

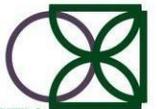


The SCCMHA
COMPLIANCE PROGRAM
AND
False Claims Information
2023

**The Following
Presentation
Consists of Two Trainings:**

**1. Compliance Program and
False Claims (Slides 2-36)**

**2. Healthcare Privacy at SCCMHA
(Slides 37-115)**



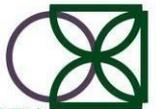
SAGINAW COUNTY
COMMUNITY MENTAL
HEALTH AUTHORITY

Special Note for those employed in a Self Determination arrangement

- *Your employment in a Self Determination arrangement is made possible through the use of Medicaid funding.*
- *Medicaid funds originate from SCCMHA and our training requirement source: Mid-State Health Network.*

Purpose of SCCMHA Compliance Program and False Claims Policy

- SCCMHA has a formal commitment to aid in preventing, detecting, investigating, and reporting potential fraud and abuse occurrences.
- SCCMHA's intention is to minimize the possibility of improper conduct by SCCMHA, its employees and contractual providers.



SCCMHA Compliance Staff

- SCCMHA Chief Compliance Officer

AmyLou Douglas

797-3506



At the completion of this training

- You will have a working knowledge of the SCCMHA Compliance Program as well as federal and Michigan laws impacting health care.
- You will have an increased understanding of your role in safeguarding Medicaid funding.
- You will be able to identify resources available to assist you in this role.
- You should use this presentation as a resource if you have questions later in the year.

Why?

Why do we need to know about and understand these regulations, including the federal and Michigan False Claims Acts?



Rising Health Care Costs

Every dollar lost to fraud, waste or abuse is one less dollar available for consumer services.





(1) Center for Medicare and Medicaid Services (CMS)

1. FEDERAL. CMS provides operational direction and policy guidance to the States and to healthcare providers.

(2) State of Michigan (MDHHS)

2. STATE. The Michigan Department of Health and Human Services (MDHHS) oversees the administration of the Medicaid Program for Michigan.

Overview of Medicaid Program Administration for Behavioral Health Services

The Medicaid Program is funded by both the federal and state governments, and is directly administered by the States with approval and oversight by CMS.

3. REGIONAL. MDHHS contracts with Prepaid Inpatient Health Plans (PIHPS) to manage Behavioral Health benefits (mental health and substance use disorder) in 10 regions across Michigan.

Shiawassee

Saginaw

BABH

Tuscola

Newaygo

Lifeways

GIHN

CMHCM

MCN

Huron

CEI CMH

Right Door

SUD Providers

(3) Mid State Health Network (MSHN)

(4)

(5) Local Service Providers

4. COUNTY. MSHN contracts with SUD Providers and with each of the CMHSPs in Region 5 to provide Mental Health and SUD services to Region 5 customers.

5. LOCAL. Each CMHSP contracts with various service providers to provide mental health services to the customers located in that CMHSP's county.



What is Compliance? Doing the Right Thing!

- **What does this look like in an ORGANIZATION'S BEHAVIOR?**
 - A formal program specifying an organization's policies, procedures, and actions within a process to help prevent and detect violations of laws and regulations.
 - However, Compliance is MORE than a program within an organization, it is an organization-wide philosophy that guides decision-making processes.
- **What does this look like in INDIVIDUAL BEHAVIOR?**
 - Following laws and rules that govern healthcare;
 - Being honest, responsible, and ethical;
 - Preventing, detecting, and reporting unethical and illegal conduct;
 - Preventing, detecting, and reporting Fraud, Waste, and Abuse (FWA) of Federal and/or State funds.

The Seven Elements of an Effective Compliance Program

1. Implementing written policies, procedures, and standards of conduct
Code of Conduct; Corporate Compliance Plan; Policies & Procedures
2. Designating a compliance officer and compliance committee
Compliance Officer (Rich Garpiel); Compliance Oversight Committee
3. Conducting effective training and education
Initial training at hire, annual reviews, as needed
4. Developing effective lines of communication
Open-door policy to Compliance Officer; Anonymous reporting; Whistleblower protections
5. Conducting internal monitoring and auditing
Annual FY Compliance Review and Monitoring; Provider Network Reviews
6. Enforcing standards through well-publicized disciplinary guidelines
Contained in Employee Handbook, Code of Conduct, Corporate Compliance Plan, and Policies & Procedures
7. Responding promptly to detected offenses and undertaking corrective action
All reports of wrongdoing will be promptly and confidentially investigated, and appropriate remedial action taken (can include Corrective Action Plans, repayments, notification to outside government agencies, training, etc.).

SCCMHA STANDARDS OF CONDUCT

This Slide represents a Summary –
Please refer to the SCCMHA Employee Handbook for additional information

Code of Conduct

- Confidentiality: Protect the privacy of those we serve
- Alcohol & drug free environment
- Free of harassment of any kind
- Avoidance of conflict of interest
- Report any suspected or actual Fraud, Waste and Abuse
- Do not solicit or accept gifts
- Safe, respectful work environment: all employees will be treated with dignity and respect
- Political contributions will not be made with agency funds or resources

Ethics

- ☐ Carefully read and understand the Code of Ethics associated with your professional license (MSW, LLP, LPC, etc. all have a different Code of Ethics)
- ☐ Establish and maintain healthy boundaries with consumers, families, and colleagues
- ☐ Avoid using your workplace as a way to promote personal interests or paid endeavors
- ☐ Immediately warn if a consumer discloses intent to harm self or others
- ☐ Ensure continuity of treatment and services (transfer and discharge responsibilities)
- ☐ Avoid sexual impropriety
- ☐ Adequately document services/billings/communications
- ☐ Treatment should be suitable to condition (amount, scope, duration matches the need)



INTERSECTION OF COMPLIANCE AND ETHICS

Organizational Ethics

What is the role of compliance when it comes to ethics?

Compliance supports the organization toward an ethical culture. The OIG Compliance Guidelines state that one purpose of a compliance program is to, “..increase the likelihood of preventing, identifying, and correcting unlawful and unethical behavior at an early stage”

What does this look like?

Establishing policies, procedures, and business processes that support and encourage employees to act in conformity with the organization’s values. Examples include a Code of Conduct, and other standards that encourage transparency and open communication.

Which of the following are actual or potential Conflicts of Interest that should be reported to your supervisor or HR?

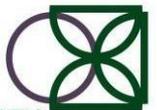
1. You accepted paid outside employment at a contracted provider of SCCMHA, but it is only part-time and will not interfere with your normal work schedule for SCCMHA.
2. Your spouse works for a vendor that is seeking to contract with SCCMHA.
3. Your job at SCCMHA includes referring consumers to providers and your daughter works at a provider organization.
4. You are completing a Master's Degree Program and are performing your internship at a provider of SCCMHA.

ALL OF THE ABOVE!! Actual, potential, and even the appearance of a Conflict of Interest should be disclosed to your supervisor or HR. This supports transparency and integrity at SCCMHA.



If you, a beneficiary, or SCCMHA cause or allow the misuse of Medicaid funds - -
each of you, a beneficiary, or SCCMHA could be exposed to:

- Federal criminal prosecution
 - State criminal prosecution
 - Federal civil prosecution
 - State civil prosecution
 - Federal administrative civil penalties
- ❖ **NOTE: Medicaid fraud can be committed by an Employer, Employee, or Beneficiary.**

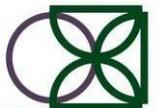


Laws Impacting Healthcare

Deficit Reduction Act (DRA) 2005

- The DRA requires education and training for employees, contractors and agents that contains detailed information about the Federal False Claims Acts, whistleblower provisions, and information about preventing and detecting Fraud, Waste, and Abuse in the Federal health care programs.
- The DRA requires written policies that include detailed provisions consistent with State and Federal False Claims Acts, whistleblower provisions, and other applicable laws.
- Employee Handbook includes reference to State and Federal laws, rights of employees to be protected as Whistleblowers, and related policies and procedures

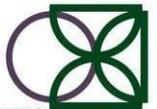
The DRA is about Education, Written Standards, and creating increased joint oversight between Federal and State governments



Laws Impacting Healthcare

FEDERAL FALSE CLAIMS ACT (FCA)

- The False Claims Act is a federal statute that covers fraud involving any federally funded contract or program, including the Medicaid program.
- The FCA establishes civil liability for certain acts, including:
 - Knowingly presenting a false or fraudulent claim to the government for payment;
 - Knowingly making, using, or causing to be made or used, a false record or statement to get a false or fraudulent claim paid or approved;
 - Conspiring to defraud by getting a false or fraudulent claim allowed or paid;
 - Knowingly making, using, or causing to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the government.
- **“Knowingly”** means:
 - Actual knowledge of the information;
 - Acting in deliberate ignorance of the truth or falsity of the information; or
 - Acting in reckless disregard of the truth or falsity of the information.
 - ****No proof of specific intent to defraud is required!!****



Laws Impacting Healthcare

Federal False Claims Act

- Examples:
 - Up-coding
 - Billing for unnecessary services or billing twice for the same service
 - Billing for services or items that were not provided
 - Billing for items or services performed by an excluded individual
 - Failing to repay overpayments within 60 days of identification
 - Substantiated violations of other health care laws
- Penalties:
 - Civil monetary penalties ranging from **\$5,500 to \$11,000** for EACH false claim;
 - Treble damages – **three times the amount of damages** incurred by the federal government related to the fraudulent or abusive conduct;
 - Exclusion from participation in State and Federal programs;
 - Federal criminal enforcement for intentional participation in the submission of a false claim.
 - Penalties provided for under other health care laws that were violated.



Laws Impacting Healthcare

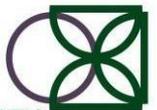
FEDERAL FALSE CLAIMS ACT



Scenario: Consumer Sally was scheduled for 60 minutes of psychotherapy with Dr. Smith. Sally arrived for her appointment extremely upset and in crisis. The receptionist immediately contacted an ambulance. While waiting for the ambulance, Sally never left the waiting room. Dr. Smith interacted with Sally for approximately 5 minutes until the ambulance arrived and transported her to a nearby hospital.

Dr. Smith had 60 minutes scheduled for Sally B. and was unable to schedule other consumers during that time block. He saw Sally, even if it was for only 5 minutes. Dr. Smith submitted a claim for Sally's visit, for 60 minutes of psychotherapy. The claim was paid out of Medicaid.

A month later, as part of a routine Medicaid Services Verification audit, Sally's claim was selected as part of the audit sample. When auditors contacted Dr. Smith's office to obtain documentation to support the service billed, Dr. Smith instructed his receptionist (the one who called the ambulance) to create a Progress Note for 60 minutes of Psychotherapy, furnished to Sally on the day she went to the hospital. The receptionist created the note, Dr. Smith signed it and dated it the day Sally went to the hospital, and the Progress Note was provided to the auditors to support the service billed.



Laws Impacting Healthcare

FEDERAL FALSE CLAIMS ACT

- **Problems identified on the previous slide:**
 - A claim was submitted to Medicaid for a 60 minute psychotherapy service when Dr. Smith only saw Sally for only 5 minutes.
 - Appears to be intentional – fraud
 - Dr. Smith instructed receptionist to create Progress note for 60 minutes for an audit.
 - Documenting a service not provided; intentional – fraud
 - Receptionist created a note and Dr. Smith, signed and back dated it. Receptionist and Dr. intentionally created, signed and presented note to auditors to support a service that was not provided but billed.
 - Falsifying documentation for payment; intentional by both the receptionist and Doctor – fraud.

Laws Impacting Healthcare

MICHIGAN FALSE CLAIMS ACT

- The Michigan False Claims Act mirrors the Federal False Claims Act, with an expanded definition of “knowledge”
- MCL 400.602
 - “Knowing” and “knowingly” means that a person is in possession of facts under which he or she is aware or should be aware of the nature of his or her conduct and that his or her conduct is substantially certain to cause the payment of a Medicaid benefit. Knowing or knowingly includes acting in deliberate ignorance of the truth or falsity of facts or acting in reckless disregard of the truth or falsity of facts. Proof of specific intent to defraud is not required. (Emphasis added)
 - Michigan allows for constructive knowledge. This means that if the conduct “reflects a systematic or persistent tendency to cause inaccuracies” then the conduct may be fraud, rather than simply a good faith error or mistake.

Laws Impacting Healthcare

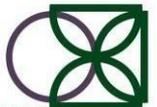
OTHER APPLICABLE LAWS

Anti-Kickback Statute [42 USC § 1320a-7b(b)]

- Health care providers and suppliers MAY NOT offer, pay, solicit or receive anything of value in exchange for the referral of patients or services covered by Medicaid or Medicare.
- Fines can include up to \$25,000 per violation and up to 5 years in prison per violation

Exclusion Authorities (Federal and State)

- Providers must ensure that no Federal Funds are used to pay for any items or services furnished by an individual who is debarred, suspended or otherwise excluded from participation in any federal health care program. This includes salary, benefits, and services furnished, prescribed, or ordered.
 - Federal exclusions are imposed under the Social Security Act, 42 USC § 1320a-7. They are **mandatory** and **permissive**.
 - Examples of **mandatory exclusions** are: conviction of a crime relating to patient neglect or abuse, felony conviction of health care fraud, etc.
 - Conviction of program related crimes
 - Conviction relating to patient abuse
 - Felony conviction related to health care fraud
 - Felony conviction related to controlled substance
 - Examples of **permissive exclusions** are: misdemeanor conviction relating to health care fraud, conviction relating to fraud in a non-health care program, etc.



Laws Impacting Healthcare

OTHER APPLICABLE LAWS

- **Examples of Permissive Exclusions: (this is not an exhaustive list)**
 - Conviction relating to fraud
 - Conviction relating to obstruction of an investigation or audit
 - Misdemeanor conviction relating to controlled substance
 - License revocation or suspension
 - Exclusion or suspension under Federal or State health care program
 - Claims for excessive charges or unnecessary services and failure of certain organizations to furnish medically necessary services

- <https://exclusions.oig.hhs.gov/> is the link to the federal exclusions database. The federal list is commonly referred to as the LEIE – ‘List of Excluded Individuals and Entities’. Anyone who hires an individual or entity on the LEIE may be subject to civil monetary penalties.

- <https://oig.hhs.gov/exclusions/> - this link explains all the information on the federal Exclusions website.

- **Michigan:**
 - Social Welfare Act, MCL 400.111a-f

Laws Impacting Healthcare

OTHER APPLICABLE LAWS

Civil Monetary Penalties Law (42 USC § 1320a – Federal)

- Allows the Office of the Inspector General (OIG) to impose civil penalties (MONEY) for violations of the Anti-Kickback Statute and other violations including submitting false claims and making false statements on applications or contracts to participate in a Federal health care program

Criminal Health Care Fraud Statute (18 USC 1347 - Federal)

- Makes it a criminal offense to knowingly and willfully execute a scheme to defraud a health care benefit program. Health care fraud is punishable by imprisonment of up to 10 years, and fines of up to \$250,000. Specific intent is not required for conviction.
- With respect to violations of this statute, a person does not need to have actual knowledge of this section or specific intent to commit a violation of this section

Stark Law

- U.S. federal laws that prohibit physician “self-referral”, specifically, a physician may not refer a Medicare or Medicaid patient to an entity providing designated health services (“DHS”) if the physician or an immediate family member of the physician has a financial relationship with that entity.

Laws Impacting Healthcare

WHISTLEBLOWER PROTECTION

- **Federal Statute**

- Federal Whistleblower protection is designed to protect against the fraudulent use of public funds by encouraging people with knowledge of fraud against the Government to “blow the whistle” on wrongdoers.
- Individuals can file a “Qui tam” lawsuit on behalf of the government. This law provides for a reward in the form of a share of the recovery.
- Anyone initiating a qui tam case may not be discriminated or retaliated against in any manner by their employer. The employee is authorized under the False Claims Act to initiate court proceedings to make themselves whole for any job-related losses resulting from any such discrimination or retaliation.

- **Michigan Statute**

- Michigan also provides protection for employees who report a violation or suspected violation of a State or Federal law, rule, or regulation to a public body; unless the employee knows the report is false.
- Employers may not discharge, threaten, or otherwise discriminate against an employee regarding the employee’s compensations, terms, conditions, location, or privileges of employment.

Laws Impacting Healthcare

Offering to pay someone to make referrals to your entity, or accepting payment for making referrals violates what law?

Placing an employee on a corrective action plan because they reported suspected fraud occurring within the agency would be a violation of this law.

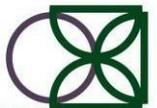
Using federal funds to pay the salary and benefits of a person who is barred from participating in Medicare and Medicaid would violate this law.

Identifying that your provider has received an overpayment, but failing to repay that overpayment amount within 60 days of quantifying the amount violates what law?

Increased Federal resources to fight Medicaid fraud, waste, and abuse.

Match the Definitions (on the left) with the Law (on the right)

- Federal False Claims Act
- Whistleblowers Protection Act
- Anti-kickback Statute
- Exclusion Authorities
- Deficit Reduction Act



FRAUD, WASTE, & ABUSE

FRAUD

Fraud is an intentional deception or misrepresentation by a person with the knowledge the deception could result in unauthorized benefit to him/herself or some other person. This includes any act that constitutes fraud under applicable Federal or State laws.

Fraud can include billing for services that were not rendered, performing medically unnecessary services solely to obtain payment, altering documentation to obtain higher payment (upcoding), and deliberate duplicate billing.

Example

Dr. Smith's submission of a claim for a service not rendered, and creation of a fake progress note to support that claim.

FRAUD, WASTE, & ABUSE

WASTE

Waste is an overutilization of services, or other practices that result in unnecessary costs. Waste is not generally considered to be caused by criminally negligent actions, but rather the misuse of resources.

Waste can include healthcare spending that can be eliminated without reducing the quality of care or causing redundant testing

EXAMPLE

A consumer received an Assessment from Provider X last month. There has been no significant change in Consumer's condition, nor any change in the treatment being delivered. Provider X performs another Assessment and submits a claim for payment.

FRAUD, WASTE, & ABUSE

ABUSE

Abuse are practices that are inconsistent with sound fiscal, business or medical practices & result in an unnecessary cost to the payor, or in reimbursement for services that are not medically necessary or fail to meet professionally recognized standards for healthcare.

Abuse can include the submission of claims that do not comply with billing guidelines, providing services that are not medically necessary or do not meet professionally recognized standards, submitting bills to Medicare/Medicaid instead of the primary insurer.

CAUTION – Abuse can develop into Fraud if there is evidence that the individual knowingly and willfully (on purpose) conducted the abusive practices.

EXAMPLE of an Abuse that could develop into Fraud

Provider X has multiple sites and decided that billing is easier if all claims are submitted listing a single location of service and a single clinician associated with that location of service, rather than the claims reflecting the clinician who actually furnished the service, and the location where it was actually furnished.



Service Documentation Requirements

Michigan Medicaid Provider Manual requirements (non-exhaustive list) (Medicaid Provider Manual Section 15: Record Keeping)

- The clinical record must be sufficiently detailed to allow reconstruction of what transpired for each service billed.
- All documentation must be signed and dated by the rendering health care professional
 - Documentation, including signatures, must be legible
 - If a signature is not legible, the clinician's name and credentials should be printed below
- For services that are time-specific according to the procedure code billed, providers must indicate in the medical record the actual begin time and end time of the particular service
- Progress notes must include the following:
 - Goal(s) and/or Objective(s) of the Plan of Service addressed
 - Progress/lack thereof toward desired outcome



WHO TO CONTACT IF YOU HAVE A CONCERN

- If you, as an SCCMHA employee, contractor, or agent becomes aware of any type of concern regarding the False Claims Act, it is recommended that the matter be referred to the **SCCMHA Compliance Officer**, for review and investigation:

The SCCMHA Compliance Officer, AmyLou Douglas, can be reached at: 989-797-3574 or
Toll Free Hotline - 855-797-3417

SCCMHA has a NO RETALIATION policy

WHO TO CONTACT IF YOU HAVE A CONCERN

- If you are involved with Fiscal Intermediary/Self Determination many resources are available which may be used to report a concern:
 1. The Management Chain of Command – If an employee suspects that another employee (including those in management positions) or other party has violated the Code of Ethics, company policies and procedures, or any applicable local, state or federal statute, regulation, guideline or law, the employee should immediately report that concern through the chain of command.
 2. If you know or have a good faith suspicion that fraud or misconduct relating to Medicare or Medicaid has been committed, please contact the SCCMHA Hotline:
Local Number: 989-797-3574 or
Toll-Free Hotline: 855-797-3417
 3. SCCMHA has a NO RETALIATION policy

WHO TO CONTACT IF YOU HAVE A CONCERN

Contact the Compliance Officer – If an individual does not feel comfortable reporting a compliance concern to their supervisor, they may contact the Compliance Officer. The Compliance Officer will research the matter while preserving confidentiality to the extent possible and permitted by law.

WHO TO CONTACT IF YOU HAVE A CONCERN

- SCCMHA maintains an environment that promotes ongoing, open communication among employees, contractors, and agents.
- SCCMHA encourages employees, contractors, and agents to communicate directly about any compliance issue or other matters of concern without the fear of retaliation or intimidation.
- SCCMHA does not tolerate retaliation or intimidation against anyone for reporting a perceived or potential violation of the Federal or State FCA.
- Furthermore, SCCMHA does not tolerate retaliation or intimidation against anyone for participating in the investigation of an alleged violation. Anyone who engages in retaliatory, or intimidation actions will be disciplined, up to and including termination.

REVIEW: The False Claims Act

The False Claims Act is a major factor in combating contractor fraud and recovering losses due to Medicare and Medicaid fraud.

If you suspect Medicaid Fraud or Abuse

Call the SCCMHA Hotline

797 – 3574



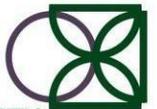
1-855-797-3417



Healthcare Privacy at SCCMHA

Privacy Regulations:

- HIPAA (Privacy & Security)
 - 42 CFR Part 2
- Michigan Mental Health Code
 - Michigan HIV Laws



SAGINAW COUNTY
COMMUNITY MENTAL
HEALTH AUTHORITY

Special Note for those employed in a Self Determination arrangement

- *Your employment in a Self Determination arrangement is made possible through the use of Medicaid funding.*
- *Medicaid funds originate from SCCMHA and our training requirement source: Mid-State Health Network.*

Protecting Consumer Privacy

- The privacy of SCCMHA consumers, (including their records), are protected by several federal and state laws and regulations – These protections continue even after the consumer no longer receives services from SCCMHA or is no longer alive.
- While you may not have to be an expert in each of these laws – you do need to understand and follow the essential parts of them.

- You need to recognize



a Red Flag

What is a Red Flag?



- A red flag is a
 - Pattern,
 - Practice,
 - Or a specific activity that could indicate a violation of compliance rules, including Privacy rules, may have occurred.
- You are expected to understand the various rules well enough so if you sense that something is not right – you see a red flag in your mind and recognize a potential problem.
- You should then contact your supervisor or the Compliance Office Hotline to resolve the potential problem.



**Do you have a
Compliance
Question?**



**SCCMHA Compliance
989-797-3574
Or
- Toll free -
855-797-3417**



HIPAA

Key Concepts

- Covered Entity (CE)
- Health Information
- Individually Identifiable Information
- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)



HIPAA

Key Definitions

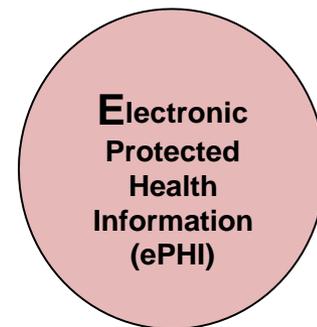
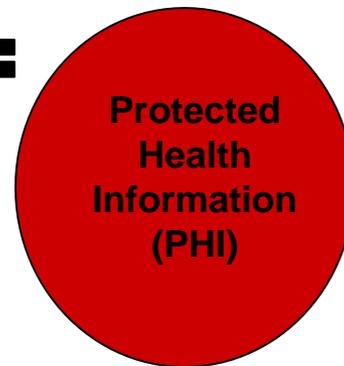
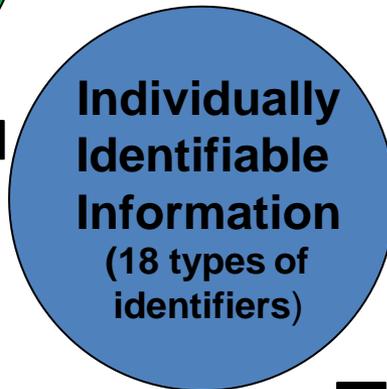
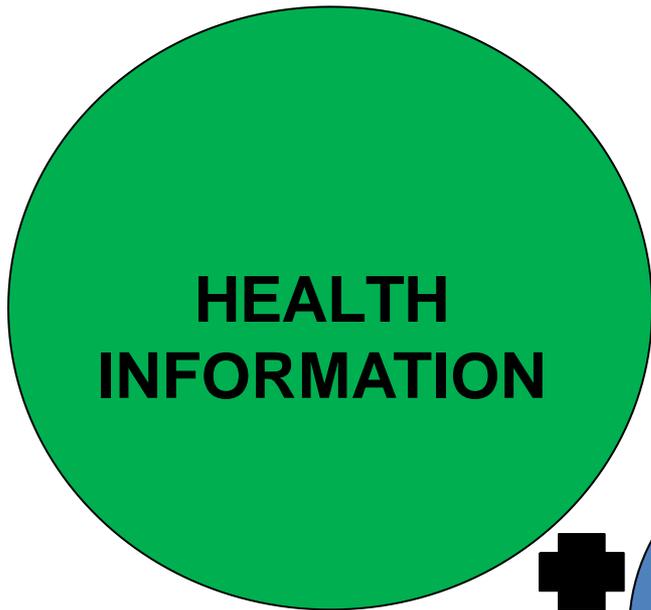
- **Covered Entity (CE)**
 - Health Care Providers; for example –
 - SCCMHA
 - Healthcare providers that contract with SCCMHA
 - Physicians, Nurses
 - Health Care Insurers; for example –
 - Blue Cross
 - Medicaid
 - Health Care Clearinghouses

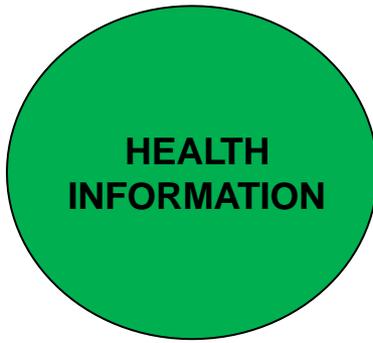
ALL Covered Entities Have a Duty to Protect PHI

A “covered entity” is:

- any person or organization
- that furnishes, bills or is paid for health care services
- in the normal course of business.
- SCCMHA is a Covered Entity.
- As an employee of a Covered Entity, YOU also have responsibilities.







HIPAA

Key Definition



- **Health Information**

- any information, whether oral or recorded in any form or medium, that–
 - a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; **and**
 - b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

**Even after the death of a consumer,
the consumer's health information continues
to be protected.**



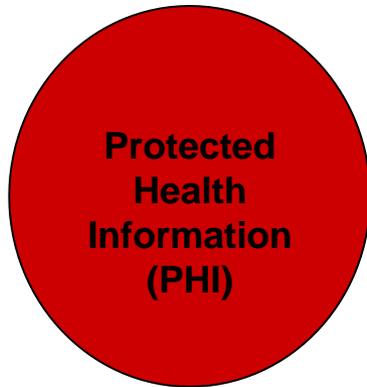
**Individually
Identifiable
Information**
(18 types of
identifiers)

HIPAA Key Definitions

- **Individually Identifiable Information**
 - a subset of **health information** collected from an individual, including . . .
 - **18 types** of demographic information:
 - That identifies the individual; or
 - There is a reasonable basis to believe the information can be used to identify the individual.

- Individually Identifiable Information-

1. Patient names
2. Geographic subdivisions (smaller than state)
3. Telephone #s
4. Fax #s
5. Social Security #s
6. Vehicle identifiers
7. E-mail addresses
8. Web URLs and IP addresses
9. Dates (except year)
10. Names of relatives
11. Full face photographs or images
12. Healthcare record #s
13. Account #s
14. Biometric identifiers (fingerprints or voiceprints)
15. Device identifiers
16. Health plan beneficiary #s
17. Certificate / license #s
18. Any other unique number, code, or characteristic that can be linked to an individual.



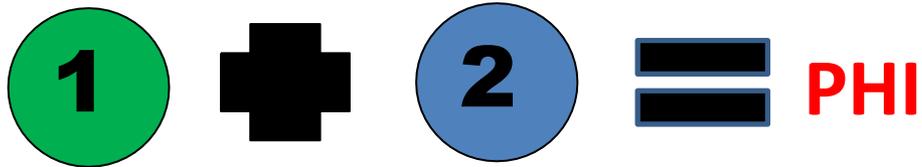
HIPAA

Key Definitions

- **Protected Health Information** (PHI) covered under the HIPAA Privacy Rule is:
 - Individually identifiable health information, that is
 - Transmitted or maintained in any form or medium (paper, electronic, oral), is
 - Created or received by a covered entity, business associate or employer, and is
 - Related to health care or payment for health care.



Protected Health Information



2 components of PHI



Contains Health Information . . .

- i. oral, fax, written, electronic -
- ii. Created or received -
- iii. By health care provider, health plan, public health authority, employer, insurer, others
- iv. **Relating to past, present or future -**
- v. **Physical or mental health status -**
- vi. Health care -
- vii. Payment for health care

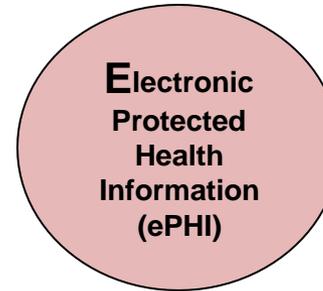


Identifies the Client . . .

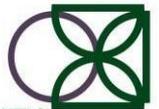
18 types of demographic information



HIPAA Key Definitions



- **Electronic Protected Health Information**
(ePHI)
 - Any PHI covered under HIPAA, that is
 - created, received, used or maintained in an **electronic form**, is
 - covered under the HIPAA Security Rule



HIPAA Security Rule

- The **Security Rule** protects a subset of information covered by the **Privacy Rule**, which is all individually identifiable health information that a covered entity creates, receives, maintains or transmits in electronic form.
- The **Security Rule** calls this information “electronic protected health information” (**e-PHI**).
- The **Security Rule** does not apply to PHI transmitted **orally** or in **writing** – **BUT**, the **Privacy Rule** does.



Teleworking / Remote Work Policy

- SCCMHA Policy Number 313 applies to Teleworking / Remote Work Policy and should be reviewed prior to an individual performing telework or remote work
- HIPAA Privacy and Security policies are to be complied with during teleworking and Remote Work
- Any agency materials taken home should be kept in the designated area at home and not be made accessible to others.
- If SCCMHA documents or information cannot be secured and kept private at the alternative worksite, it should not be printed in hard copy.

HIPAA Security Rule

1. **The HIPAA Security Rule** establishes national standards to protect an individuals' electronic protected health information
2. These national standards can help avoid some of the common security gaps that lead to cyber attack or data loss. They can protect the people, information, technology, and facilities that you may depend on to carry out your primary mission: helping your patients.
3. The HIPAA **Security Rule** requires covered providers to implement security measures, which help protect patients' privacy by creating the conditions for patient health information to be available but not be improperly used or disclosed.

HIPAA Security Rule

1. Physical Safeguards

- physical measures, policies, and procedures to protect the electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2. Facility Access and Control

- physical access (i.e., walls, doors, locks) to the facilities is limited and controlled, while ensuring that authorized access is allowed.

3. Workstation and Device Security.

- Policies and procedures to specify proper use of and access to workstations and electronic media.
- Policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

PHI & Email

(How to handle email which contain consumer related information – PHI)

- 1. GENERAL RULE:** Email or data files which contain PHI should only be sent using (1) **a secure line** OR (2) **encryption**
- Email sent within SCCMHA - **both sender & receiver** have an email address ending in “**sccmha.org**” These emails should contain the following comment in the header: **PHI Content Caution**
- Email sent **outside** SCCMHA – if either the sender, the receiver, or both, do not have an **sccmha.org** address - the preferred method is the **Sentri II messaging system**
- If the Sentri II messaging system is not possible, **use encryption**

Login Tips

(User Name and Passwords)

1. Usernames and passwords should not be shared.
2. Passwords should **not be written down**
3. Use of SCCMHA computer equipment will be monitored.
4. Passwords should be complex:
 - a) Passwords should be long – the more characters used, the stronger the password
 - b) Include Numbers, Letters, Upper Case, Lower Case, Symbols

General Tips

1. All SCCMHA computers use current Anti-Virus software
2. Users should not leave their computer workstation unattended or unlocked
3. Users should not bypass physical security measures (such as propping open doors which should be locked)
4. Only SCCMHA-provided or approved equipment will be allowed on the SCCMHA network

Telephone Tips

1. Only SCCMHA provided cellphones and SCCMHA configured cellphones will be allowed to contain SCCMHA email and connect to SCCMHA Wi-Fi.
2. The SCCMHA telephone system and all messages generated or handled by SCCMHA voicemail are part of the business equipment and data assets of SCCMHA and are not the property of the users of the system.
3. Policy 08.01.06 provides detailed information –
PLEASE REVIEW THIS POLICY

Video-Conferencing

1. During a nationwide public health emergency (such as Covid-19), SCCMHA may choose to use audio or video communication technology to provide telehealth services to patients.
2. Under such circumstances, only an SCCMHA-approved non-public facing remote communication product may be used to communicate with patients.
3. A “non-public facing” remote communication product is one that, as a default, allows only the intended parties to participate in the communication.
4. Use of public-facing remote communication products, such as TikTok, Facebook Live, Twitch, or a public chat room are unacceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication.

Video-Conferencing

The following are the only SCCMHA- approved tools for use with Video Conferencing

1. **Skype For Business:** May be used for meetings involving internal staff and leadership meetings. This is especially important when PHI has the potential to be displayed/discussed.
2. **ZOOM Pro:** May be used for all external meetings as well as SCCMHA CME Training. PHI is never to be displayed/discussed.
3. **DOXY.ME:** May be used for all virtual meetings, visits etc. with Consumers and/or Guardians.

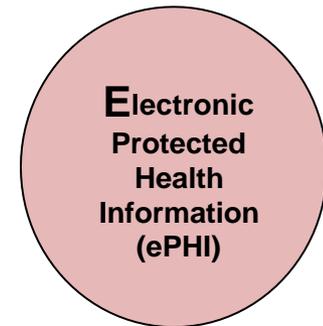
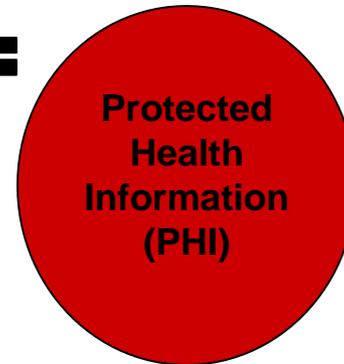
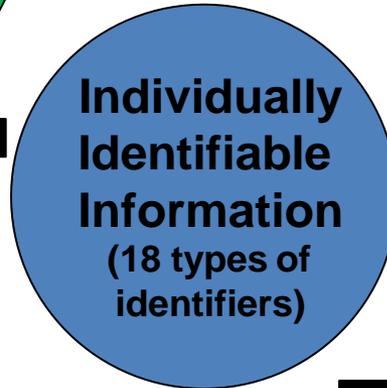
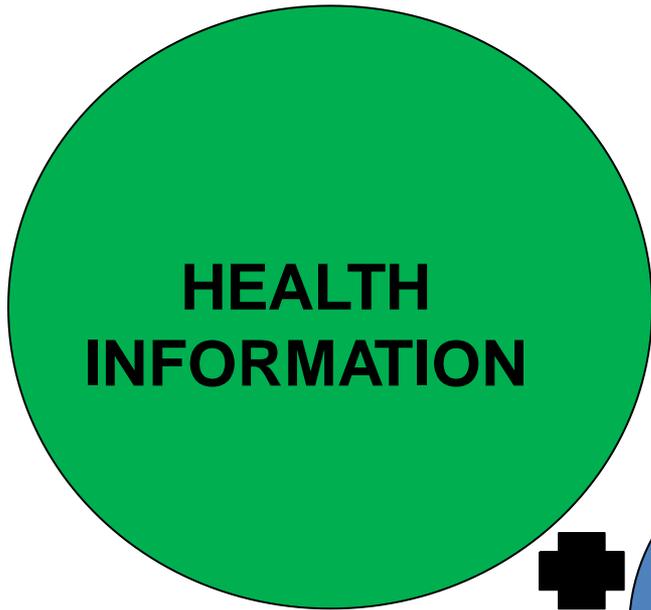


Video-Conferencing

For assistance with Video-Conferencing, contact either your immediate supervisor, or the Help-Desk.



Overview



A CLOSER LOOK AT THE HIPAA PRIVACY RULE



HIPAA Privacy Rule

In general, the HIPAA Privacy Rule requirements are:

1. HIPAA applies to most health care providers;
2. HIPAA sets a federal floor for protecting PHI across all mediums - electronic, paper, and oral
3. **State law** - Michigan - may provide greater protections;
4. HIPAA limits how CEs may use & disclose PHI which they receive or create;
5. HIPAA gives individuals rights with respect to their PHI;
 - a. Right to examine their medical records;
 - b. Right to obtain a copy of their medical records;
 - c. Right to ask CEs to amend their medical record if the information is inaccurate or incomplete
6. HIPAA imposes administrative requirements for CEs;
7. HIPAA establishes civil penalties for violations.
8. HIPAA continues to protect PHI even after the individual's death

HIPAA Requirements

HIPAA requires that PHI is protected, in whatever the PHI that is created, stored, or transmitted.

form

Consider the following forms of PHI:

- Verbal (i.e. in person, on the phone, etc.).
- Paper (i.e. chart, progress notes, prescriptions, referral forms, scratch paper, etc.)
- Computer applications/systems (i.e. electronic health record (EHR), etc.)
- SCCMHA computer hardware / equipment (PCs, laptops, PDAs, pagers, fax machines cell/multifunctional phones, etc.)

Disclosure

- The use or disclosure of PHI without

1. A written authorization or
2. An exception to the rules

is prohibited!



HIPAA PRIVACY: DISCLOSURES

1. TREATMENT

- CEs may disclose PHI for treatment activities to another health care provider

2. PAYMENT

- CEs may disclose PHI to another CE or health care provider for the CE's payment purposes

3. HEALTH CARE OPERATIONS

- CEs may disclose PHI to another CE for certain specified activities (e.g., quality improvement initiatives)

• **AUTHORIZATION**

- The individual/consumer may authorize the release of their own PHI in writing with a signature and date . . . provided other requirements are met



HIPAA PRIVACY: DISCLOSURES

CEs may only use and disclose PHI according to specific guidelines

1. The CE is **REQUIRED** to disclose upon request:
 - a. To the HHS Secretary
 - b. To the individual

2. The CE is **PERMITTED** (but not required) to disclose:
 - a. For treatment, payment, and health care operations (TPO)
 - b. Incidental Uses & Disclosures
 - c. When the individual has the opportunity to agree or object
 - d. Specific “public purpose” disclosures – such as to public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births
 - e. Limited data sets which require a data use agreement between the parties
 - f. De-identification (ALL identifiers have been removed)
 - g. With authorization from the consumer – when in doubt, get an authorization





Limit Disclosure

Covered Entities, including SCCMHA, should **limit** their uses, disclosures and requests for PHI to the **minimum amount necessary** to achieve the stated purpose.

- For **routine & recurring disclosures**, a covered entity should **limit the disclosure of PHI to only the amount reasonably necessary to achieve the purpose of the disclosure or request.**
- For **non-routine disclosures**, the covered entity should review each individual request.

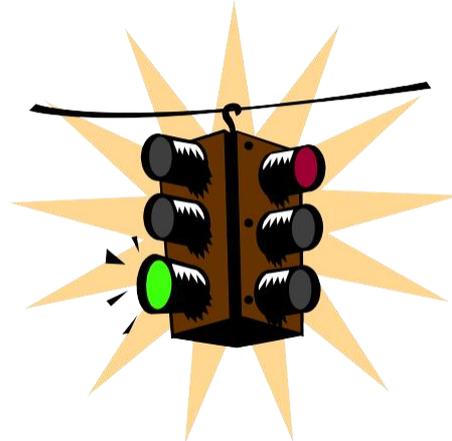


WHO Protects PHI?

1. **Federal Government** enforces HIPAA.
 - Civil penalties up to **\$25,000** for Failure to Comply
 - Criminal Penalties:
 - **\$50,000** fine and up to **1 year in prison** for knowingly obtaining and wrongfully sharing information
 - **\$100,000** fine and up to **5 years in prison** for obtaining and disclosing through false pretenses.
 - **\$250,000** fine and up to **10 years in prison** for obtaining and disclosing for commercial advantage, personal gain, or malicious harm.
2. **SCCMHA** through the *Notice of Privacy Practices*
3. **SCCMHA Employees** – by following the SCCMHA policies and procedures.

Disclosure With Written Authorization

Disclosures that are
Not Otherwise Permitted
are allowed with
Written Authorization



Healthcare Privacy

The HIPAA Authorization

- A covered entity must obtain the individual's written authorization for any **use or disclosure of PHI that is not:**
 1. **treatment, payment or health care operations**
or
 2. **otherwise permitted by the Privacy Rule.**

A HIPAA authorization must meet certain requirements – or it is NOT valid.

Privacy Regulations Beyond HIPAA

- ❑ 42 CFR Part 2
- ❑ Michigan Mental Health Code
- ❑ HIV / AIDS



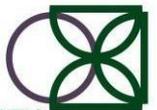
Alcohol and Other Drug (AOD) Confidentiality Rule 42 CFR Part 2



42 CFR Part 2

The Alcohol and Other Drug (AOD) Confidentiality Rule

- Protects any type of information that could potentially link an individual, by name or otherwise, to a substance abuse treatment program.
- 42 CFR Part 2 provides extra protection to these records to encourage persons who abuse substances to seek treatment, who might otherwise be deterred from treatment for fear their substance abuse treatment would become public information.



42 CFR Part 2

- **General Rule:**

Information that identifies an individual as a patient of a program **may not** be used or disclosed without specific patient authorization, unless an exception for the use or disclosure applies.

- **Exceptions:**

Only “**limited**” disclosures are permitted – disclose only as much information as is necessary to carry out the purpose of the disclosure. This provides more restrictions on sharing than HIPAA.

42 CFR Part 2

Behavioral Health Records

Substance Use Disorder (SUD) Records

- “Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section, be confidential and be disclosed only for the purposes and under the circumstances expressly authorized...”
- Prohibits even acknowledging an individual as a recipient of services
- Requires a **very specific**, detailed Release of Information (ROI)
- Requires information that is disclosed include a ‘Prohibition on Rediscovery’
- **No information** regarding a client should be released without a valid, 42 CFR Part 2-compliant ROI

42 CFR Part 2

- If you have ANY questions related to 42 CFR Part 2, or SUD issues, contact your supervisor or the Compliance Officer.





Michigan Mental Health Code (MHC) MCL 330.1748



Healthcare Privacy

Michigan Mental Health Code (MHC)

MCL 330.1748

The Mental Health Code provides protections for the information in the record of a consumer and other information that was acquired in the course of providing mental health services to a consumer.

Mental Health Code

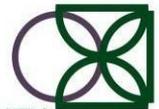
The Bottom Line

The information may be disclosed outside the department community mental health services program, licensed facility, or contract provider (whichever is the holder of the record) **only in the circumstances presented in section 748 & 748 A of the Mental Health Code.**

Mental Health Records

MI Mental Health Code

- **TREATMENT:** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or referral of a patient for health care from one health care provider to another.
- **PAYMENT:** Activities undertaken by (1) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (2) A health care provider or health plan to provide reimbursement for the provision of health care.
 - **Includes:** eligibility/coverage determinations; COB; adjudication of claims; billing; medical necessity review; utilization review activities including preauthorization, and concurrent and retrospective review.
- **Coordination of Care:** Not specifically defined by HIPAA or the MI Mental Health Code.
 - If PHI is being shared between health care providers, it may fall under the purpose of “Treatment”.
 - If PHI is being shared between entities that are not health care providers (ex. PIHP and MHP), then disclosure of PHI is limited to entities that have a current or past relationship with the consumer who is the subject of the PHI, and the PHI must pertain to such relationship (45 CFR 164.506(c)(4)).



PRIVACY & CONFIDENTIALITY

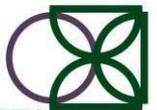
Behavioral Health Records

HIV/AIDS Information

Confidentiality of HIV/AIDS Information

MCL 333.5131

- “HIV-related information is confidential & cannot be released unless the consumer authorizes disclosure, or a statutory exception applies. This confidentiality statute applies to all reports, records & data pertaining to testing, care, treatment, reporting & research & information pertaining to partner counseling & referral services (formerly known as partner notification) under section 5114a, that are associated with the serious communicable diseases or infections of HIV & AIDS.”
- The consumer must sign a release of information containing a SPECIFIC statement if the release is to cover HIV-related information in the records before the information can be released.



PRIVACY & CONFIDENTIALITY

Behavioral Health Records

Breach Notification



- A breach occurs when there is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of that information.
- Depending on the circumstances, a breach may require notice to the consumer that his/her information was inappropriately released, mitigation efforts such as credit monitoring, notification to local media, and/or notification to the Office for Civil Rights (OCR).
- If you suspect or know of any situation involving a potential breach, it is your responsibility to report it to the Compliance Department for investigation.
- Examples:
 - Sending a letter containing PHI to the wrong address
 - Medical records/laptop being lost or stolen
 - Posting about a consumer on social media



Protected Health Information and Tricky Issues



? What About ? Divorced Parents

- A divorced parent calls to get information about their child. Can you release it?

See MHC §748(6)

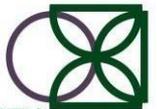
- If the parents are divorced, a parent with legal custody has the authority to provide consent – joint legal custody may exist
- If the parental rights of one parent have been terminated, the parent with sole legal custody is responsible to provide consent.
- When in doubt, call the parent who has physical custody to ask if the other parent is allowed to obtain records. If that parent says ‘No’, then ask for the corresponding court documents.



? What About ? Legal Guardians

- An individual calls to discuss a consumer's record with you and states that he/she is the consumer's **Guardian**.
- What do you do?
 - Verify that the individual **is** the consumer's Legal Guardian and in fact has access rights to the type of records being requested.
 - Sometimes even a **Guardian may be mistaken** about the extent of their authority.

Verify – Verify - Verify





? What About ? Step-Parents

- A consumer's step-parent calls to discuss their stepchild's care.
- May you discuss this with them?

NO – unless the step-parent is a legal guardian and the guardianship papers are available in the record, or a legal guardian has provided valid authorization.

Verify – Verify - Verify





? What About ? Foster-Parents

- Can foster parents get information about the child they are caring for?
 - Yes, if the foster parent has guardianship, other court papers, or an authorization from the birth parent, allowing them the right of access.
 - If the foster parent does not have proper legal papers and a health care provider is in need of the information, you may release directly to the health care provider.





? What About ? Leaving Messages

- A spouse answers the phone, or voice-mail picks *up*. What information may be provided?
 1. State your name.
 2. Ask that the individual return your call, and provide your direct phone number.
 3. Do not provide detailed information.
 4. Double check that you ended the call.





? What About ? Faxing PHI

- May PHI be faxed?
 - **Yes** – PHI may be faxed, but only when it is in the best interest of consumer care or payment of claims.
 - Sensitive PHI **should not be faxed** (HIV, mental health, AODA, STDS, etc.)

It is **best practice** to test a fax number prior to faxing PHI to it. If this is not done, then complete the following:

1. Restate the fax number to the individual providing it to you.
2. Obtain a telephone number to contact the recipient with any questions.
3. Do not include PHI on the cover sheet.
4. Verify you are including only the appropriate consumer's information (i.e. check the top and bottom pages).
5. Double check the fax number prior to “sending” it.



Proper Use of Fax machines

- **Note:** A fax machine should not be used for routine release of health information to insurance companies or other Government agencies (e.g., DHS or Social Security) where a mail or courier service is available and can be used with equal efficiency.
- **Note:** Fax machines used for transfer of PHI should be located in secure areas. They should not be located in publicly accessible areas.



? What About ? Discussing PHI

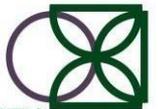
- You never know who may overhear you discussing a consumer. The consumer or coworker could be another consumer's neighbor, best friend, cousin, etc. . .
 - Remember to speak quietly - use your library voice.
 - When possible, discuss PHI privately, such as behind a closed door.
 - Avoid having discussions in waiting rooms, elevators, break rooms, hallways, outside the building, etc.





? What About ? Encountering a Consumer In a Public Area?

- Imagine that you are walking through the grocery store, and you see a consumer that you know. What should you do?
 - It's OK to greet the individual, but do not ask the consumer "how he/she is doing" or inquire about their health. It is ok to listen if he/she offers to update you on their health.
 - Let the consumer approach you first, but don't make it seem like you are trying to avoid them.

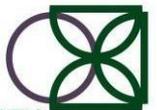




? What About ?

Talking with Friends About Work

- Do not share with family, friends, or anyone else a consumer's name, or any other information that may identify him/her, for instance:
 - It would **not** be a good idea to tell your friend that a consumer came in to be seen after a severe car accident.
 - Your friend may have heard about the car accident on the news or the TV and may even know the person involved.
- Do **not** inform anyone that a high-profile person, or their family members, were seen at work.





? What About ? Delivery & Transportation

- You need to transport paper records/PHI to another department or location. Is it ok to do this?

Yes - you may transport documents for work-related purposes.

Secure the documents so that you do not drop them:

- Carry them close to your person.
- Carry them in a container, bag, or box.
- Ensure that no consumer names are visible.
- Ensure that no records are left unattended.
- Do not leave documents exposed within your vehicle – leave them in the trunk if possible.





? What About ? Paper Documents

- When you leave your desk/cubicle, turn over or cover PHI so that others cannot read it.
 - If you have an office, you have the option of closing your door instead.
- Turn over or cover PHI when approached by a coworker to discuss an issue other than that PHI.
- Do not leave documents containing PHI unattended in fax machines, printers or copiers.
- Check your fax machines and printers frequently so documents are not left on the machine.





? What About? Subpoenas

- If you receive a subpoena related to your work at SCCMHA – never ignore it.
- Contact the SCCMHA Compliance Officer (AmyLou Douglas) as soon as possible. Guidance about the subpoena will be provided.





? What About ? Document Disposal

- How should confidential paper be disposed of?
 - Shred or place all confidential paper in the designated confidential paper bins.
 - This includes all forms of paper that may contain PHI – Post-it notes, scratch paper, envelopes.
 - Documents which do not contain PHI may be shredded or recycled.
 - Tissues, paper plates, cardboard or pizza boxes may be placed in the appropriate recycling container.
- How should electronic media (floppy disk, CD, USB Drive, etc.) be disposed of?
 - Provide electronic media to the I.S. Department for disposal.

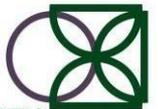


Use 'Reasonable Safeguards'

- Privacy principles do not prohibit an incidental disclosure of patient information as long as reasonable safeguards are taken to minimize the disclosure.
- What is 'reasonable' depends on the situation.

Examples of Reasonable Safeguards

- **Avoid conversations about one consumer in front of other consumers or their visitors/families.**
- **Lower your voice when discussing consumer information in person and/or over the phone.**
- **Avoiding conversations about consumers in public places, such as elevators, public hallways, or the cafeteria.**



How much PHI to Disclose?

- When it is practical, no information (PHI) should be disclosed unless it is relevant to the authorized purpose for which disclosure was sought.
- Disclose the least amount of PHI as is necessary.

Are you aware of a Breach?

- A 'breach' is a violation of a SCCMHA compliance-related rule. These include violations of HIPAA or other confidentiality regulations.
- If you suspect a potential breach has occurred, notify your supervisor or the SCCMHA Compliance Officer (AmyLou Douglas) at 797-3506.
- It is not necessary to contact your supervisor before contacting the Compliance Officer.



Possible Penalties

- The possible penalties for a HIPAA privacy violation include fines, jail time and possible loss of employment:
 - Start at \$100 fine per violation, up to \$1,500,000.
 - An employer may impose disciplinary action up to discharge.

Authorizations to Release Information

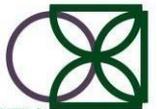
- Each of the laws that involve the records of SCCMHA consumers have specific requirements about releasing (sharing) information. It can be confusing!
- **General Rule**: Share no information about a consumer of SCCMHA services – even the fact that they are receiving services of any type from SCCMHA.
- **Valid Release**: **IF** you have a valid release (authorization), information may be shared/released in compliance with the authorization.
- Releasing information without a valid authorization may be a serious breach of confidentiality.





Reminders

- Documents containing PHI or other sensitive information must be properly shredded in a cross-cut shredded or placed in an approved shredding bin container when no longer needed.
- Shred immediately or place in securely locked boxes or rooms to await shredding.
- Media, such as CDs, disks, or thumb drives, containing PHI/sensitive information must be cleaned or sanitized before reallocating or destroying.
 - NOTE: “Sanitize” means to eliminate confidential or sensitive information from computer/electronic media by either overwriting the data or magnetically erasing data from the media.
 - NOTE: Deleting a file does not actually remove the data from the media.





More Reminders

- PCDs include handheld, notebook, and laptop computers, smart phones, and portable memory devices such as flash disks, thumb drives, jump drives, etc.
 - Use of PCDs for ePHI must be approved by senior management.
 - PCDs must be inventoried and maintain appropriate security protection. PCDs used for PHI must be encrypted. Ask your information systems representative for help securing smart phones.

The Bottom

1. Sensitive information exists in many forms: printed, spoken, and electronic.
2. Sensitive information includes Social Security numbers, credit card numbers, driver's license numbers
3. There are several laws that impose privacy and security requirements, including HIPAA, 42 CFR Part 2, and the Michigan Mental Health Code.
4. Two primary HIPAA regulations are the Privacy Rule and the Security Rule.
5. Information that identifies a patient and that is combined with health information, creates PHI.

The Bottom _____ (Cont.)

6. An employee **must** have a patient's written authorization or a job-related reason for accessing or disclosing consumer information – **even if the employee is related to the consumer**
7. **Breaches of information privacy and security may result in both civil and criminal penalties, as well as SCCMHA sanctions. Employees must report such breaches.**
8. By the nature of your job, you may have access to information about SCCMHA consumers. **NO SNOOPING!** Be aware that access to consumer records may be audited. Unauthorized access to a consumer's record (even a relative's record) may result in disciplinary action.
9. **Be cautious about re-disclosing information gained from another entity's records.**

The Bottom _____ (Cont)

10. Do not discuss consumer information in an environment where other people (who do not have a need to know the information) are present (for example, hallways or elevators). Share the least amount of information which will still accomplish the goal of the signed consent.
11. Be cautious about subpoenas – know the requirements.
12. Keep the disclosed records in a secure environment.
13. The authority of the adult signing the consent should be clearly identified.

PRIVACY & CONFIDENTIALITY

Behavioral Health Records

TRUE OR FALSE?

Behavioral health providers cannot ever share my records without my permission.

FALSE

TRUE

HIPAA, the MI MHC, and 42 CFR Part 2 all contain specific **exceptions** for when PHI may be shared without first obtaining patient consent. Check with your Compliance Officer to verify if an exception applies.

Protected Health Information (PHI) cannot be shared by email.

FALSE

TRUE

Before sending any PHI electronically, check your agency's policies and make sure that it is **encrypted** or otherwise protected, and that it is addressed to the correct recipient.

If your agency receives a request from a provider for a patient's most recent Treatment Plan (mental health only) to assist that provider in appropriately treating the patient, it is acceptable to send the provider the patient's entire record.

FALSE

TRUE

Non-SUD PHI can be shared without an ROI for Treatment, Payment, and Coordination of Care purposes in accordance with HIPAA. **HOWEVER**, only the minimum amount of information necessary to accomplish the purpose of the disclosure may be disclosed.

Enforcement Bodies



Center for Medicare and Medicaid Services (CMS)

- Federal Agency with the US Department of Health and Human Services (HHS) that administers the Medicare program and work in partnership with state governments to administer Medicaid programs.

Office of the Inspector General (OIG)

- Enforcement division of the Federal Health and Human Services (HHS) agency, and of the Michigan Department of Health and Human Services.
- In charge of investigating Fraud, Waste, and Abuse in the Medicaid/Medicare Programs, and pursuing civil judgments under the Civil Monetary Penalties Law.

Office for Civil Rights (OCR)

- In charge of enforcing HIPAA Privacy and Security Rules. Levy huge civil penalties against entities that violate HIPAA.
- Implement and monitor Corporate Integrity Agreements.

Department of Justice (DOJ)

- Federal enforcement agency in charge of criminally prosecuting individuals/entities under applicable Federal laws.
- Works collaboratively with the OIG.

Michigan Attorney General

- Health Care Fraud Division in charge of investigating Fraud, Waste, and Abuse in the Michigan Medicaid/Medicare Programs.
- Can prosecute individuals/entities criminally under applicable State laws.



- When in doubt about **ANYTHING** related to Compliance -
- when you see a red flag,
- consult with your supervisor or the Compliance Office.

REPORTING RESPONSIBILITIES

It is your right and your responsibility to report actual and suspected Compliance violations to the SCCMHA Compliance Officer

You may not be intimidated, threatened, coerced, discriminated against, or subjected to other retaliatory action for making a good faith report of an actual or suspected violation.

SCCMHA Compliance Reporting

Compliance Hotline:

989-797-3574 or 855-797-3417

In-person, by telephone, or via email to:

AmyLou Douglas

989-797-3506

Amylou.douglas@sccmha.org



Main Facility

500 Hancock, Saginaw, Michigan 48602

Phone: (989) 797-3400

Toll Free: 1-800-258-8678

Michigan Relay 711

24 Hour Mental Health Emergency Services

(989) 792-9732

Toll Free: 1-800-233-0022

www.sccmha.org



Healthcare Privacy

