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.

Self Determination in compliance with SCCMHA

COMPLIANCE PROGRAM

AND

False Claims Information

2019

The Big Picture

- Compliance Overview
  - False Claims Act

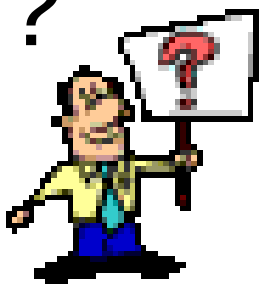
When you have completed this training . . .

- You will have a working knowledge of the SCCMHA Compliance Program as well as federal and Michigan False Claims Acts.
- 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.

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.

Causing or allowing misuse of Medicaid funds could expose both you and SCCMHA to:

- Federal criminal prosecution
- State criminal prosecution
- Federal civil prosecution
- State civil prosecution
- Federal administrative civil penalties

WHY A COMPLIANCE PROGRAM?

- The health care industry is highly regulated.
- The SCCMHA Office of Regulatory Compliance is designed to maintain current knowledge of the laws and regulations impacting SCCMHA.
- The SCCMHA Compliance program provides training for a wide range of compliance-related topics.

SCCMHA Compliance

- SCCMHA and the Fiscal Intermediary has a formal commitment -
  - to comply with relevant standards and regulations;
  - to aid in preventing, detecting, investigating, and reporting potential fraud and abuse occurrences;
  - with the intention of minimizing the prospect of improper conduct by SCCMHA and its contractual providers.

What are the Goals?

1. Education

Provide education about the applicable laws and training in matters of health-care regulations.

What are the Goals?

2. Oversight

Provide periodic auditing, monitoring and oversight of compliance with health-care regulations.

What are the Goals?

3. No retaliation

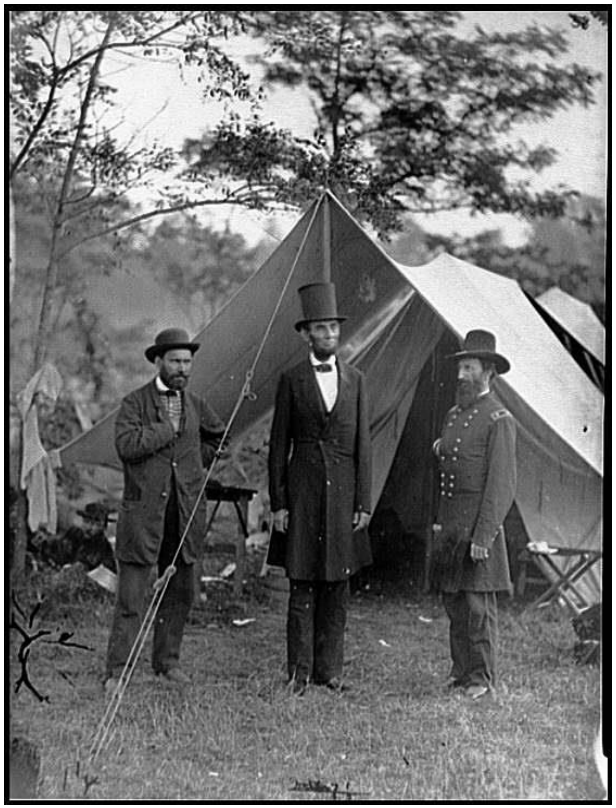
Provide an atmosphere
that encourages and enables
the reporting of non-compliance
without fear of retribution.

False Claims

What are the False Claims Acts?

- The federal and Michigan False Claims Acts are laws that were enacted to combat fraud committed by contractors against the U.S. Government and the State of Michigan.

Legislative History



- Federal False Claims Act
  - Enacted during the Civil War to combat contractor fraud against the Union Army.
- Michigan Medicaid False Claims Act
  - Enacted in 1977 to combat contractor fraud against the State of Michigan

Get ready for some legaleese and some definitions!!

What is Medicaid Fraud?

- Fraud:
  - an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person.

WHO can commit Medicaid Fraud?

- A Managed Care Organization
- A health care contractor
- A health care subcontractor
- A health care provider
- An health care employee, or
- A Medicaid beneficiary/Medicaid managed care enrollee

What does “False” Mean?

A claim is “false” if it is wholly or partially untrue or deceptive.

The Basics -

A person is liable under the False Claims Act if they **“knowingly”** . .

- Present a false or fraudulent claim to the U.S government;
- Make, use or cause to be used, a false record or statement to obtain payment from the government;
- Conspire to defraud the government by having a false claim paid;

Since you have to ‘knowingly’ present a false or fraudulent claim for payment to violate the Act . . .

All we have to say is

“I didn’t know”

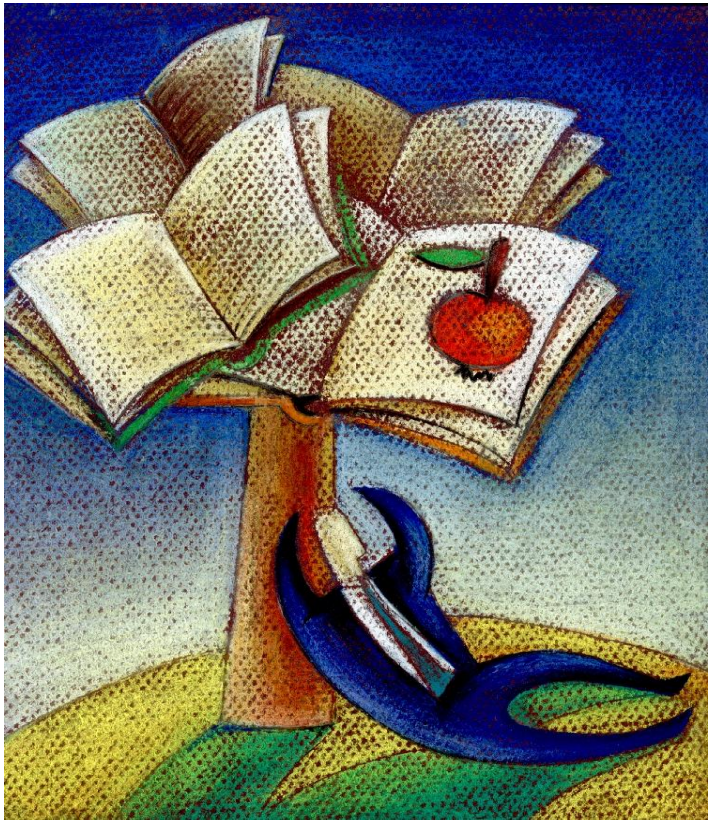
And there’s no problem.

Right??

Uh . . .

What does “knowing” Mean?

A person is “**knowing**” if he is in possession of facts under which he is aware **or should be aware** of the nature of his conduct and that his conduct is substantially certain to cause the payment of a Medicaid benefit.



Let's flesh that out a little

- 'knowing' and 'knowingly" means that a person, regarding the information on a claim –

1. has actual knowledge the information is false;
2. acts in deliberate ignorance of whether the information is true or false; **or**
3. acts in reckless disregard of whether the information is true or false

Reckless disregard?

For example:

- Completing claims with little or no factual basis
- Failing to document **actual** time spent on the project
- Poor record keeping
- Approving claims without reviewing them for accuracy.

And there doesn't have to be proof of specific intent to defraud

But what about a Mistake?

"Knowing" conduct does not include conduct which is in error or mistake

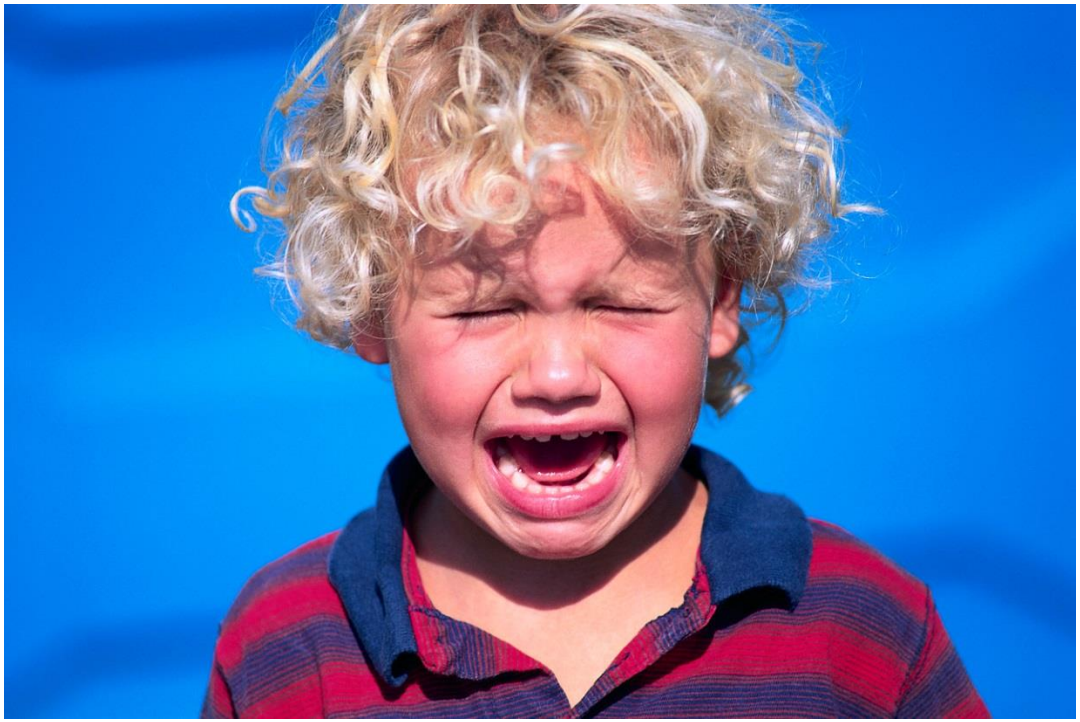
unless

the person's course of conduct indicates a systematic or persistent tendency to cause inaccuracies to be present.

Is there a pattern?

- A course of conduct is "systematic" if it has, shows or involves a system, method or plan.
- A course of conduct is "persistent" if it is constantly repeated.
- A system, method or plan to cause inaccuracies indicates an actual knowledge of falseness, and
- constant repetition indicates a constructive knowledge of falseness.

All done -



It was not <u>that</u> bad!!

Consequences

So if **you** violate the Act . . .

What could happen?

Civil Penalties Under the federal False Claims Act

- Triple (3X) damages **plus**
- up to $11,000 per claim **plus**
- Potential exclusion from participation in the Medicaid program **and**
- The amount of the false claim does not matter!

False – is False!

Aiding and Abetting

(MCL 767.39)

- Every person involved in the commission of an offense, whether he directly commits the offense or procures, counsels, aids or abets in its commission, may be convicted and punished as if he directly committed the offense.
- To be convicted as an aider and abettor, one must have the intent necessary to be convicted of the crime as a principal.

Federal Regulations

In addition, several Federal Regulations can be used in the prosecution of Medicaid fraud;

- False Claims Act
- Social Security Act
- Federal Mail and Wire Fraud
- Health Care Fraud
- Theft or Embezzlement
- False Statements

Federal Regulations

Why would Civil Federal Regulations be used?

1. **Civil prosecution** does not require proof of fraud –
2. It is enough if the provider acted in “reckless disregard” or “delibarate ignorance”
3. Whistleblower provisions allow for private citizens to collect a portion of the monies recouped.
4. Very high penalties assessed on a per claim for violators

But wait, There's also the Michigan False Claims Act . . . (MCL 400.601)

Similar to the federal False Claims Act

- Applies to state and political subdivisions
- Same defintions of knowing and knowingly
- Triple damages and penalties upto $10,000 per false claim
- Permits whistleblower lawsuits
- Michigan attorney general has the option to prosecute the claim as a criminal act

Michigan Criminal Statutes

Michigan has two statutes designed to combat health-care fraud (similar to federal regulations).

- one dealing with Medicaid claims,

  Medicaid False Claims Act, MCL 400.601

- one dealing with private insurance claims.

  Health Care False Claims Act, MCL 752.1001

Michigan
Medicaid False Claims Act

- A person may not make or present or cause to be made or presented to an employee or officer of this state a claim under the social welfare act upon or against the state, **knowing** the claim to be **false**.

Michigan
Health Care False Claims Act

- A person may not make or cause to be made or presented to a health care corporation or health care insurer a claim for payment of health care benefits **knowing** the claim to be **false**.

Penalties

- MFCA – Each false claim is a felony punishable by imprisonment of up to four years and/or a fine of up to $50,000.
- MFCA – Conspiracy or aiding a false claim is a felony punishable by imprisonment of up to ten years and/or a fine of up to $50,000.

How to reduce liability -

- If a false claim occurs, the court may assess ‘not less than’ double damages and costs IF within 30 days of discovery . .
  - the entity self reports
  - full cooperation is given with any investigation
  - no legal proceedings have commenced regarding the violation; and
  - the entity has no knowkledge of a governmental investigation of the violation

What is SCCMHA doing to prevent false claims?

SCCMHA takes all allegations of fraud, waste or abuse very seriously

SCCMHA's Anti-fraud policies

- SCCMHA has implemented policies and procedures to prevent health care fraud and comply with the False Claim Acts.

WHO TO CONTACT IF YOU HAVE A CONCERN

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

The Compliance Officer at 989-797-3574 or Toll Free Hotline

1-855-797-3417

WHO TO CONTACT IF YOU HAVE A CONCERN

- All involved with Fiscal Intermediary/Self Determination may also use many other reporting mechanisms to report a concern such as::
  - Use 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.
  - 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

    SCCMHA has a NO RETALIATION policy

WHO TO CONTACT IF YOU HAVE A CONCERN

- Contact the Compliance Officer – If an employee feels that s/he cannot report a compliance concern through the management chain of command, or other areas, contact the Compliance Officer. The Compliance Officer helps assure that SCCMHA and its employees, providers, and others that do business with SCCMHA comply with all applicable laws, rules and regulations. The Compliance Officer will research the matter for you while preserving confidentiality to the extent permitted by law.

- Use the Hot Line – at 797-3574 or 1-855-797-3417, is a confidential service, available 24 hours a day, 7 days a week. An employee may make a call anonymously, or, if the employee does identify him/herself, the confidentiality will be maintained within the limits of the 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 issues 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.

Conclusion and Summary

- SCCMHA has an effective compliance programs in place designed to monitor/prevent improper billing and documentation practices

- Documentation practices must provide a clear path leading from well established medical necessity, to treatment plans, to effective services.

If you suspect
Medicaid Fraud or Abuse

Call the SCCMHA Hotline

797 – 3574

1-855-797-3417

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.

Healthcare Privacy

Privacy Regulations:

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

General Examples of Medicaid Fraud

- Claiming hours on your time sheet which were not actually worked
- Forging an employer's signatures
- Adding time after the employer has signed the time sheet
- Asking the employer to pre-sign blank time sheets.
- Claiming you worked with two employers at the same time when you actually only worked with one

All are examples of possible Medicaid Fraud!!!!!

Prepared by:

Rich Garpiel

SCCMHA Compliance Officer / Privacy Officer

989-797-3574 or Toll Free Hotline

1-855-797-3417

rgarpiel@sccmha.org

Protecting Consumer Privacy

- The privacy of consumers who receive services from SCCMHA, as well as their records, are protected by several **federal and state** laws and regulations.

- 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 when you sense that something is not right – you see a red flag in your mind.
- You should then contact your supervisor or the Compliance Office Hotline to resolve the potential problem.

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

HIPAA
Key Definitions

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

HIPAA
Key Definitions

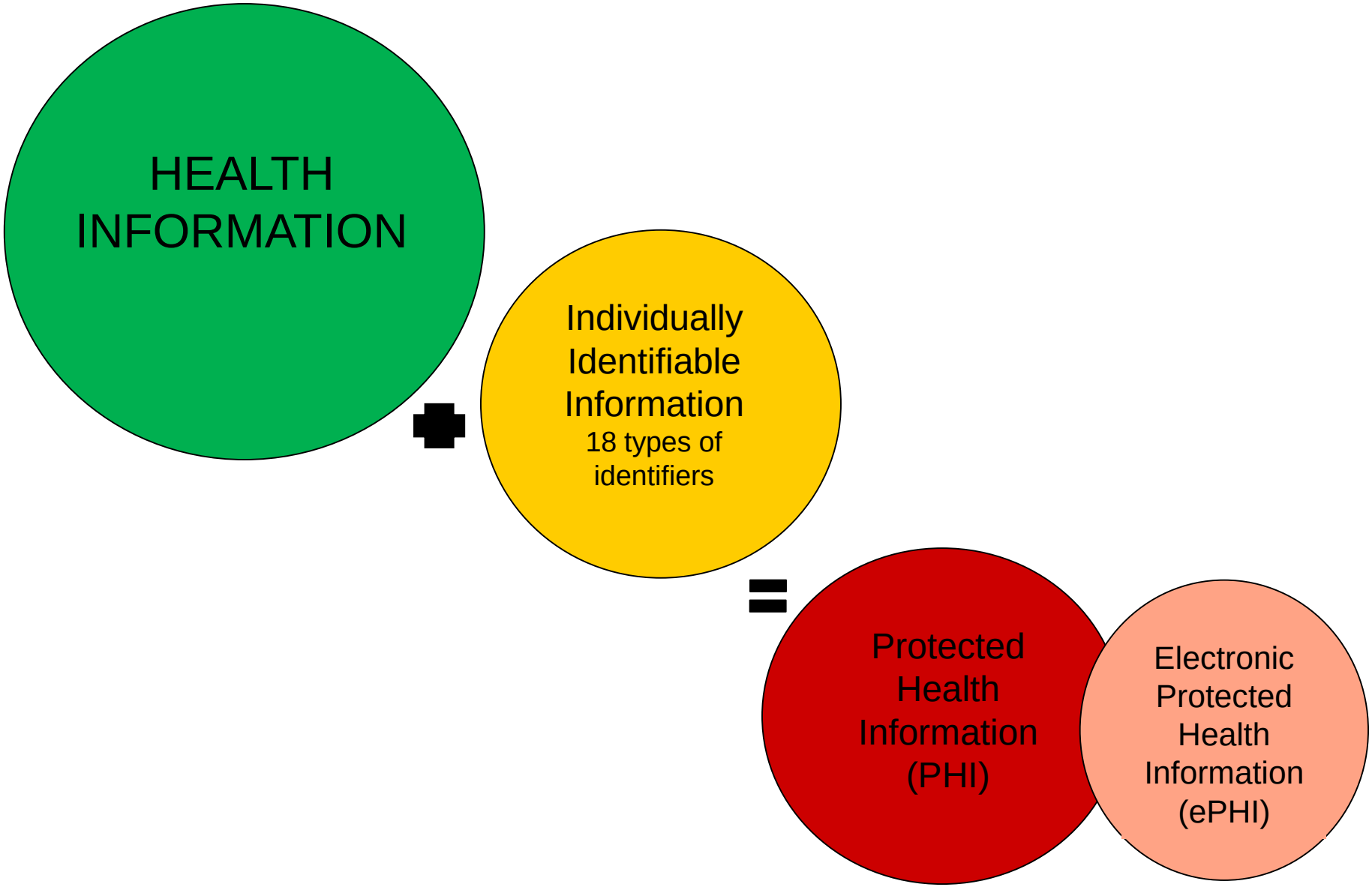
- **Covered Entity** (CE)
  - Health Care Providers; for example –
    - SCCMHA
    - Healthcare providers that contract with SCCMHA
    - Physicians
  - Health Care Insurers; for example –
    - Blue Cross
    - Medicaid
  - Health Care Clearinghouses

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 and YOU are a Covered Entity


HEALTH INFORMATION
Individually Identifiable Information
18 types of identifiers
Protected Health Information (PHI)
Electronic Protected Health Information (ePHI)

HIPPA 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.

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)
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium (paper, electronic, oral)
  - Created or received by a covered entity, business associate or employer
  - Related to health care or payment
  - PHI Remains protected after a persons death

Protected Health Information

2 components

1. Identifies the Client . . .
2. 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

HIPAA Key Definitions

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

HIPAA Security Rule

1. The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information

2. These safeguards 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.

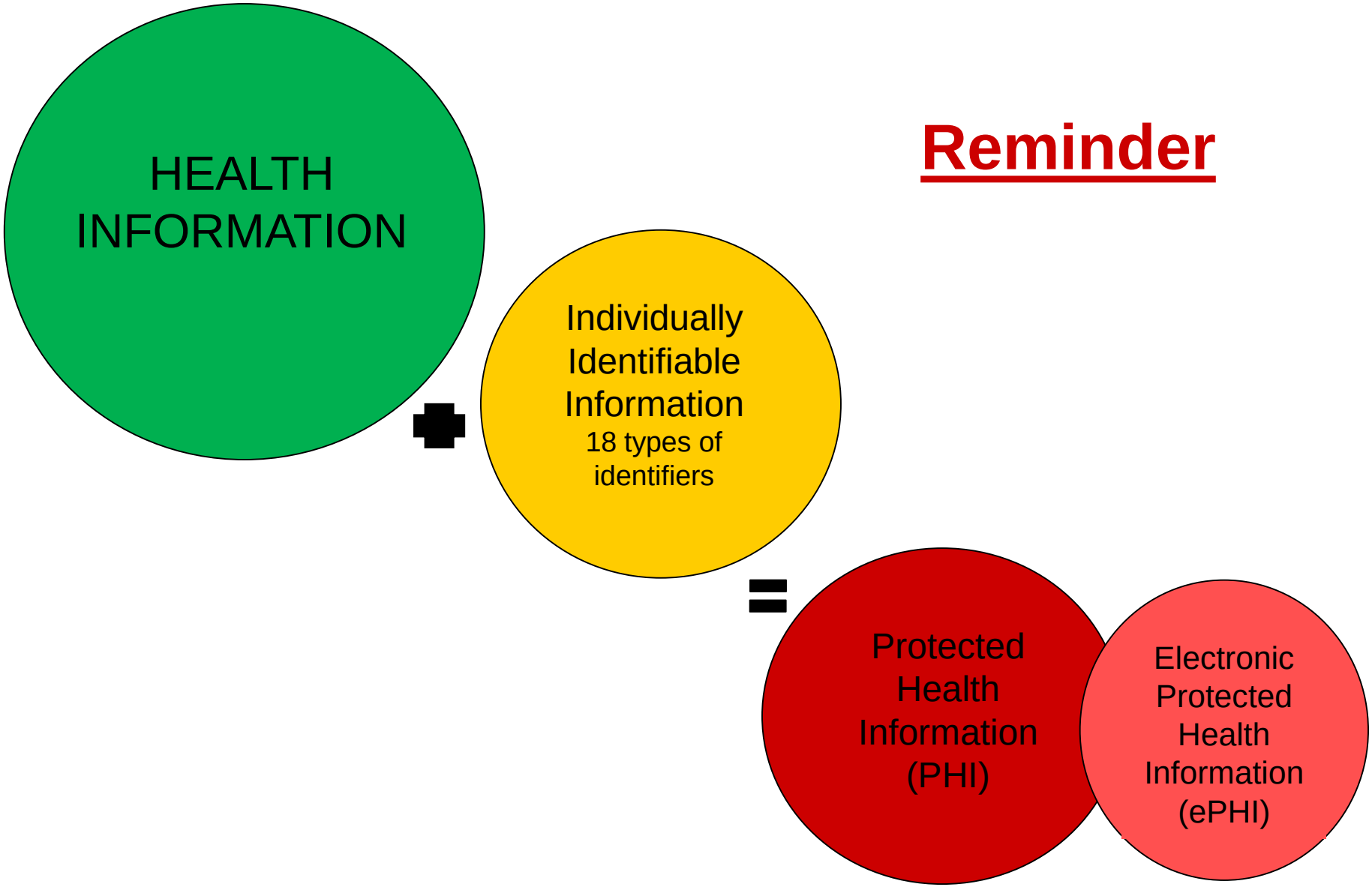
HIPAA Security Rule

- **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.

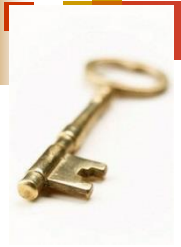
- **Facility Access and Control**
  - physical access (i.e., walls, doors, locks) to the facilities is limited and controlled, while ensuring that authorized access is allowed.

- **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).

Reminder


HEALTH INFORMATION
Individually Identifiable Information
18 types of identifiers
Protected Health Information (PHI)
Electronic Protected Health Information (ePHI)

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 in inaccurate or incomplete
6. HIPAA imposes administrative requirements for CEs;
7. HIPAA establishes civil penalties for violations.

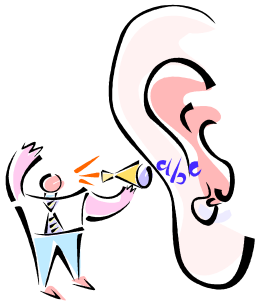
HIPAA Requirements

HIPAA requires that PHI is protected, in whatever **form** that PHI that is created, stored, or transmitted in. Consider the following forms:

- **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.)

Forms of Sensitive Information

Sensitive Information can exist in various forms. . .



Spoken

Written

electronic

It is the responsibility of <u>every</u> healthcare provider to

protect the privacy and security of sensitive information

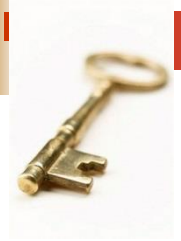
in **ALL** forms.

THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

Disclosure

- **The use or disclosure of PHI without**
  - ***A written authorization*** **or**
  - ***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 may authorize the release of their 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:
   a. To the HHS Secretary
   b. To the individual

- The CE is **PERMITTED** to disclose:
  1. For treatment, payment, and health care operations (TPO)
  2. Incidental Uses & Disclosures
  3. Individual has the opportunity to agree or object
  4. Specific “public purpose” disclosures
  5. Limited data sets (facially de-identified, requires data use agreement between the parties)
  6. De-identification (ALL identifiers have been removed)
  7. With authorization from the consumer – when all ese fails, get an authorization

Limited 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.

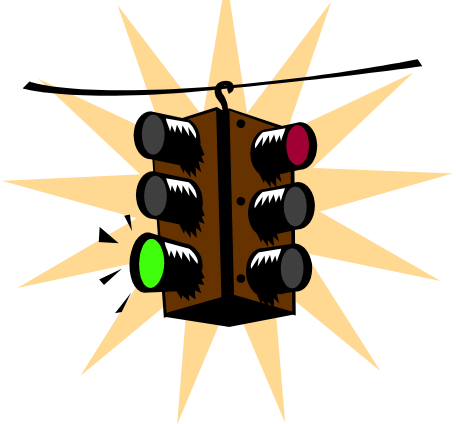
WHO Protects PHI?

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.

AUTHORIZATION TO SHARE OR DISCLOSE PHI

Disclosure With Written Authorization

Disclosures that are
Not Otherwise Permitted
are allowed with
Written Authorization



The HIPAA Authorization

- A covered entity must obtain the individual's written authorization for any **use or disclosure of PHI that is <u>not:</u>**
  - **treatment, payment or health care operations**

    or
  - **otherwise permitted by the Privacy Rule.**

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

Other Privacy Regulations

Beyond HIPAA

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

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

- Protects <u>any type</u> of information that could potentially link an individual, by name or otherwise, to a **<u>substance abuse treatment program</u>**.

- <u>42 CFR Part 2</u> 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.

What is 42 CFR 2 ?

- Title 42: Public Health **Code of Federal Regulations**
  Part 2: Confidentiality of Alcohol and Other Drug Abuse Patient Records

- These are the federal statutes that establish the guidelines for disclosure and use of the information contained in the patient record of an individual seeking and receiving treatment for alcohol and other drug abuse.

The AOD Confidentiality Rule 42 CFR Part 2

- **Purpose**:

42 CFR Part 2 is intended to encourage people who abuse substances to seek treatment, who might otherwise be discouraged from treatment for fear that 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 so much information as is necessary to carry out the purpose of the disclosure

Michigan Mental Health Code (MHC) MCL 330.1748

3. 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.**

Protected Health Information and Tricky Issues

? 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 **a Guardian may be mistaken** about the extent of their authority. **Verify – Verify - Verify**

? 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.

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 Outside of Work

- Imagine that you are walking through the grocery store, and you see an SCCMHA consumer. 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 ?
Paper Documents

- Turn over or cover PHI when a visitor enters the home.
- 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 ? Document Disposal

- How should confidential paper be disposed of?
  - Shred or destroy all confidential paperwork.
    - 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.

Use ‘Reasonable Safeguards’

- Privacy principles do not prohibit an incidental disclosure of patient information so 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 to Disclose?

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

Are you aware of a Breach?

- A ‘breach’ is a violation of SCCMHA compliance regulations. These include violations of HIPAA or other confidentiality regulations.
- If you are aware of a breach, notify your supervisor or contact the SCCMHA Office of Regulatory Compliance (Rich Garpiel) at 797-3539.

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.
  - SCCMHA may recommend disciplinary action up to discharge.

Authorizations to Release Information

- General Rule: Share no information about a consumer of SCCMHA services – even the fact that they are receiving services of any type from SCCMHA.

- Releasing information without a valid authorization may be a serious breach of confidentiality.

Reminders

- Documents containing PHI or other sensitive information must be shredded 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.

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 a number of laws that impose privacy and security requirements, including 42 CFR Part 2, and the Michigan Mental Health Code.**
4. Two primary HIPAA regulations are the Privacy Rule and the Security Rule**.**
5. **When used to identify a patient and combined with health information, Individually Identifiable Information create 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.

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. 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. Keep the disclosed records in a secure environment.

12. **The authority of the adult signing the consent should be clearly identified.**

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