement also applies to electronic 837 files.

The Claims Processors will assist the Provider on behalf of provider relations but will not make corrections of any claims submission data fields for the Provider. Claims with errors remaining after submission will be returned or denied.

Please refer to Procedure 09.10.01.01.02 Sentri Claims Adjudication Reason Codes. It outlines the various claim's remittance error messages processed through Sentri.

If there is a payor precedent to SCCMHA, the Provider must enter and preferably scan the COB information on the service line item and/or provide proof of COB information to the Claims Processer. For non-panel out of network claims, COB information can be submitted via Sentri messaging, fax 989-799-3918 or US Mail.

SCCMHA will make timely payments to all providers for covered services as outlined in their signed provider participation agreement. Paper claims received at SCCMHA will be date stamped when received. Claims received thru Sentri will have recorded and automated submission date. Clean claims will be paid within 30 days of receipt. This standard may vary for services rendered under a sub-contract in which other timeliness standards such as documentation have been specified and agreed to by both parties.

- Claims Payment:

SCCMHA's provider participation agreement requires providers to bill SCCMHA their actual cost of providing the service rendered (Usual & Customary Fee). Claims will be paid based on the rate established within their signed provider participation agreement.

False Claims: If a claim submitted by the provider is paid by SCCMHA, but is subsequently determined to be a false claim (i.e., improper or unsubstantiated), SCCMHA is entitled to recover its costs by deducting the amount of the false claim from the provider's future claims or requiring reimbursement by the provider. In addition to the amount of the false claim, SCCMHA costs may include, but are not limited to, associated administrative costs and expenses. SCCMHA also reserves the right to seek any other remedies available at law and/or in equity.

ACTION	RESPONSIBILITY
1. Mail paper claims in UB04 or HCFA1500 837 compliant format to SCCMHA	Network Services Provider
2. If submitting electronically, either by 837 file or direct data entry into Sentri. Provider to Run and Review their batches' Adjudication Report in Step #2 of Sentri claims submission	Network Services Provider
3. If submitting electronically, Provider is to correct any errors prior to final submission of Claims to SCCMHA	Network Service Provider
4. Provider to Submit Clean Claims to SCCMHA via either US mail system or electronically, this also includes associated COB information required if CMH is not primary Payor.	Network Services Provider
5. SCCMHA will Adjudicate Claims timely	Claims Processors
6. SCCMHA Claims Processors will Assist Providers with Resolving Claim Errors. It is the Providers Responsibility to submit Clean Claims	Claims Processors
7. SCCMHA Claims Processors will return or deny Batches if Claims are not Clean	Claims Processors

Finance Department Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Electronic Claims Submission by Provider	**Chapter:** 09.10.01 - Claims	**Subject No:** 09.10.01.01.01
		
Effective Date: 10/1/06	**Date of Review/Revision:** 3/28/07, 6/24/10, 11/18/11, 6/15/12, 6/2/14, 5/13/16, 6/20/18, 6/14/19, 1/27/20, 12/28/23, 12/30/25 **Supersedes:** 09.02.01.01.30	**Approved By:** Chief Of Network Business Operations **Authored By** Chief of Network Business Operations **Reviewed By:** Claims Processors

Purpose:
To provide instruction to network providers on claims entry and submission using the Sentri claims processing software.

Application:
SCCMHA Claims Processors
SCCMHA Chief of Network Business Operations
SCCMHA Provider Network

Policy:
None

Standards:
None

Definitions:

Adjudication- Reported process that shows whether the claim has errors. The Adjudication Report should be run prior to submission of claims to SCCMHA. Final adjudication is performed by the SCCMHA Claims Processors.

Approval- recommendation for payment.

Approved Claims- Approved claims in this procedure refer to the claims that have been entered and edited by the provider to be submitted to SCCMHA for payment. Claim entry and provider approval is achieved by completing Steps 1 & 2 on the Sentri claims processing menu.

Authorization- The document allowing the provider to render and bill for services. These person served-specific authorization numbers are obtained through SCCMHA Care Management Dept. as requested by the person served's primary record holder.

Claim Form- UB04 (CMS 1450) or HCFA 1500 (CMS 1500).

Claims Processing/Management - Sentri view that allows access to claims submission functions.

CMHSP- Community Mental Health Service Program. Saginaw County Community Mental Health Authority is one of Michigan's CMHSPs.

Entered Claims- Entered claims in this procedure refer to the claims that have completed Step 1 of the Sentri claims processing menu.

Reconsider- Process where a claim line is backed out by SCCMHA Claim Processors. This places a credit on the Provider's payable account.

SCCMHA- Saginaw County Community Mental Health Authority

SCCMHA Sentri software- The E.H.R. claims processing system and software used by SCCMHA for processing and payment of claims.

837 File – HIPAA compliant electronic file submission

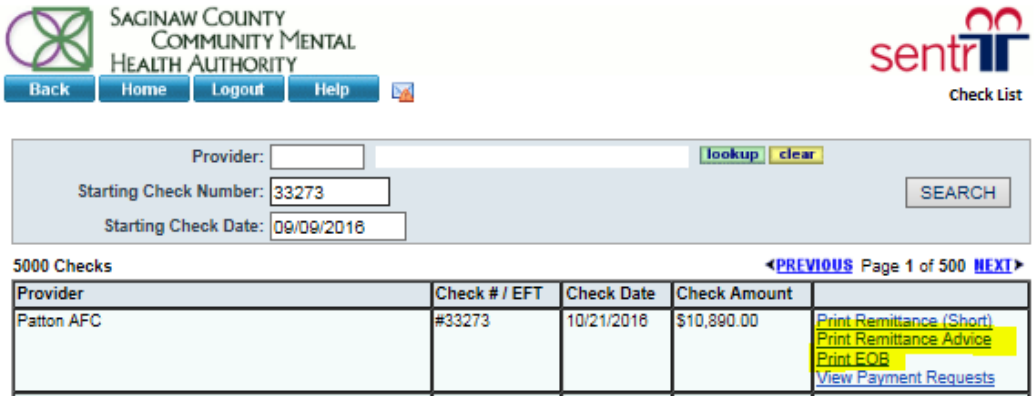
References:
SCCMHA Provider Registration and Maintenance for Access to Sentri Claims Module – 09.10.01.01.06
SCCMHA Sentri Claims Submission by Provider– 09.10.01.01.01
SCCMHA Sentri Claims Adjudication Reason Codes – 09.10.01.01.02

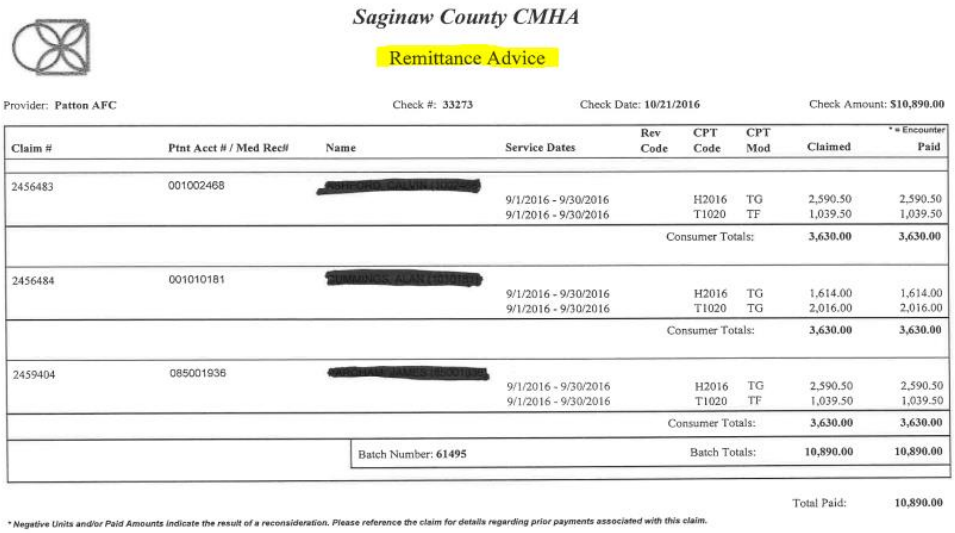
Exhibits:
None

Procedure:

ACTION	RESPONSIBILITY
1. Enter claims into Sentri System	Provider
2. Adjudicate the batch and review for errors. Make corrections and re-adjudicate for final submission	Provider
3. Send Batch(es) to CMHSP (or SCCMHA)	Provider
4. Final Adjudication/applicable COB review for Submitted Approved Claims from Provider	SCCMHA Claims Processor(s)
5. Submits Electronic Funds Transfer (EFT) or Print checks	SCCMHA General Ledger Staff Accountant/Accounts Payable Clerk
6. Print remittance advice and explanation of benefits to include with check.	Claims Processors for non-panel providers; Provider prints if claim electronically submitted
7. Contracted Provider's electronic funds transfers (EFT)	SCCMHA General Ledger Staff Accountant/Accounts Payable Clerk

Sample visuals of Remittance Advice/EOB reports:





Saginaw County CMHA

Remittance Advice

Provider: **Patton AFC** Check #: **33273** Check Date: **10/21/2016** Check Amount: **$10,890.00**

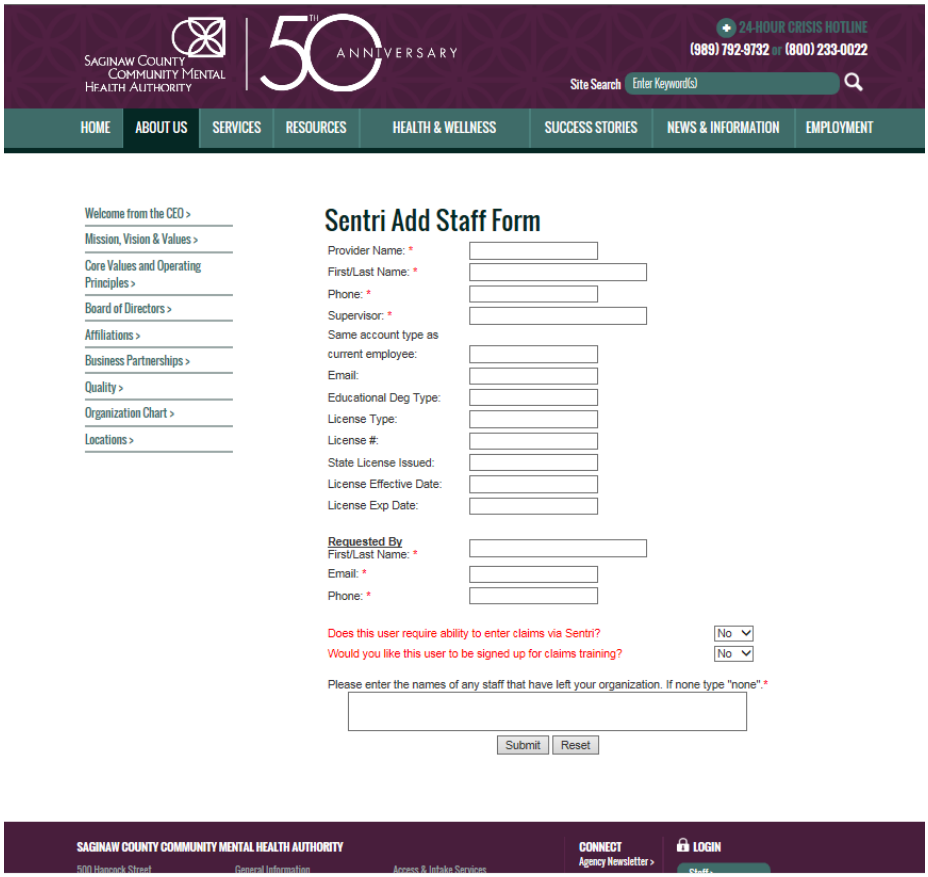
Claim #	Ptnt Acct # / Med Rec#	Name	Service Dates	Rev Code	CPT Code	CPT Mod	Claimed	* = Encounter Paid
2456483	001002468	[redacted]	9/1/2016 - 9/30/2016		H2016	TG	2,590.50	2,590.50
			9/1/2016 - 9/30/2016		T1020	TF	1,039.50	1,039.50
					Consumer Totals:		**3,630.00**	**3,630.00**
2456484	001010181	[redacted]	9/1/2016 - 9/30/2016		H2016	TG	1,614.00	1,614.00
			9/1/2016 - 9/30/2016		T1020	TG	2,016.00	2,016.00
					Consumer Totals:		**3,630.00**	**3,630.00**
2459404	085001936	[redacted]	9/1/2016 - 9/30/2016		H2016	TG	2,590.50	2,590.50
			9/1/2016 - 9/30/2016		T1020	TF	1,039.50	1,039.50
					Consumer Totals:		**3,630.00**	**3,630.00**
		Batch Number: **61495**			Batch Totals:		**10,890.00**	**10,890.00**

Total Paid: **10,890.00**

** Negative Units and/or Paid Amounts indicate the result of a reconsideration. Please reference the claim for details regarding prior payments associated with this claim.*

- Provider claims are either entered directly into the Sentri system or through a HIPAA 837p or 837i compliant format.

- The provider must contact the SCCMHA IS Department Help Desk via SCCMHA website link (teamdynamix.com)https://sccmha.teamdynamix.com/TDClient/63/Portal/Requests/TicketRequests/NewForm?ID=QZgvpkBO4NM_&RequestorType=Service or email Hdesk@sccmha.org to make arrangements for electronic access to Sentri claims module. Please reference procedure 09.10.01.01.6-SCCMHA Provider Registration and Maintenance for Access to Sentri Claims Module for additional information.



Answer "Yes" to the following two questions on the "Sentri Add Staff" form to request Sentri claims access and to request training on the Sentri claims system.

Does this user require ability to enter claims via Sentri? Yes

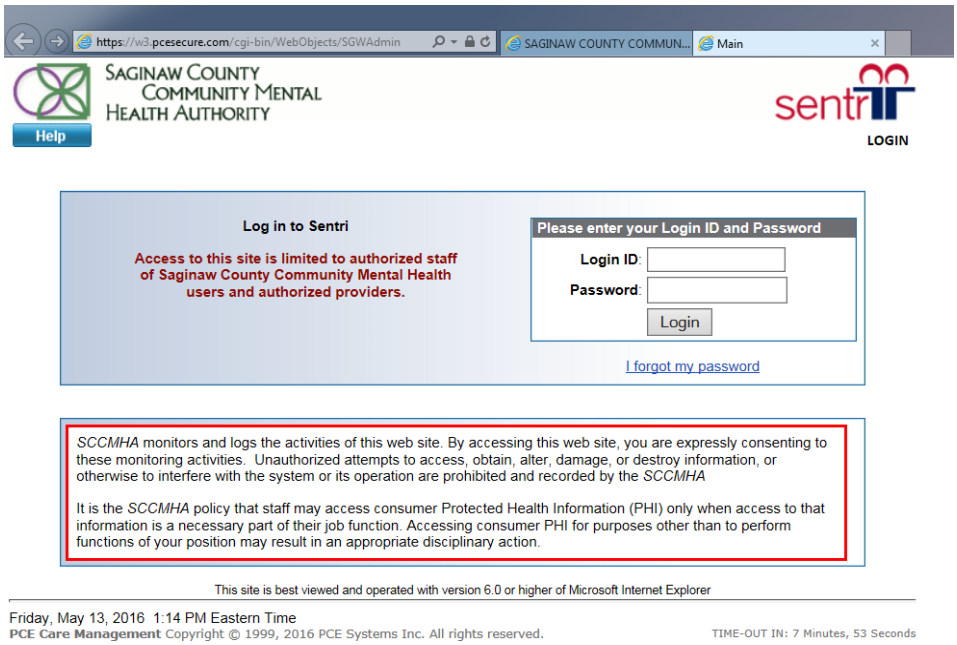
Would you like this user to be signed up for claims training? Yes

- Call the Claims Processing Department to set up training, if needed.
  - After obtaining the Log In, and Password, the provider can log into https://w3.pcesecure.com/cgi-bin/WebObjects/SGWAdmin

  - Logins should not be shared and should be kept secure. SCCMHA staff, service programs and network providers will abide by current HIPAA requirements to protect the privacy and security of the health information of persons who are service recipients of SCCMHA. SCCMHA is a "Covered Entity" as defined by HIPAA

and HIPAA compliance is an employment and contractual obligation for all members of the SCCMHA provider network workforce.

Snapshot of Sentri Login Screen:

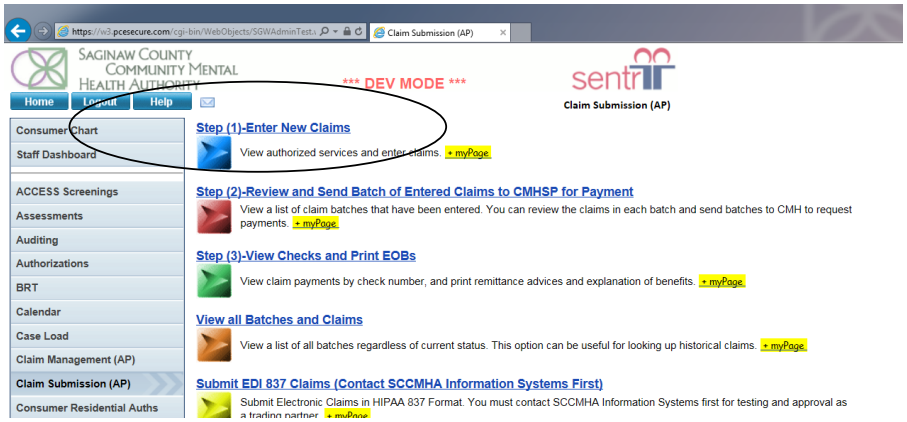


CLAIMS PROCESSING IN SENTRI

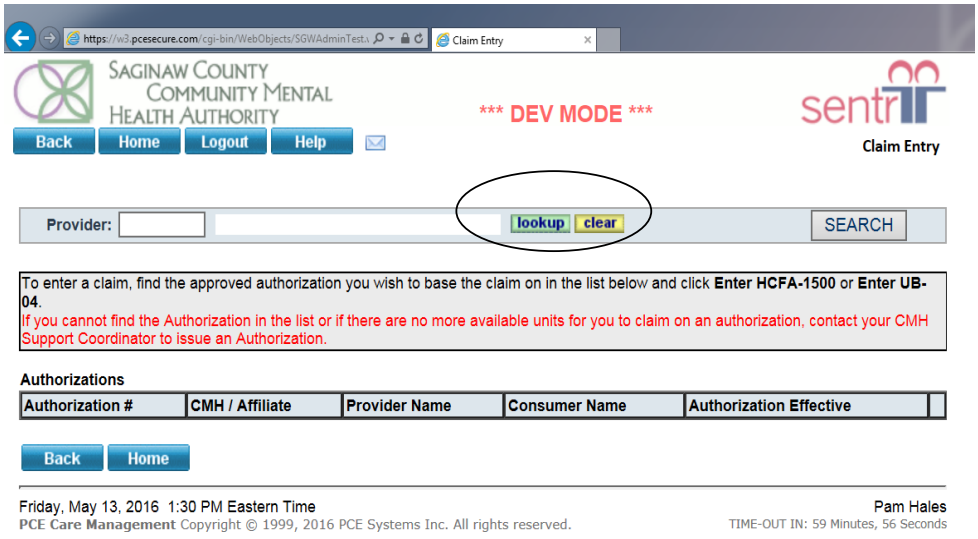
After logging into Sentri, click on **"Claim Submission"** button on the left side of the screen.

STEP 1

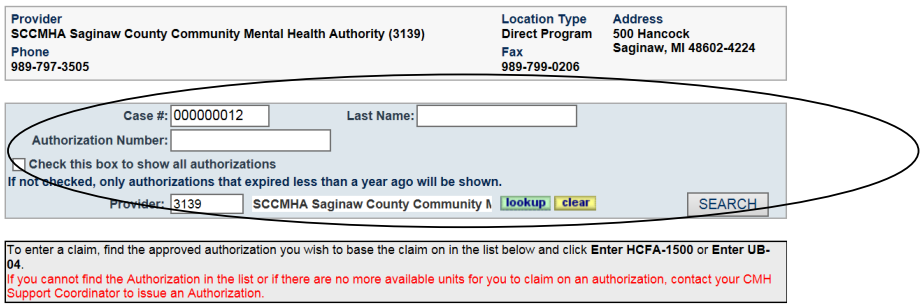
A) Click "Step (1) - Enter New Claims"



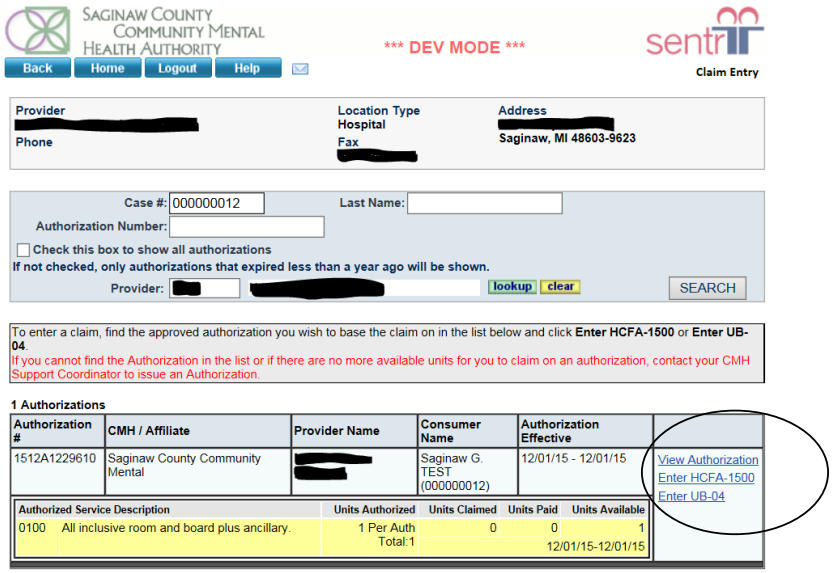
B) Click "Lookup" and type in Provider name.



C) Enter either the person served "Case#" or "Last Name" and click the "Check this box to show all authorizations". Then click "**Search".**



D) Authorizations will appear for the person served in newest to oldest order. Note: There may be more than one page of authorizations to view. Find the authorization that matches the provider, date range and code that you are preparing to bill for. Use the blue links circled below to proceed to the correct billing form (the HCFA-1500 or the UB-04); there is also a link to "View Authorization" that will allow you to see more detail regarding the authorization.



If you are unable to locate an authorization, you will **not** be able to continue entering claims for this person served. Please contact the person served's assigned primary record holder to have an authorization requested, or to check the status of the authorization.

TIP - Be Proactive - Make your inquiries via Sentri messaging or secure email so they are documented. Set up some kind of tracking and be sure to follow up on the same email thread.

Create your own internal set of procedures:

- What does the Billing Clerk do when they can't enter a claim because the Authorization is missing or needs correction?
- How are you going to track this claim to make sure it gets submitted?
- How long should the Billing Clerk wait before the next level of your internal Management gets involved?
- What is causing the missing Authorization? Is the problem chronic?
- Do you need a formal Correction Action Request system?

Don't wait to reconcile SCCMHA's check against your internal system to find out the claim was never submitted.

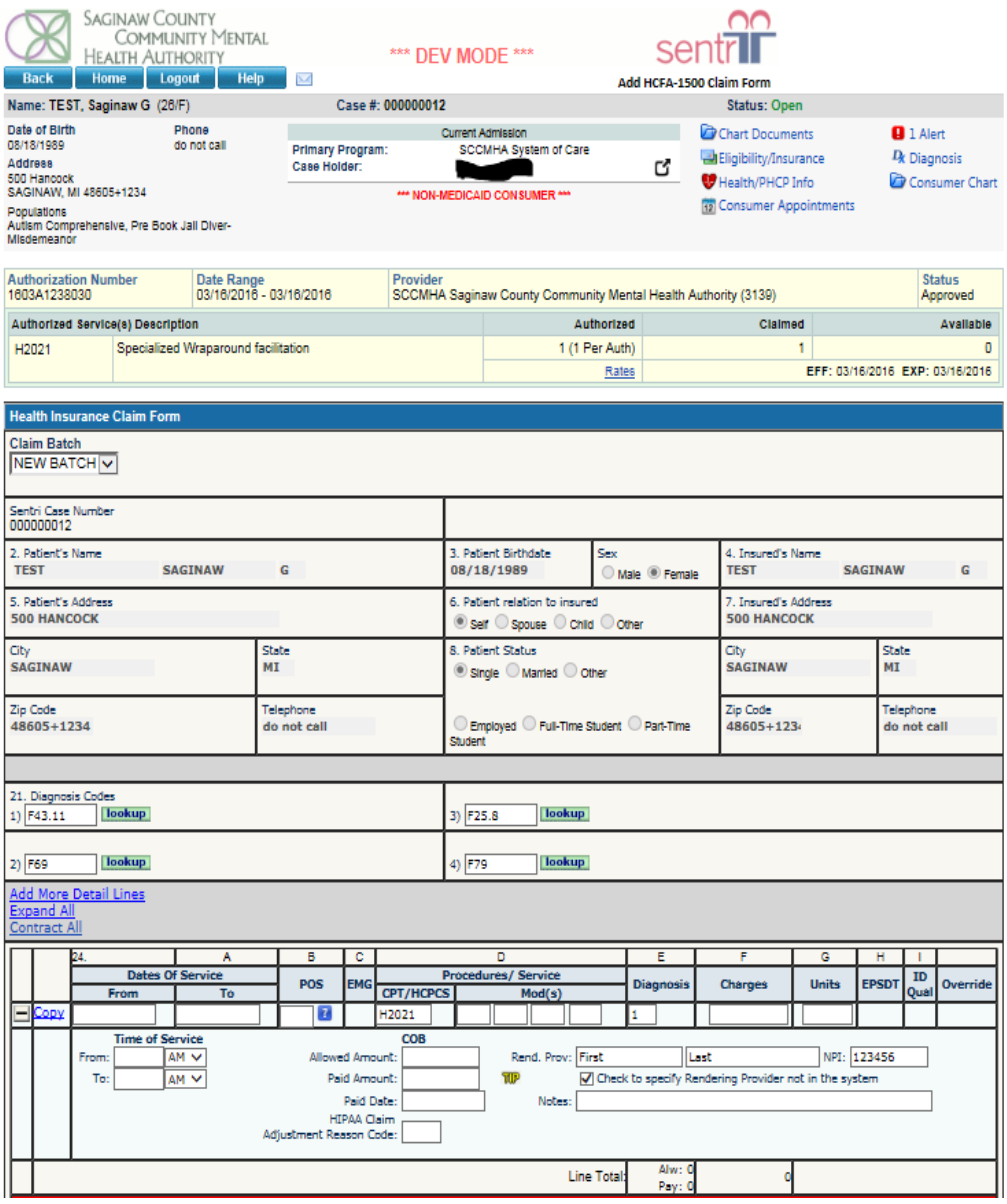
SCCMHA Claims Processors do not have authority or access to create or change Authorizations.

Timely claim submission will help your organization's cash flow.

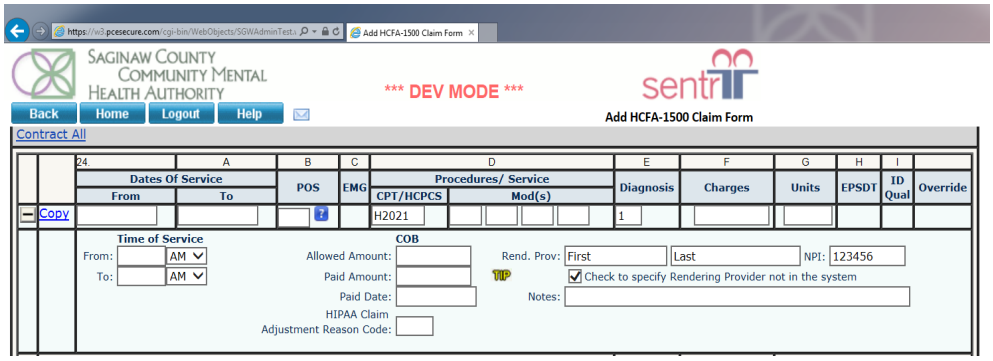
SCCMHA is required to submit various reports to their PHIP and Michigan Department of Health & Human Services (MDHHS) throughout the year regarding funding requirement forecasts. We need timely claim submission to allow us to provide accurate figures to submit. This has a direct effect on the funds that are made available to SCCMHA from the MDHHS.

E) Enter claim information into the electronic form. A number of the fields will automatically pre-populated with person served data that is housed in Sentri. Other fields will need to be manually entered.

Sample: HCFA-1500 Form



Box #24 of the HCFA contains a number of fields that require manual entry such as: Dates of Service, POS (Place of Service), CPT/HCPCS (procedure code), Mod(s) (Modifiers), Charges, Units, COB (Coordination of Benefits), NPI number, and Time of Service fields.



24 A. Dates of Service
The dates you enter must fall in between the dates on the Authorization or the line will error out. Are you using the correct Authorization?

24 B. POS Place of Service
Sentri has a menu item to obtain current list. Below is a sample list:

25 Records.

Code	Description
01	01-Pharmacy
02	02-Telehealth
03	03-School
04	04-Homeless Shelter
09	09-CCI / Jail / Prison
10	10-Telehealth at Home
11	11-Office
12	12-Home
13	13-Assisted Living Facility
14	14-Group Home (AFC)
15	15-Mobile Unit
20	20-Urgent Care Facility
21	21-Inpatient Hospital
22	22-Outpatient Hospital
23	23-Emergency Room-Hospital
31	31-Skilled Nursing Facility
32	32-Nursing Facility
33	33-Custodial Care Facility
41	41-Ambulance-Land
51	51-Inpatient Psych. Facility

24 C. EMG – is left blank.

24 D. Procedures/Service
CPT/HCPCS code along with any Modifiers as listedon the Authorization. If you get an error message refer back to the Authorization. Are you using the correct Authorization number?

24 E. Diagnosis Code

24 F. Charges
Providers are to bill SCCMHA their actual costs. Claims will be paid based on the rate established in the signed Provider Participation Agreement.

24 G. Units
See PIHP/CMHSP ENCOUNTER REPORTING HCPCS and REVENUE CODES for rules on Units of measure.

PIHP/CMHSP ENCOUNTER REPORTING
HCPCS and REVENUE CODES

GENERAL RULES FOR REPORTING

1a. Rounding rules for HCPCS reporting:

"Up to 15 Minutes"	15 Minutes	30 Minutes	45 Minutes	60 Minutes
1-15 = 1 unit	1-14 minutes= 0*	0-29 minutes = 0*	0-44 minutes = 0*	1-59 minutes = 0*
16-30 = 2 units	15-29 = 1 unit	30-59 = 1 unit	45-89 = 1 unit	60-119 = 1 unit
31-45 = 3 units	30-44 = 2 units	60-89 = 2 units	90-134 = 2 units	120-179 = 2 units
46-60 = 4 units	45-59 = 3 units		135-179 = 3 units	180-239 = 3 units
61-75 = 5 units	60-74 = 4 units			240-299 = 4 units
76-90 = 6 units	75-89 = 5 units			300-359 = 5 units
91-105 = 7 units	90-104 = 6 units			360-419 = 6 units
106-120 = 8 units	105-119 = 7 units			420-479 = 7 units
	120-134 = 8 units			480-539 = 8 units

* Do not report if units equal zero.

1b. Rounding rules for CPT reporting of 15-minute codes:

Units	Time
0	0-7 minutes
1	8-22 minutes
2	23-37 minutes
3	38-52 minutes
4	53-67 minutes

1. Select the service (see CPT code descriptions).
2. Report a timed service based on face-to-face time on each date of service.
3. The CPT rule states that a unit of time is attained when the mid-point is passed.

Effective 10/1/2019
On the web at: http://www.michigan.gov/bhdda Reporting Requirements,
PIHP/CMHSP Reporting Cost Per Code and Code Chart Page 2

If you get an error with "Units Exhausted", check the Authorization screen in Sentri. There might be another Authorization with remaining units. You may have to request more units from primary record holder.

Notes on Time of Service fields

- "Time of Service" fields are found in box #24 of the HCFA-1500 form located in Sentri. When adding the "From" & "To" times of service, note the AM/PM. AM is the default, so make sure that you pick the correct time of day.
- These fields are displayed by clicking the **"+"** sign on the left-hand side of the form, next to the blue "Copy" link.
- Time of Service fields may be required depending on the CPT code. **The start/stop time must equal the units. The claim will error out if they don't match.**

Notes on Coordination of Benefit fields

-
- "Coordination of Benefit" line specific fields are found in box #24 of the HCFA-1500 form located in Sentri.
- This COB field is displayed by clicking the **"Attachment"** link on the bottom left-hand side of the form.
- The "Coordination of Benefit" info can be uploaded or scanned into each claim line to include the following:
  - **"Allowed Amount"** (REQUIRED field)
  - **"Paid Amount"** (REQUIRED field)
  - **"Paid Date"** (REQUIRED field)
  - **"HIPAA Claim Adjustment Reason Code"** (REQUIRED field)
  - **"Notes"**– this text box can be used by the provider to document/communicate any specific notes regarding the specific claim line.

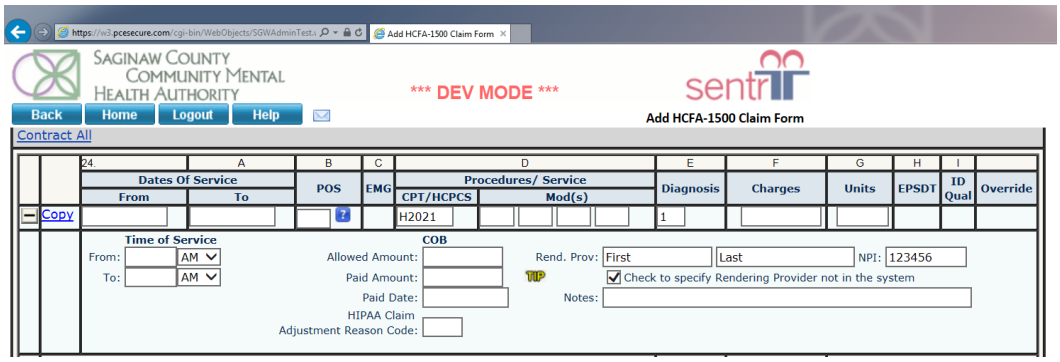
TIP Notes on "Copy" feature.

A claim line can be copied by clicking the blue "**Copy**" link on the left-hand side of the Sentri HCFA-1500 form. After clicking **"Copy"**, a calendar will appear that will allow you to designate the days of the month where you'd like the current claim line copied.

Notes on NPI (National Provider Identifier) if applicable.

- "**Rendering Provider**" and "**NPI**" line specific fields are found in box #24 of the HCFA-1500 form located in Sentri.
- These fields are displayed by clicking the **"+"** sign on the left-hand side of the form, next to the blue "Copy" link.

- Click the box next to: **"Check to specify Rendering Provider not in the system"**
- Then fill in the following fields
- "**Rend. Prov**" – Rendering Provider
- "**NPI**" –National Provider Identifier

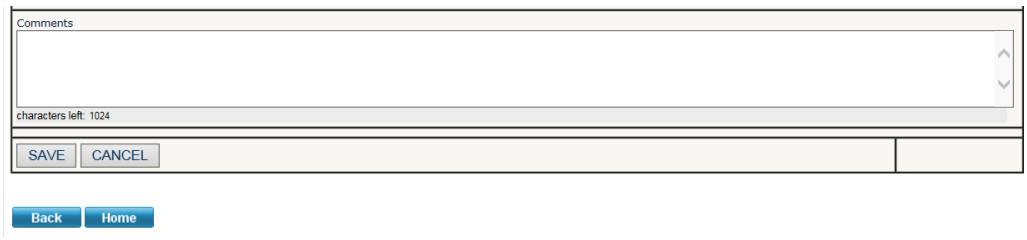


TIP How to add a new Rendering Provider to Sentri
Biller or claims processor to send an email to helpdesk@sccmha.org. Email should state the name of the Billing Provider, the full legal name and NPI # of the new rendering provider you wish to add to Sentri.

E) Enter any notes related to the claim in the "Comment" field at the bottom of the form.

F) When finished adding dates of service and times of service, you must **SAVE** at the bottom of the form and go on to add other claims or proceed to the next step.

G) When the form is complete, click "**Save**" at the bottom of the claim.



Sentri will assign a batch number. Keep track of your batch numbers in some kind of log.

Always remember to SAVE the claim!

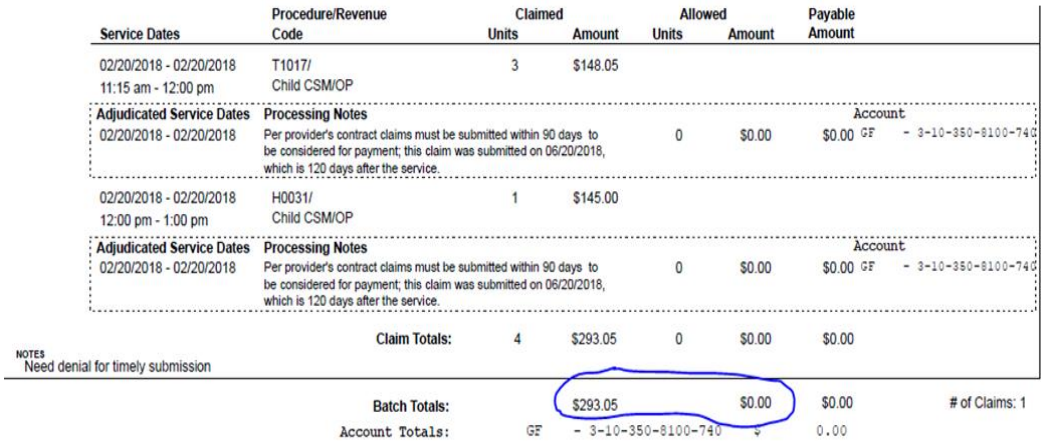
STEP 2

After all claims have been entered, return to the "Claims Management" home page and click **"Step (2) – Review and Send Batch of Entered Claims to CMHSP for Payment"**.

Run and review the Adjudication Report and look for errors. You can review these on the screen. Smaller batches are sometimes more manageable than 100-page claim's batch.

Correct the errors and re-adjudicate the batch. Run and review the Adjudication Report again until all the errors are corrected and you have a "clean claim".

Review the bottom of the batch to check to see if the numbers at the bottom match.



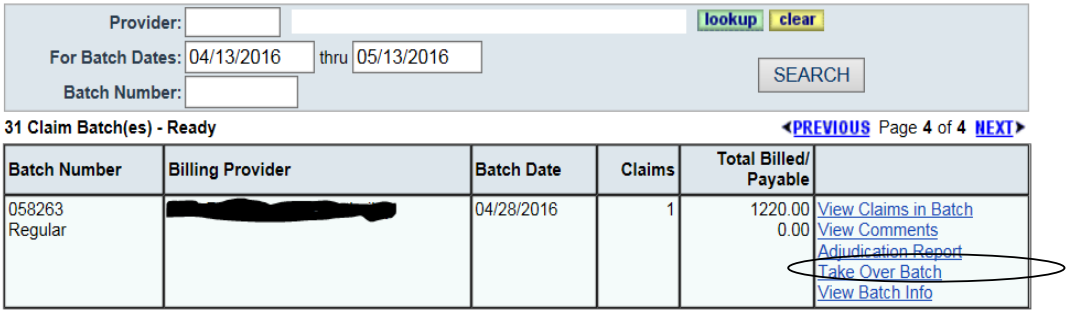
Service Dates	Procedure/Revenue Code	Claimed Units	Claimed Amount	Allowed Units	Allowed Amount	Payable Amount	
02/20/2018 - 02/20/2018 11:15 am - 12:00 pm	T1017/ Child CSM/OP	3	$148.05				
Adjudicated Service Dates	**Processing Notes**					Account	
02/20/2018 - 02/20/2018	Per provider's contract claims must be submitted within 90 days to be considered for payment; this claim was submitted on 06/20/2018, which is 120 days after the service.			0	$0.00	$0.00	GF - 3-10-350-8100-740
02/20/2018 - 02/20/2018 12:00 pm - 1:00 pm	H0031/ Child CSM/OP	1	$145.00				
Adjudicated Service Dates	**Processing Notes**					Account	
02/20/2018 - 02/20/2018	Per provider's contract claims must be submitted within 90 days to be considered for payment; this claim was submitted on 06/20/2018, which is 120 days after the service.			0	$0.00	$0.00	GF - 3-10-350-8100-740
	Claim Totals:	4	$293.05	0	$0.00	$0.00	
NOTES Need denial for timely submission							
	Batch Totals:		$293.05		$0.00	$0.00	# of Claims: 1
	Account Totals:	GF	- 3-10-350-8100-740			0.00	

In the above sample the Batch Total Claimed Amount is $ 293.05. The amount in the Allowed Amount column is Zero. This means SCCMHA is not paying for this line item.

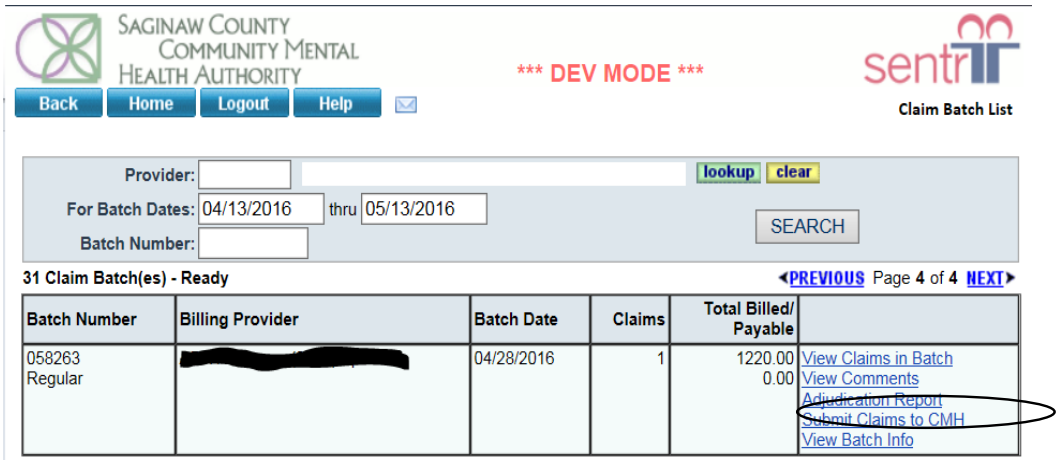
Reference Procedure 09.10.01.01.02 Sentri Claims adjudication Reason Codes

Do not wait until you are missing a payment to reconcile your claims. Reconcile them before you take the next step.

If Claims Processor is assisting the biller, then click the blue link that says, "**Take Over Batch**"



Then click the blue link that says, "**Submit Claims to CMH**"



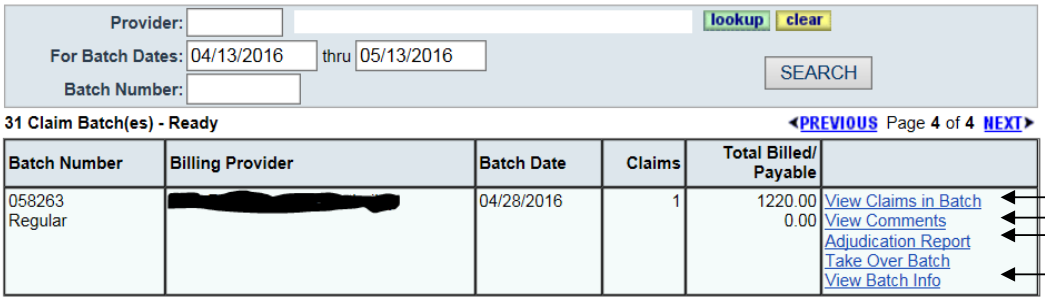
Important: This step is necessary for claims to be sent to SCCMHA for processing. Failure to complete this step will result in no claim payment and/or possible claim denial.

When the batch is submitted to SCCMHA it is date stamped by Sentri; or for paper claims date stamped by customer service or claims processor. SCCMHA Claim Processors will review each batch in the order that they are received. They may return a batch to you for correction.

SCCMHA Claim Processors will assist new billers with error messages. **Claim Processors cannot make corrections to your claims**. Claim Processors cannot override error messages. They must obtain approval from Chief of Network Business Operations.

Please review your Sentri messaging timely and make the necessary changes. If you re-submit the claim again without making the changes/corrections, the claim may be denied.

OTHER INFORMATION obtained through the "Step (2)-Review and Send Batch of Entered Claims to CMHSP for Payment" screen



The "Step (2)- Review and Send Batch of Entered Claims to CMHSP for Payment" screen will allow you to access the following links:

a) "<u>View claims in Batch</u>" will allow you to:

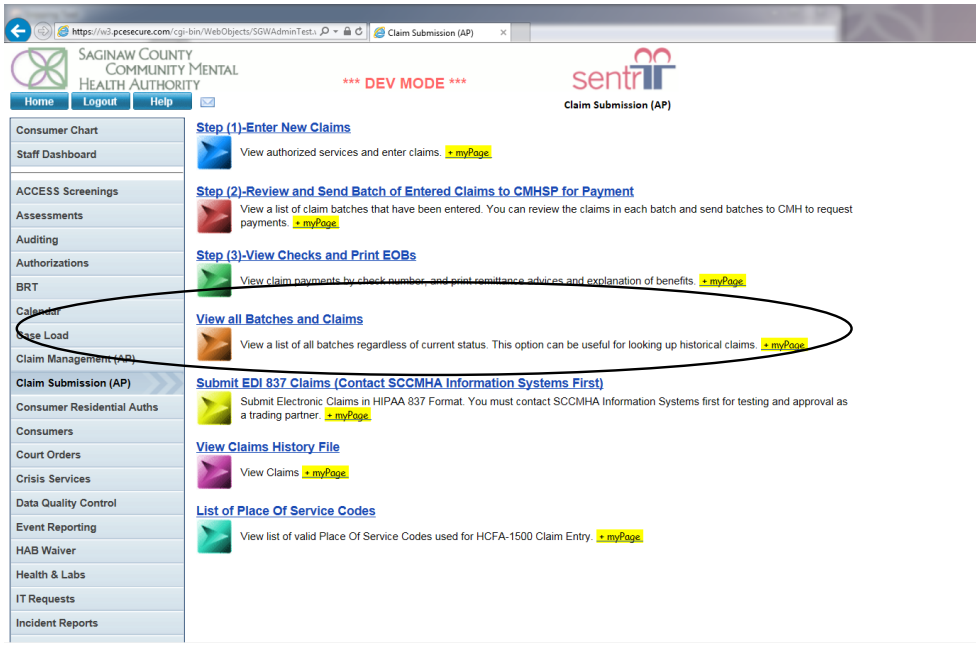
- View a claim
- Change a claim
- Delete a claim

b) "**<u>View Comments</u>**" allows a provider/claims processor to view any comments typed into the comment field located at the bottom of the claim entry form.

c) "**<u>Adjudication Report</u>**" allows you the ability to review the claims entered in the batch through a "*Batch Edit Report"*, click on the "Adjudication Report" link and then click on the icon at the top of the screen to view/print the report.

d) **"<u>View Batch Info</u>"** gives a summary of batch information

OTHER INFORMATION obtained through "Claims Submission" Home Page



a) "**Step (3)- View Checks and print EOBs"** by entering the desired check number and clicking "Search".

b) "**View all Batches and Claims"** allows providers to status their claim batches.

c) "**Submit EDI 837 Claims (Contact SCCMHA information Systems First helpdesk@sccmha.org) for system to system setup and testing**" these electronic setups are used by providers who upload their claims using an electronic 837p or 837i file.

d) "**View Claims History File**" allows provider to view paid claims.

e) "**List of Place of Service Codes**" shows Place of Service reference list.

RECONSIDER A CLAIM

The process of reconsidering a claim zeros out the line item on a claim that is in error. It will process as a credit on the Billing Provider's Account.

If you have errors that need to be corrected after the batch is processed. A request to reconsider a claim must be made in writing via Sentri Message system to the Claim Processer assigned to your account.

Please provide the claim number, the person served's Name, Sentri ID#, Date of Service, and reason for the request for reconsider and dollar amounts.

The claim will be reconsidered by a SCCMHA Claims Processor. The Claims Processor will notify you when complete. If applicable, you can re-enter the corrected services/claim(s).

SCCMHA Event Verification – Audit results from SCCMHA Provider Network Audit Department.

If errors are found during an audit, you will receive a letter from SCCMHA Audit Department. **Providers are not to submit refund checks.**

The below Claims Processor assigned to your account will Reconsider the Claims to Zero. This will put a credit on your account and will be netted from the next check or EFT. The letter may state that provider can re-bill the claim fixing whatever is wrong. It is important that the claim is zeroed out first. Otherwise, you may get a duplicate service error. Contact your Claims Processor to help resolve any re-billing issue.

Finance Department Procedure Manual Saginaw County Community Mental Health Authority		
Subject: UB 04 (CMS-1450) Uniform Billing Form Instructions	**Chapter:** 09.10.01 - Claims	**Subject No:** 09.10.01.01.05
		
Effective Date: October 1, 2006	**Date of Review/Revision:** 10/1/06, 5/23/07, 7/1/10, 11/10/11, 6/15/12, 6/2/14, 4/27/16, 5/1/17, 6/20/18, 6/14/19, 2/27/20, 1/4/24, 12/30/25	**Approved By:** Chief of Network Business Operations
	Supersedes:	**Authored By:** Chief of Network Business Operations **Reviewed By:** Claims Processors

Purpose:
In order to insure accurate and timely payment of claims, the following specific claims related guidelines have been issued.

Application:
SCCMHA Claims Processors
SCCMHA Chief of Network Business Operations
SCCMHA Provider Network and Non-Contract Providers

Policy:
None

Standards:
None

Definitions:
None

References:
SCCMHA Cash Management Policy- Subject No. 05.02.03
SCCMHA Financial Liability for Mental Health Services Policy- Subject No. 05.02.06

Exhibits:
Exhibit A - Example of UB 04 (CMS 1450) Claim Form

Procedure:

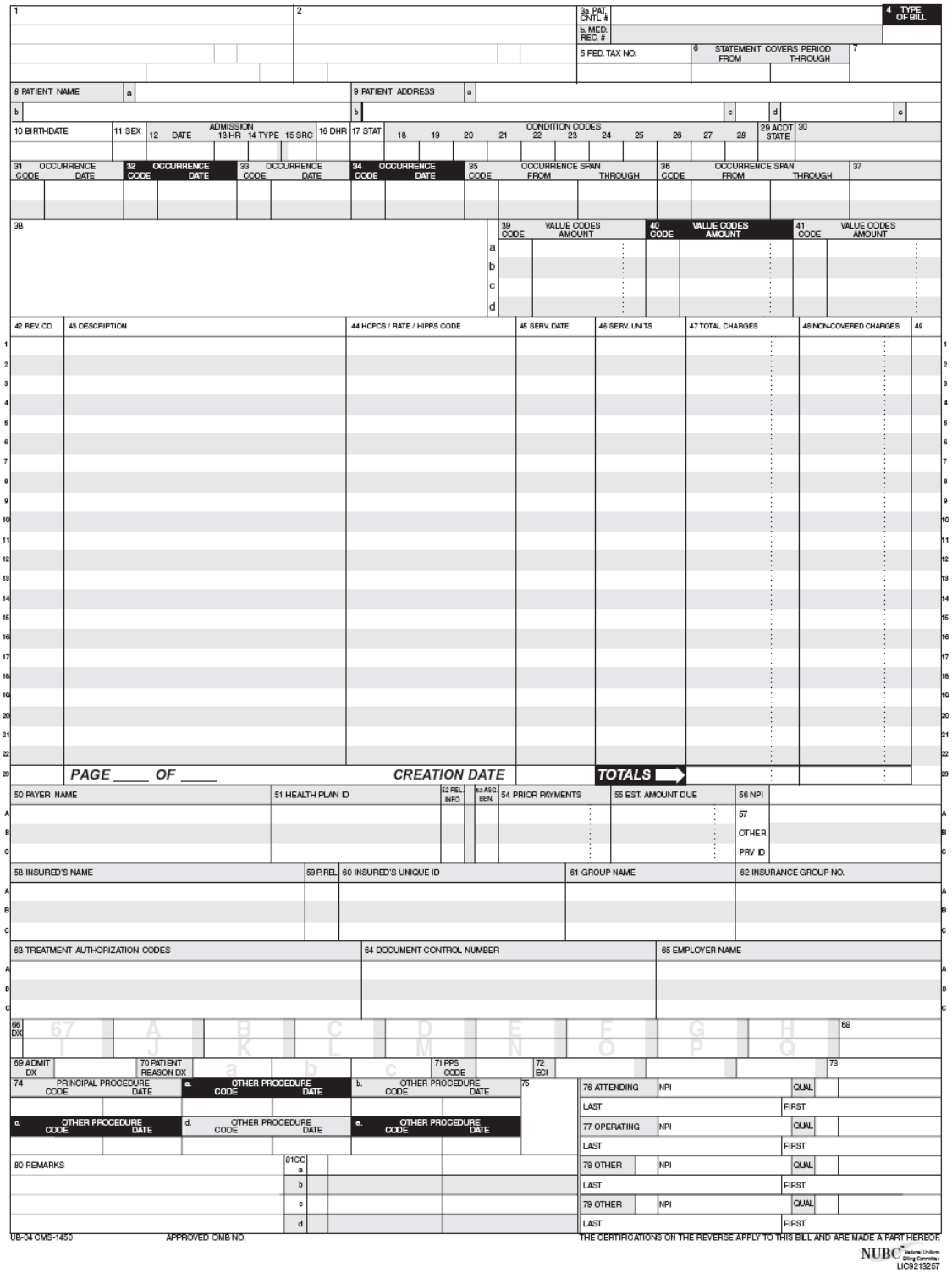
ACTION	RESPONSIBILITY
1. Enter claims for submission to SCCMHA Sentri or Fill out UB04 Paper Claim for SCCMHA	Network Services Provider
2. If submitting electronically, Provider to Run and Review the Adjudication Report in Step #2 on Sentri	Network Services Provider
3. If submitting electronically, Provider is to correct any errors prior to final submission of Claims to SCCMHA	Network Service Provider
4. Provider to Submit Clean Claims to SCCMHA via either US mail system or electronically	Network Services Provider
5. SCCMHA will Adjudicate Claims	Claims Processors
6. SCCMHA Claims Processors will Assist Providers with Resolving Errors. It is the Providers Responsibility to submit Clean Claims	Claims Processors
7. SCCMHA Claims Processors will return or deny Batches if Claims are not Clean	Claims Processors
8. Print and Analyze Adjudication Reports	Claims Processors

UB 04 or CMS -1450

- Box 1 Provider Name
  Provider Street Address
  Provider City, State, Zip
- Box 2 Pay-to Name
  Pay-to Address
  Pay-to City, State, Zip
- Box 3a Patient Control Number
- Box 3b Medical Record Number
- Box 4 Type of Bill
- Box 5 Federal Tax Number
- Box 6 Statement Covers Period-From/Through
- Box 7 Unlabeled
- Box 8 Patient Name-ID
- Box 9 Patient Address-Street
  Patient Address-City
  Patient Address-State
  Patient Address-Zip
  Patient Address-County Code
- Box 10 Patient Birth date
- Box 11 Patient Sex
- Box 12 Admission Date
- Box 13 Admission Hour
- Box 14 Type of Admission/Visit
- Box 15 Source of Admission
- Box 16 Discharge Hour
- Box 17 Patient Discharge Status
- Box 18-28 Condition Codes
- Box 29 Accident Status
- Box 30 Unlabeled
- Box 31-34 Occurrence Code Date
- Box 35-36 Occurrence Span Code
  From/Through
- Box 37 Unlabeled
- Box 38 Responsible Payor Party Name/Address
- Box 39-41 Value Code-Code
  Value Code-Amount
- Box 42 Revenue Code
- Box 43 Revenue Code Description
- Box 44 HCPCS/Rate/HIPPS/Rate Codes
- Box 45 Service/Creation Date
- Box 46 Units of Service
- Box 47 Total Charges
- Box 48 Non-Covered Charges
- Box 49 Unlabeled

- Box 50 Payer Name-Primary
  Payer Name-Secondary
  Payer Name-Tertiary
- Box 51 Health Plan-ID
- Box 52 Release of Information
- Box 53 Assignment of Benefits
- Box 54 Prior Payments
- Box 55 Estimated Amount Due
- Box 56 National Provider Identifier (NPI)
- Box 57 Other Provider ID-Primary, Secondary, Tertiary
- Box 58 Insured's Name-Primary, Secondary, Tertiary
- Box 59 Patient's Relationship-Primary, Secondary, Tertiary
- Box 60 Insured's Unique ID-Primary
- Box 61 Insurance Group Name-Primary, Secondary, Tertiary
- Box 62 Insurance Group Number-Primary, Secondary, Tertiary
- Box 63 Treatment Authorization Code-Primary, Secondary, Tertiary
- Box 64 Document Control Number
- Box 65 Employer Name-Primary, Secondary, Tertiary
- Box 66 Diagnosis Version Qualifier
- Box 67 Principal Diagnosis
- Box 67 AQ Other Diagnosis
- Box 68 Unlabeled
- Box 69 Admitting Diagnosis Code
- Box 70 Patient Reason for Visit
- Box 71 PPS Code
- Box 72 External Cause of Injury Code (E-code)
- Box 73 Unlabeled
- Box 74 Principal Procedure Code/Date
- Box 74 AE Other Procedure Code
- Box 75 Unlabeled
- Box 76 Attending-NPI/Qual/ID
  Attending-Last/First Name
- Box 77 Operating-NPI/Qual/ID
  Operating-Last/First Name
- Box 78-79 Other ID-NPI/Qual/ID
  Other ID-Last/First Name
- Box 80 Remarks
- Box 81 Code-Qual/Code/Value

Exhibit A


1
2
3a PAT. CNTL #
b MED. REC. #
4 TYPE OF BILL
5 FED. TAX NO.
6 STATEMENT COVERS PERIOD FROM THROUGH
7
8 PATIENT NAME
9 PATIENT ADDRESS
10 BIRTHDATE
11 SEX
12 ADMISSION DATE
13 HR
14 TYPE
15 SRC
16 DHR
17 STAT
CONDITION CODES
29 ACDT STATE
30
31 OCCURRENCE CODE DATE
32 OCCURRENCE CODE DATE
33 OCCURRENCE CODE DATE
34 OCCURRENCE CODE DATE
35 OCCURRENCE SPAN CODE FROM THROUGH
36 OCCURRENCE SPAN CODE FROM THROUGH
37
38
39 VALUE CODES CODE AMOUNT
40 VALUE CODES CODE AMOUNT
41 VALUE CODES CODE AMOUNT
42 REV. CD.
43 DESCRIPTION
44 HCPCS / RATE / HIPPS CODE
45 SERV. DATE
46 SERV. UNITS
47 TOTAL CHARGES
48 NON-COVERED CHARGES
49
PAGE _____ OF _____
CREATION DATE
TOTALS
50 PAYER NAME
51 HEALTH PLAN ID
52 REL. INFO
53 ASG. BEN.
54 PRIOR PAYMENTS
55 EST. AMOUNT DUE
56 NPI
57 OTHER PRV ID
58 INSURED'S NAME
59 P REL
60 INSURED'S UNIQUE ID
61 GROUP NAME
62 INSURANCE GROUP NO.
63 TREATMENT AUTHORIZATION CODES
64 DOCUMENT CONTROL NUMBER
65 EMPLOYER NAME
66 DX
67
68
69 ADMIT DX
70 PATIENT REASON DX
71 PPS CODE
72 ECI
73
74 PRINCIPAL PROCEDURE CODE DATE
a. OTHER PROCEDURE CODE DATE
b. OTHER PROCEDURE CODE DATE
75
c. OTHER PROCEDURE CODE DATE
d. OTHER PROCEDURE CODE DATE
e. OTHER PROCEDURE CODE DATE
76 ATTENDING NPI QUAL
LAST FIRST
77 OPERATING NPI QUAL
LAST FIRST
78 OTHER NPI QUAL
LAST FIRST
79 OTHER NPI QUAL
LAST FIRST
80 REMARKS
81CC
UB-04 CMS-1450
APPROVED OMB NO.
THE CERTIFICATIONS ON THE REVERSE APPLY TO THIS BILL AND ARE MADE A PART HEREOF.
NUBC
LIC9213257

Operations Department Procedure Manual Saginaw County Community Mental Health Authority		
Subject: Provider Network Appeal Process for Claim Payment Denial	**Chapter**: 09.10 Operations Department Procedures	**Subject No:** 09.10.01.01.13
Operations		
Effective Date: 12/8/2021	**Date of Review/Revision:** 11/28/22, 1/16/24, 12/30/25 **Supersedes:**	**Approved By:** Chief of Network Business Operations **Authored By:** Chief of Network Business Operations **Reviewed By:** Chief Financial Officer, Director of Network Services, Public Policy & Continuing Education, Claims Processor(s)

Purpose:
Process to establish steps when a Network Provider requests an appeal from a claim payment denial.

Application:
Claims Processor(s)
Chief of Network Business Operations
Director of Network Services, Public Policy, Continuing Education, OBRA/PASARR and Enhanced Health Services
Chief Financial Officer

Policy:
It is the policy of SCCMHA to assure providers are paid for services rendered. Providers must submit clean claims timely for timely payment. Any claims denial has an appeal process that providers can follow. Please see SCCMHA policy Network Service Provider Appeals & Dispute Resolution 05.07.04.

Standards:

All SCCMHA service provider programs will be offered the same opportunities to resolve claim disputes and arrive at mutually agreeable outcomes with Saginaw County Community Mental Health Authority.

Definitions:
PRIMARY PROVIDER – for purposes of this procedure, is defined as a SCCMHA provider network service delivery program/integrated team (CSM, CSM-IDD, ACT, Wrap-around, Home-Based, School-Based Therapy, Therapy-Only, M2M Therapy, SUD-Only) that facilitates individual plans of services (IPOS) and requests their authorizations for medically necessary services outlined in IPOS. Separate service programs directly operated by SCCMHA are each considered program providers by each department or unit, and as such are members of the SCCMHA service provider network.

SECONDARY PROVIDERS – Provider programs which render additional supports and/or services, including residential, applied behavioral analysis, and other community support services for SCCMHA person served, as authorized by PRIMARY PROVIDER.

NON-PANEL PROVIDER – Any service provider without a current, signed provider participation agreement, such as for the purchase of emergency, DME, Out-of-State, or non-routine services needed by person served.

References:
SCCMHA --Network Service Provider Appeals and Dispute Resolution Policy 05.07.04

Exhibits:
None

Procedure:
1. When a SCCMHA service provider seeks to resolve a discrepancy regarding a denial of claim payment, the first step is for the Provider to submit a written communication to their assigned Claims Processor(s) requesting an appeal with detailed information outlining the claim number, date of service, and why they are requesting an appeal.

2. The Claims Processor(s) will review the written appeal and supporting documentation for recommendation to SCCMHA Chief of Network Business Operations.

3. The SCCMHA Chief of Network Business Operations will respond via written communication to the Provider as well as the assigned Claims Processor(s) in compliance with SCCMHA Network Service Provider Appeals and Dispute Resolution Policy 05.07.04.

4. If appeal/dispute is approved by Chief of Network Business Operations or Director of Network Services, Public Policy, Continuing Education, OBRA/PASARR and Enhanced Health Services

, the Claims Processor(s) will adjudicate the claim with as-needed overrides for payment and upload the appeal/override approval into the specific claim batch notes via PDF file format.

ACTION	RESPONSIBILITY
1. Service Provider to submit written appeal request identifying claim ID along with any supporting documentation to assigned Claims Processor(s)	Service Provider
2. Claims Processor(s) to review appeal and supporting documentation for recommendation to Chief of Network Business Operations	Claims Processor(s)
3. Will respond to Service Provider via written communication and will give copy of notification to the Claims Processor(s)	Chief of Network Business Operations or Director of Network Services, Public Policy, Continuing Education, OBRA/PASARR and Enhanced Health Services
4. Claims Processor(s) will adjudicate the claim with as-needed overrides for payment if approved.	Claims Processor(s)

Tab 8

Network Services

<table>
<tr><td colspan="3">Network Services Procedure Manual
Saginaw County Community Mental Health Authority</td></tr>
<tr><td>Subject: MDHHS Universal Credentialing for Licensed Clinical Staff</td><td>Chapter: Network Services- Credentialing</td><td>Subject No: 09.04.05.08</td></tr>
<tr><td colspan="3">Network Services & Public Policy</td></tr>
<tr><td rowspan="2">Effective Date: 10/1/2025</td><td>Date of Review/Revision:</td><td rowspan="2">Approved By:
Jennifer Keilitz, Director of Network Services, Public Policy, Continuing Education, OBRA/PASARR, & Enhanced Health Services

Authored By:
Melynda Schaefer and Cassandra Ward

Reviewed By:
Melynda Schaefer and Cassandra Ward</td></tr>
<tr><td>Supersedes:</td></tr>
</table>

Purpose: To ensure all Licensed staff can complete services and bill according to Medicaid guidelines. Licensed staff must be tracked in the Michigan Department of Health and Human Services, Behavioral Health Customer Relationship Management (MDHHS BH CRM/MiCAL) system to ensure the appropriate information is used for billing purposes.

Policy: It is the policy of the Saginaw County Community Mental Health Authority (SCCMHA) that all individuals providing care and treatment to persons with disabilities served by SCCMHA must be properly credentialed. In accordance with Public Act 282 of 2020, the Michigan Department of Health and Human Services (MDHHS) has established a uniform credentialing process for licensed and/or certified providers and practitioners. This process is implemented through the Behavioral Health Universal Credentialing – Customer Relationship Management (BH UC-CRM) system.

Application: This procedure applies to all service delivery program staff employed by the Saginaw County Community Mental Health Authority (SCCMHA) who hold either a limited or full professional license in the State of Michigan.

Standards: None

Definitions:
BH CRM: Behavioral Health Customer Relationship Management

MiCAL: Michigan Crisis and Access Line
Licensed Staff: An individual that holds an active license issued by the state of Michigan through the Department of Licensing and Regulatory Affairs (LARA).

References:
SCCMHA Procedure 09.04.03.01 Credentialing of SCCMHA Providers and Staff
SCCMHA Policy 05.06.03 Competency Requirements for the SCCMHA Provider Network
SCCMHA Policy 05.06.03.01 Credentialing and Recredentialing of SCCMHA Providers and Staff
SCCMHA Policy 05.06.03.03 Specialty Behavioral Health Credentialing & Supervision Requirements
Behavioral Health and Developmental Disabilities Administration, Provider Credentialing Universal_Credentialing_FAQs_-_11.2024.pdf

Exhibits A: Universal Credentialing Practitioner Guide

Procedure:

ACTION	RESPONSIBILITY
Board Operated: SCCMHA/Credentialing Coordinator gets notification from SCCMHA Human Resources of onboarding new licensed staff.	SCCMHA Human Resources Department
Notifies Senior Applications; Information Security and BI Administrator of new staff and requests access for them in the MDHHS BH CRM/MiCAL.	SCCMHA Credentialing Coordinator
Senior Applications; Information Security and BI Administrator sends SCCMHA's CEO the staff request and once approved, Senior Applications; Information Security and BI administrator grants access and sends confirmation email to SCCMHA Credentialing Coordinator of MDHHS BH CRM/MiCAL access upon completion.	SCCMHA Senior Applications; Information Security and BI Administrator, and SCCMHA CEO
SCCMHA Credentialing Coordinator sends licensed staff an email requesting creation of MiLogin for Business account to have access to the MDHHS BH CRM/MiCAL portal.	SCCMHA Credentialing Coordinator

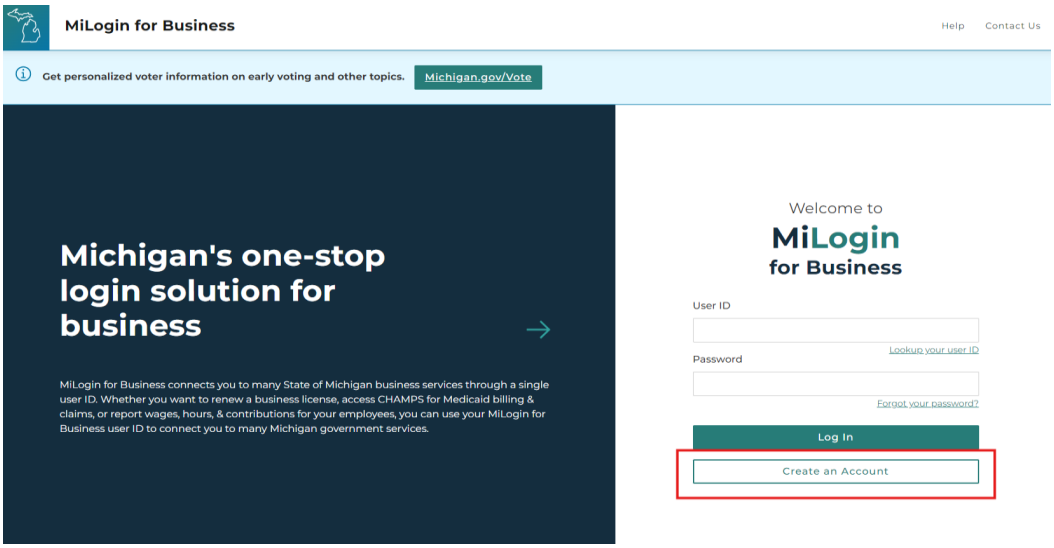
SCCMHA licensed staff creates MiLogin for Business account and adds MDHHS CRM/MiCAL online service. See exhibit A for details on this.	SCCMHA Licensed Staff
Creates Universal Credentialing Profile in the MDHHS BH CRM/MiCAL.	SCCMHA Credentialing Coordinator
MDHHS sends the licensed staff an email requesting them to complete their credentialing profile with a provided link.	MDHHS Automated Response
When applicable, Credentialing Coordinator schedules appointment with SCCMHA licensed staff to complete MDHHS CRM/MiCAL Universal Credentialing in person with primary source verification documents.	SCCMHA Credentialing Coordinator

Exhibit A:

Skip Steps 1 through 7 if you have an existing MiLogin account

Step 1

Navigate to the MiLogin Third Party portal located at https://MiLogintp.michigan.gov/. Click “Create an Account”.

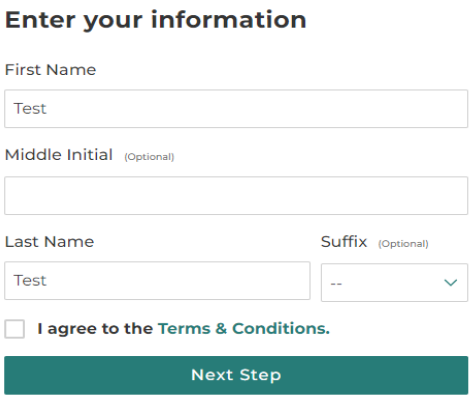


Step 2

1. Enter your SCCMHA email address.
2. The system will send a passcode to your email address
3. Enter the passcode, then click “Next Step”.

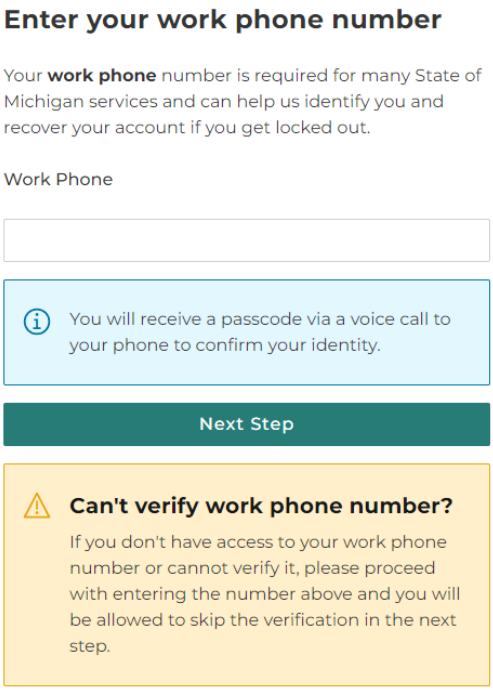
Step 3

On the following page, complete all required information then click “Next Step”.



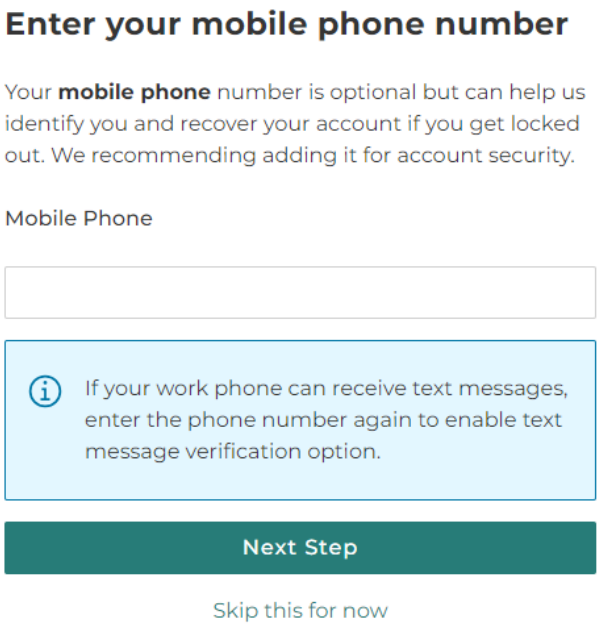
Step 4

Enter your work phone number. A passcode will be sent via voice call to confirm your identity. Enter the passcode, then click “Next Step”.



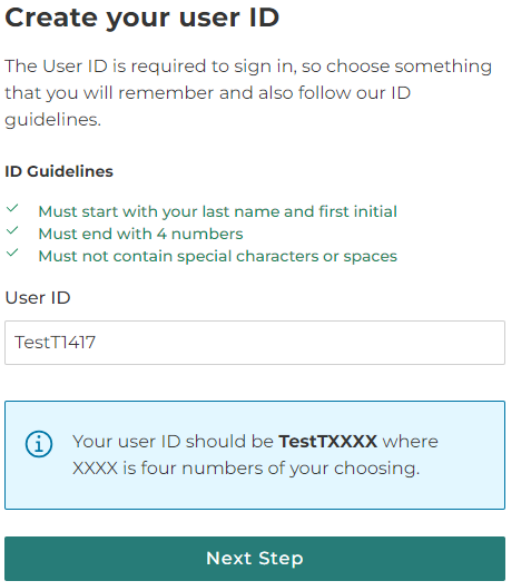
Step 5

*Optional
Enter your mobile phone number for additional account security in the event you are locked out.
Enter your mobile phone number and verify the passcode then click “Next Step”, or click “Skip this for now”.



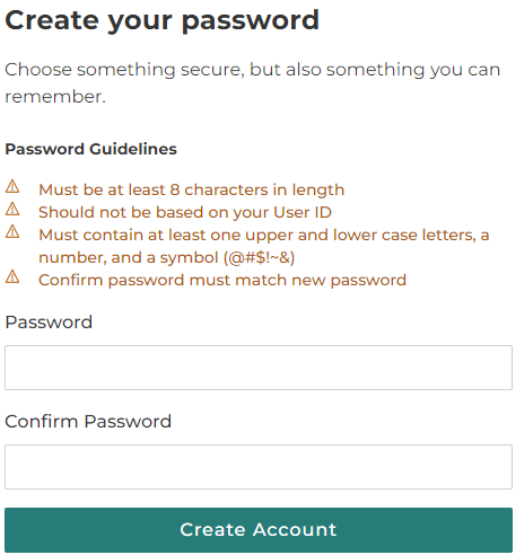
Step 6

Create your user ID following the stated guidelines.



Step 7

Create your password following the stated guidelines then click “Create Account”.

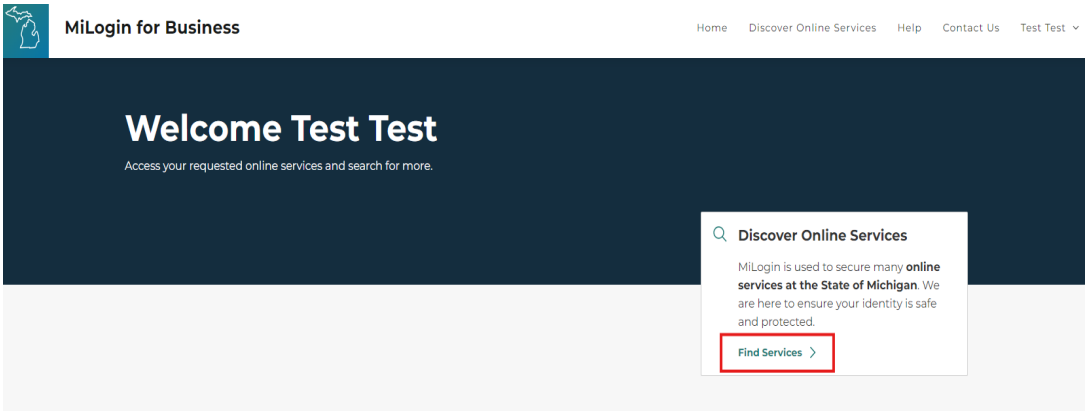


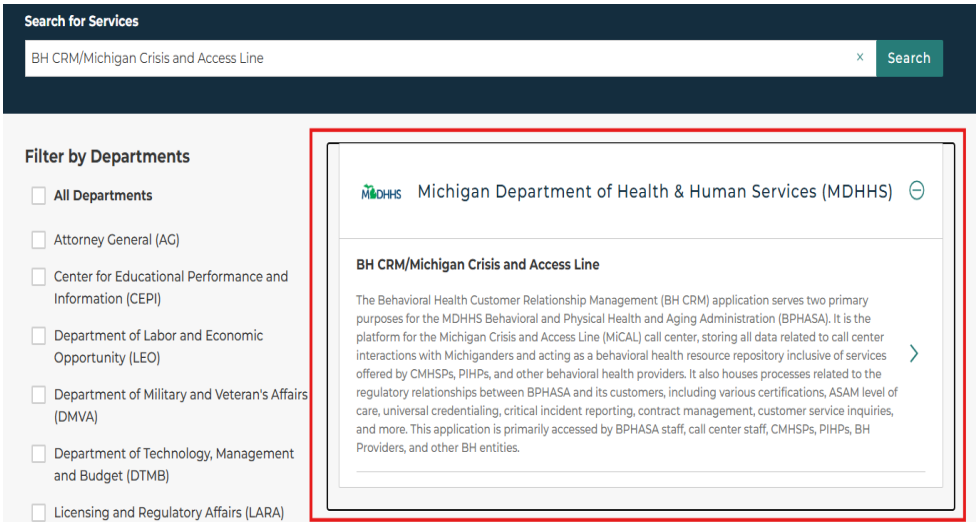
Step 8

User is directed to the MiLogin for Business: https://milogintp.michigan.gov/

Step 9

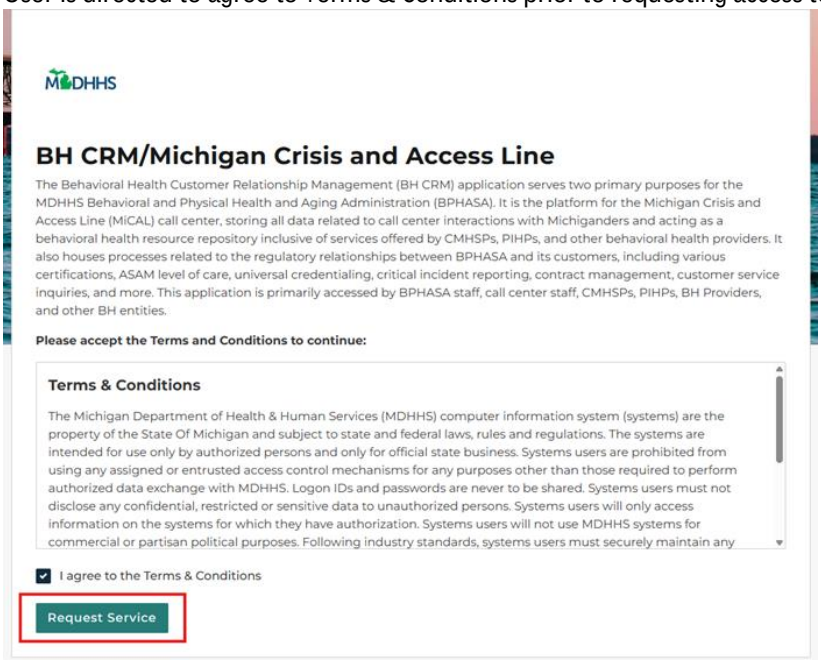
Click “Find Services” and enter ‘**BH CRM/Michigan Crisis and Access Line**’ in the search application. The application will appear in the drop-down menu. Click on the ‘**BH CRM/Michigan Crisis and Access Line**’ that appears to the bottom right of the search bar. This will give you access to the **Live Environment**.





Step 10

User is directed to agree to Terms & Conditions prior to requesting access to the service.



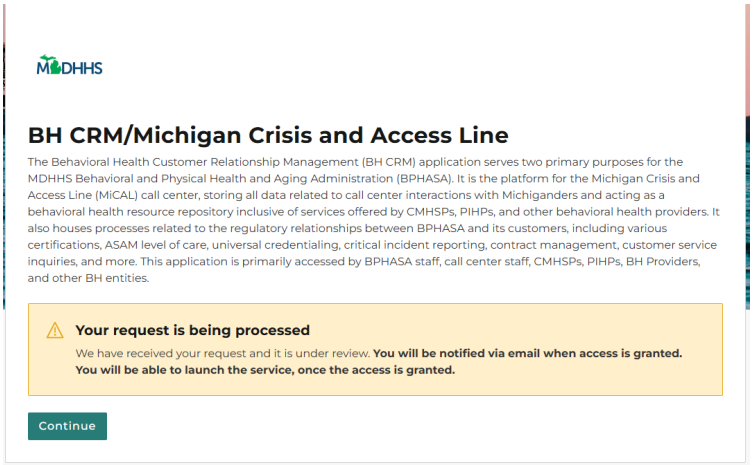
Step 11

User will be notified that your request is being processed. The MDHHS Behavioral Health CRM team will then receive your access request and either approve or reject the request.

Requests are rejected for the following reasons:

- User did not register MiLogin account with an agency email address
- User was not added to agency contact list prior to requesting access

- Email address used to request access does not match the email address listed in the system



Step 12

Once the request is approved, user will receive a notification email. User will also receive a notification email in the event that the request is rejected. Rejection emails will state why the request was not approved.

Step 13

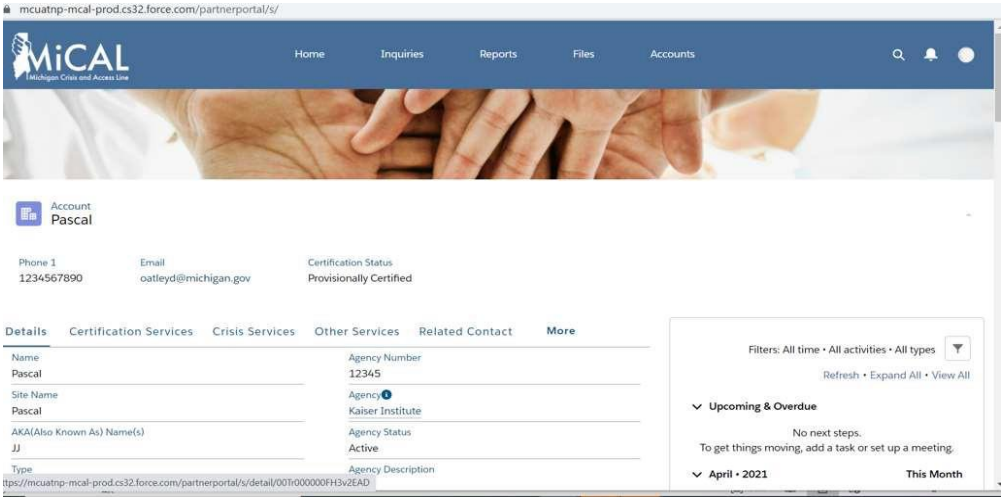
Use your login credentials to access MiLogin for Business: https://MiLogintp.michigan.gov/.

Step 14

From your Account Home Page, click on the link to access the Michigan Crisis and Access Line. Acknowledge the Terms & Conditions and complete the Multi-Factor Authentication (MFA)

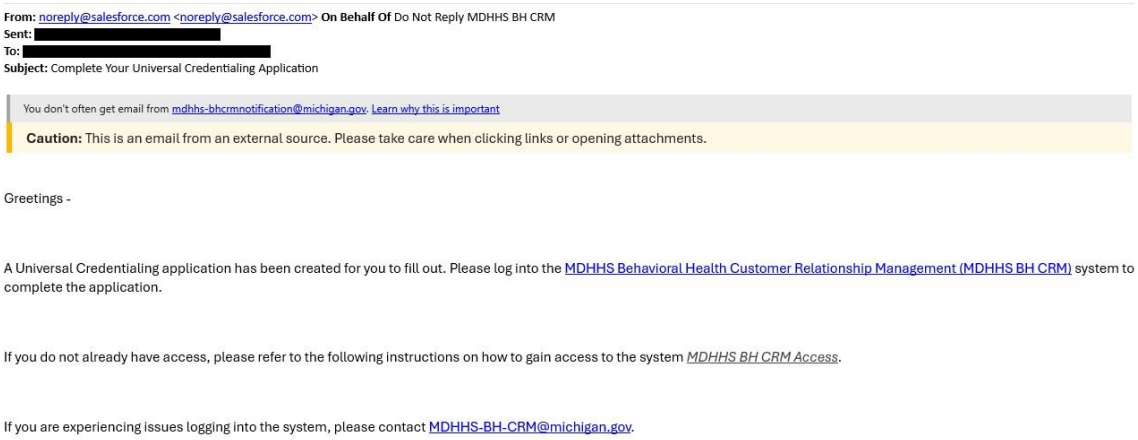
Step 15

The MDHHS BH CRM home page will automatically appear in a new tab.



MDHHS Universal Credentialing Guide
Complete and Submit Application – Practitioner Guide

1. Follow the link from noreply@salesforce.com on behalf of MDHHS BH CRM.



From: noreply@salesforce.com <noreply@salesforce.com> **On Behalf Of** Do Not Reply MDHHS BH CRM
Sent: [redacted]
To: [redacted]
Subject: Complete Your Universal Credentialing Application

You don't often get email from mdhhs-bhcrmnotification@michigan.gov. Learn why this is important

Caution: This is an email from an external source. Please take care when clicking links or opening attachments.

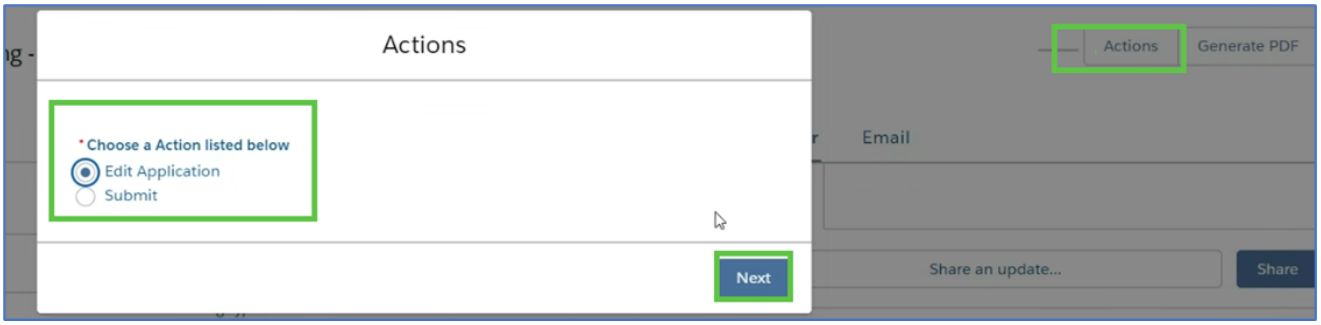
Greetings -

A Universal Credentialing application has been created for you to fill out. Please log into the MDHHS Behavioral Health Customer Relationship Management (MDHHS BH CRM) system to complete the application.

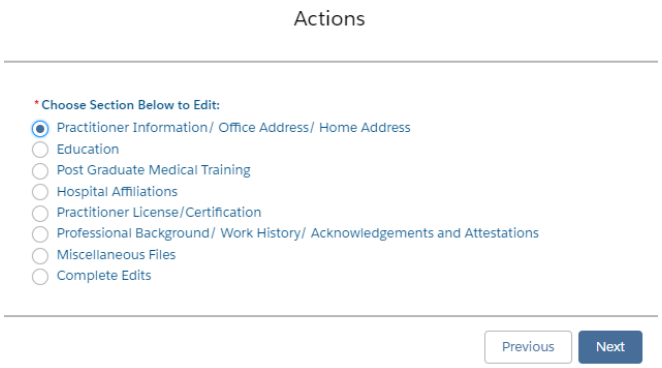
If you do not already have access, please refer to the following instructions on how to gain access to the system *MDHHS BH CRM Access*.

If you are experiencing issues logging into the system, please contact MDHHS-BH-CRM@michigan.gov.

2. Login to your MiLogin for Business account and proceed to BH CRM/Michigan Crisis and Access Line.
3. From the 'Home' page, select "Credentialing Profile" from the top of the screen. Select your "Credentialing Profile Name."
4. Select "Actions" in the top right corner of your profile, select "Edit Application" and click "Next."

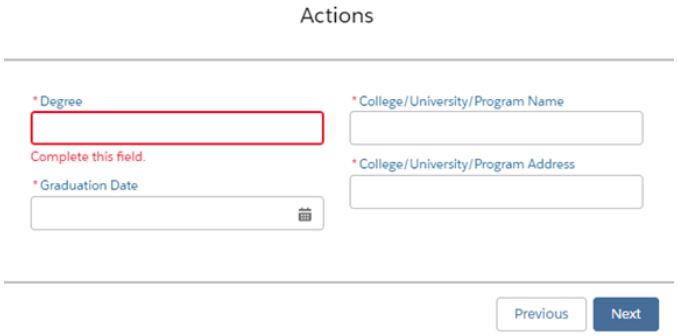


5. Choose a section to edit, starting with "Practitioner Information/Office Address/Home Address" by selecting the circle to the left of the sections name and clicking "Next".



***Please note: Only one selection can be completed at a time. Sections can be completed in any desired order. All sections that apply to your specialty must be completed prior to submission.**

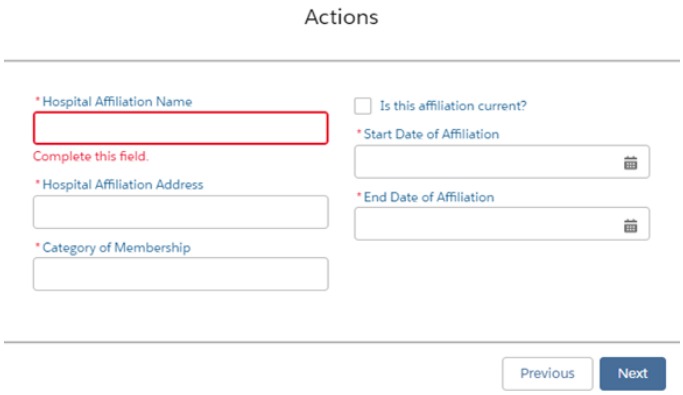
6. Complete all required information within the section. Required information is indicated by a red asterisk. Then, click "Next".
7. Select "Education" section, then click "Next". Select "Add New Record", then click "Next" and complete all required fields.



8. Once complete, select "Continue to Options Screen" and click "Next". Select "Post Graduate Medical Training" section, then click "Next". Select "Add New Record", then click "Next". Complete all required fields.

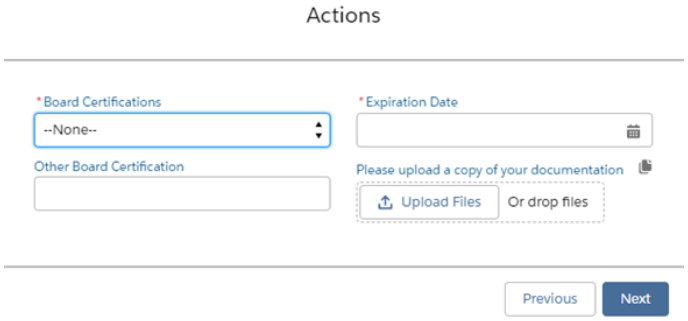
9. Once complete, select "Continue to Options Screen" and click "Next". Select "Hospital Affiliations" section, then click "Next". Select "Add New Record", then click "Next". Complete

all required fields. If affiliation is current, check the box to ensure “End Date of Affiliation” is not required.

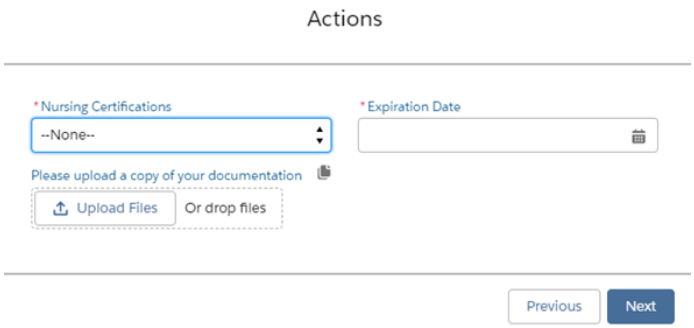


10. Once complete, select “Continue to Options Screen” and click “Next”. Select “Practitioner License/Certification” section, then click “Next”. Select “Add New Record”, then click “Next”. Complete all required fields that apply.

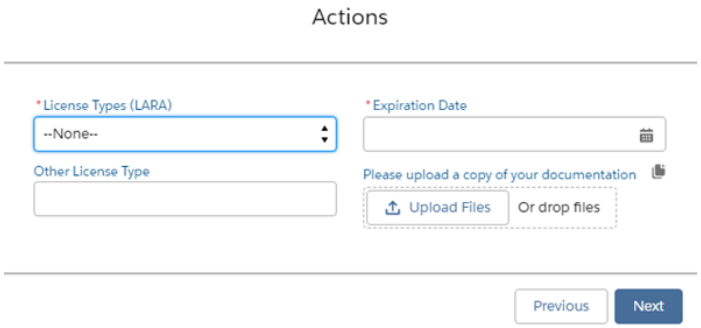
For Certification, complete all required fields, then click “Next”.



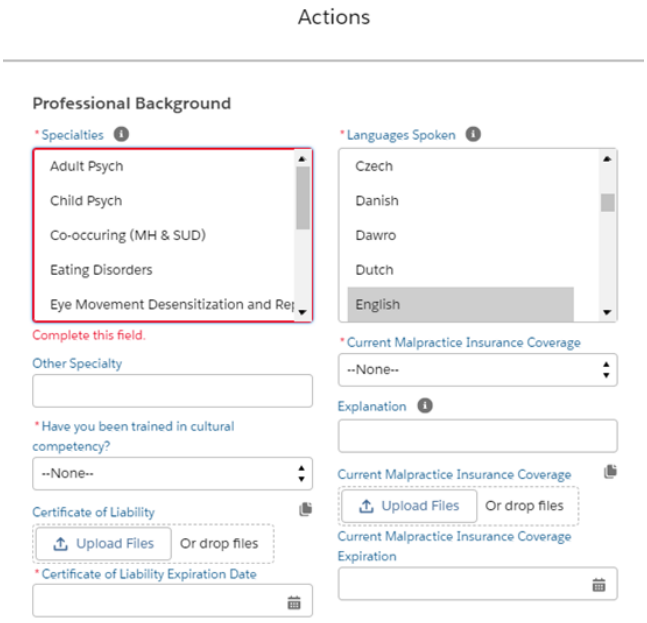
For Nursing Certification, complete all required fields, then click "Next”.

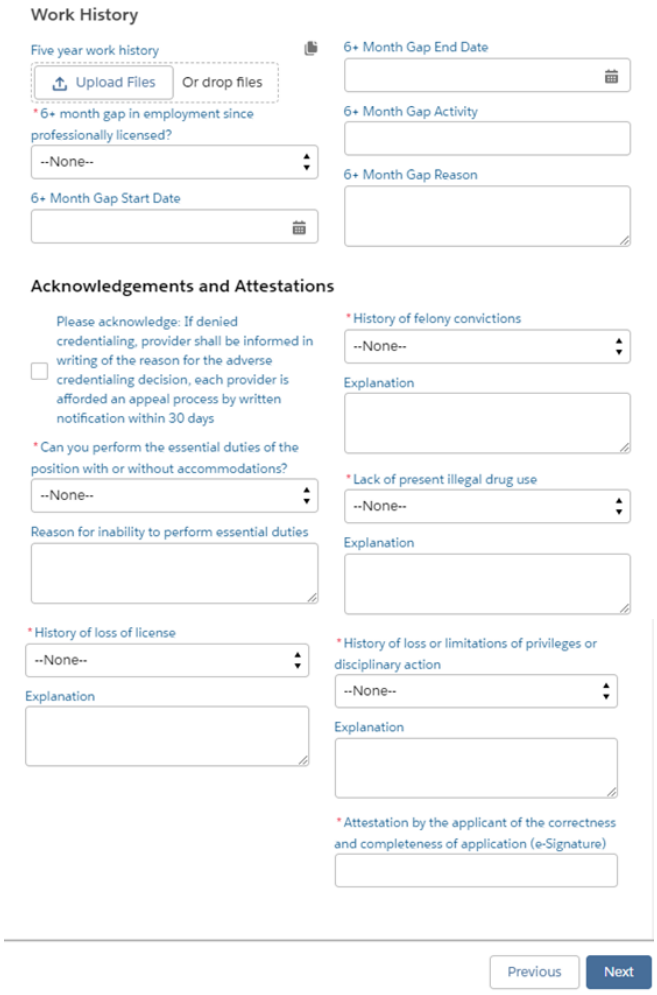


For License, complete all required fields, then click “Next”.

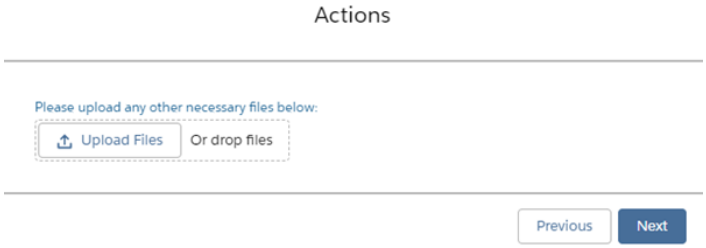


11. Once complete, select “Continue to Options Screen” and click “Next”. Select “Professional Background/Work History/Acknowledgements and Attestations” section, then click “Next”.





If there are additional files to upload, select “Miscellaneous Files”, then click “Next”. You may upload as many files as necessary via the file upload box, then click "Next”.



12. Once completed, select “Complete Edits” and click “Next”. You will be directed to the main Credentialing Profile screen where all completed information will display in the respective section. Please review all information for accuracy.
13. Select “Actions” from the top right corner of the profile. Select “Submit” and click “Next”.

14. Select “Yes” to consent to the provided statement, then click “Next”. (If “No” is selected, you will be directed back to the Credentialing Profile.)
15. Consent box will display “Your Universal Credentialing application has been submitted successfully”.