Welcome to the Missouri Department of Mental Health

Health Insurance Portability and Accountability Act (HIPAA) Training

MISSOURI DEPARTMENT OF MENTAL HEALTH

What is HIPAA?

- Acronym for Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164).
- Provides a framework for establishment of nationwide protection of patient confidentiality (Privacy Rule), security of electronic systems (Security Rule), and standards and requirements for electronic transmission of health information (Electronic Data Exchange).

MISSOURI DEPARTMENT OF MENTAL HEALTH

Privacy Rule

- Privacy Rule went into effect on **April 14, 2003**.
- Privacy refers to protection of an individual's health care data.
- Defines how patient information is used and disclosed by covered entities and business associates.
- Gives patients privacy rights and more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

MISSOURI DEPARTMENT OF MENTAL HEALTH

Security Rule

- Security (IT) regulations went into effect **April 21, 2005.**
- Security means controlling:
  - **Confidentiality** of electronic protected health information (ePHI)
  - **Storage** of electronic protected health information (ePHI)
  - **Access** into electronic information

MISSOURI DEPARTMENT OF MENTAL HEALTH

Why Comply With HIPAA?

- To show our commitment to protecting privacy
- As a healthcare provider for a DMH consumer or DMH business associate, you are obligated to comply with The Department of Mental Health's privacy and security policies and procedures
- Our consumers are placing their trust in us to preserve the privacy of their most sensitive and personal information
- Compliance is not an option, it is required
- **If you choose not to follow the rules:**
  - You could be put at risk, including **personal** penalties and sanctions
  - You could put your agency as well as The Department of Mental Health at risk, including financial and reputational harm

What is a Covered Entity (CE)?

The HIPAA rule uses the term “covered entity” to refer to those that must comply. Covered entities fall into three categories: Health Care Providers, Health Care Clearinghouses, and Health Plans.

- Health care providers may include physicians, dentists, nursing homes, hospitals, and other entities that furnish, bill, or are paid for health care.
- Health Care Clearinghouse, such as billing services or community health management information systems.
- Health Plans, such as health, dental, vision, and prescription drug insurers, HMOs, Medicare and Medicaid insurers, and employer-sponsored group health plans.

Business Associate Agreements

- Under HIPAA, Business Associates are any person or entity that performs certain functions on behalf of, or provides services to, a covered entity – and those functions involve the use or disclosure of protected health information (PHI).

- All Organizations contracting with the Department of Mental Health to provide a service to our consumers, to access our information systems, to access our data, etc. require a Business Associate Provisions Agreement (BAA).

Business Associate

Requirements

- Limit uses and disclosures of PHI to minimum necessary
- Establish a BAA with their subcontractors
- Comply with the BAA and the same HIPAA; administrative, physical and technical safeguard rules as covered entities (CEs)
- Report to CE Breach of Unsecured PHI
- Comply with Privacy Rule to extent it must carry out a CE's obligation under Privacy Rule

MISSOURI DEPARTMENT OF MENTAL HEALTH

HIPAA Regulations

HIPAA Regulations require we protect our consumer's PHI in all media including, but not limited to, PHI created, stored, or transmitted in/on the following media:

- **Verbal Discussions** (i.e. in person or on the phone)
- **Written** on paper (i.e. chart, progress notes, encounter forms, prescriptions, x-ray orders, referral forms and explanation of benefit (EOBs) forms)
- **Computer Applications and Systems** (i.e. electronic health record (EHR), Practice Management, Lab and X-Ray)
- **Computer Hardware/Equipment** (i.e. PCs, laptops, PDAs, pagers, fax machines, servers and cell phones)

MISSOURI DEPARTMENT OF MENTAL HEALTH

Why is Privacy and Security Training Important?

- It is everyone's responsibility to take the confidentiality of consumer information seriously.
- Anytime you come in contact with consumer information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations.
- The law requires us to train you. Federal, state, and department regulations training is required for new staff, and annually thereafter.
- To ensure your understanding of the Privacy and Security Rules as they relate to your job.

HIPAA Definitions (PHI)

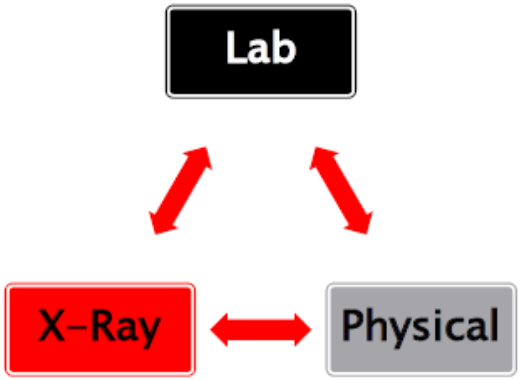
What is Protected Health Information (PHI)?

- Protected Health Information (PHI) is individually identifiable health information that is:
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse and that
    - Relates to the past, present, or future physical or mental health or condition of an individual;
    - Relates to the provision of health care to an individual
    - The past, present or future payment for the provision of health care to an individual.

HIPAA Definitions (PHI) cont.

What Does PHI Include?

- Information in the health record, such as:
  - All Consumer Identifiers
  - Encounter/visit documentation
  - Lab results
  - Appointment dates/times
  - Invoices
  - Radiology films and reports
  - History and physicals (H&Ps)



HIPAA Definitions (Identifiers)

What are Consumer Identifiers?

PHI includes information by which the identity of a consumer can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. Some examples are listed below.

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth, date of death)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

MISSOURI DEPARTMENT OF MENTAL HEALTH

HIPAA Definitions (Uses/Disclosures)

What Are Uses and Disclosures?

- **Uses**
  - When we review or use PHI internally (i.e. audits, training, customer service, or quality improvement).

- **Disclosures:**
  - When we release or provide PHI to someone (i.e. attorney, patient or faxing records to another provider).

Using and Protecting PHI

HIPAA and DMH Policies require staff granted access to our consumer data to:

- Assure that a consumer's PHI is only released to authorized individuals or agencies.
- Access and use a consumer's health record only as required to perform job duties and limited to the minimum necessary to complete duties.
- Sign a confidentiality agreement.
- Not discuss confidential or personal health information in a manner or place where the discussion could easily be overheard.
- Remove from public view records and files containing PHI when leaving a workstation (e.g., place in desk or file drawer, lock computer screens).
- Secure against unauthorized access at any location, including their home, to all documents and equipment that may include PHI (e.g., laptops, smart phones).
- Be sure to turn device screens away from the view of others.

Why Do We Need to Protect PHI?

- It's the law.
- To protect our reputation.
- To avoid potential withholding of federal Medicaid and Medicare funds.
- To build trust between providers and consumers.

If consumers feel their PHI will be kept confidential, they will be more likely to share information needed for care.

Who or What Protects PHI?

- **Federal Government** protects PHI through HIPAA regulations
  - Civil penalties imposed are based on each record disclosed.
    - Tier A Penalties are imposed when the offender did not know, and by exercising reasonable diligence would not have known
      - $100 for each violation, up to a max of $25,000.
    - Tier B Penalties are imposed if the violation was due to reasonable cause and willful neglect
      - $1,000 for each violation, up to a max of $100,000
      - For the most serious violations, the penalty is $50,000 per violation up to $1.5 million for each incident. al gain, or malicious harm.
- **Covered Entities**, through the Notice of Privacy Practices (NPP).
  - Employees who fail to comply with HIPAA are subject to disciplinary actions up to, and including, termination.
- **You as an employee**, by following our policies and procedures.

Criminal Penalties

Section 1177 of the HIPAA law established criminal penalties if a person knowingly violates the law. The possible penalties are as follows:

If a person knowingly obtains or misuses PHI in violation of the regulations, they could be fined up to $50,000 and sentenced up to one year in jail.

If the misuse of PHI involves or is done under false pretense, the person could be fined up to $100,000 and sentenced up to five years in jail.

If the misuse is for commercial or personal financial gain, or done for malicious harm, the person could be fined up to $250,000 and sentenced up to ten years in jail.

Breach Notification

Definition of Breach (45 C.F.R. 164.402)

A breach is defined as "an unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the privacy or security of such information."

"Unsecured protected health information" means protected health information (PHI) that is not encrypted or rendered unusable, unreadable, or indecipherable to unauthorized persons.

For instance, a lost or stolen laptop or mobile storage device which contains unencrypted PHI would be deemed a breach. If the PHI on the device is encrypted, it is considered secure and deemed to not be a breach.

What to do when a Breach occurs

Given the exceptions to the definition of a breach and the possibility of PHI being encrypted, if you have reason to be concerned that PHI has been breached, notify your supervisor promptly.

If you become aware of a possible breach on an agency's electronic security system, you are responsible for reporting the incident to your supervisor. Your supervisor should contact the DMH Chief Security Officer (CSO) promptly.

It's Important!
You Must Report HIPAA Violations

- So they can be investigated, managed, and documented
- So they can be prevented from happening again in the future
- So damages can be kept to a minimum
- To minimize your personal risk
- In some instances, the organization may be required by law to notify affected parties of lost, stolen, or compromised data

MISSOURI DEPARTMENT OF MENTAL HEALTH

Question 1 True or False

It is ok to leave specific details regarding a consumer's treatment plan with their spouse or on an answering machine if they are not at home when I call them.

Question 1 Answer

False

A spouse answers the phone, or voice mail picks up. What information may I provide?

- State your first name and that you are calling from [Organization name] (include the site).
- Ask the patient to return your call and provide your direct phone number.
- Do not provide lab results, or other detailed information, other than an appointment reminder.
- Example: “This is Sally from [Organization] calling for Johnny Doe. Please call me back at your earliest convenience at [number]. Thank you.”
- Ensure call is disconnected.

HIPAA Security Rule

- In general, the HIPAA Security Rule requires covered entities and business associates to do the following:
  - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is created, received, maintained or transmitted.
  - Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
  - Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule.
  - Ensure compliance with security by its workforce.

How We Apply the Security Rule

Administrative Safeguards

Policies and procedures are REQUIRED and must be followed by employees to maintain security (i.e. disaster, internet and e-mail use)

Technical Safeguards

Technical devices needed to maintain security.

- Assignment only level of access required to do the job
- Devices to scan ID badges
- Unique User ID / Strong Password
- User Authentication
- Audit trails

Physical Safeguards

Must have physical barriers and devices:

- Lock doors
- Monitor visitors
- Secure unattended computers

MISSOURI DEPARTMENT OF MENTAL HEALTH

Access to ePHI

Information Access Management

- Providers must implement technical policies and procedures for requesting access to the Department of Mental Health electronic information systems to ensure access is given only to those persons or software programs that have rights as specified in the HIPAA Security Rule

What Can I Do to Help Protect Our Computer Systems and Equipment?

- Workstation use
  - Operating systems are kept current with security patches
  - Current anti-malware and virus protection is installed and updated regularly
  - Restrict viewing access to others
  - Follow appropriate log-on and log-off procedures
  - Lock your workstation when not in use
  - Use automatic screen savers that lock your computer when not in use

- Know and follow organizational policies
- If devices are lost, stolen or compromised, notify your supervisor immediately!
- Do not store PHI on mobile devices unless you are authorized to do so and appropriate security safeguards have been implemented by your organization

MISSOURI DEPARTMENT OF MENTAL HEALTH

Safeguarding PHI

Confidentiality

- Securing information from improper disclosure also includes
  - Sharing PHI with only those that need to know (direct care workers, staff) in a discreet manner
  - Refraining from discussing consumer visits, conditions, progress, etc. with family, friends, neighbors, and co-workers that do not have a need to know
- Ensuring the disclosure of information reaches the intended person:
  - Verification of identity prior to releasing information without the consumer present
  - Requesting verbal authorization from the consumer to discuss their health, conditions, medications, or other PHI with those who may be present

MISSOURI DEPARTMENT OF MENTAL HEALTH

Safeguarding PHI

Availability

- Ensuring those that require information for proper treatment, payment or health care operations have access to the information they need to fulfill their job obligations
- Limiting the access to information to those that do not require access to perform the obligations of their job

Safeguarding PHI

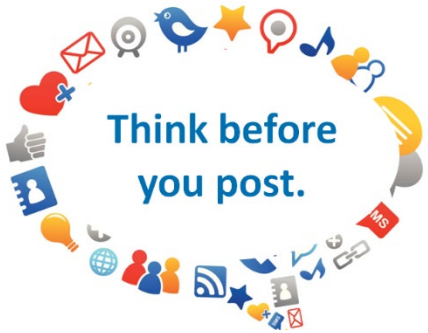
Integrity

- Ensuring the electronic transmission of data is secured in a manner to protect the integrity of the data. Protecting data integrity may include using:
  - Secure e-mail or
  - Organization communication portals that transfer files within or external to the organization for treatment, payment or operation purposes

Safeguarding PHI

Family, Friends, You and PHI

- 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.
    - Why? Your friend may hear about the car accident on the news and know the person involved
- Do not inform anyone that you know a famous person, or their family members, were seen at this organization



Safeguarding PHI

Social Media

- The HIPAA Privacy Rule prohibits the use of PHI on social media networks without the consumer's written consent and only for the specific purpose mentioned in the consent form. That includes any text about specific consumers as well as images or videos that could result in a consumer being identified.
- Social media such as Snapchat, Facebook, Twitter, or Instagram are common applications used to post health tips, exchange knowledge, introduce new staff and communicate with peers.
- While social media presents many benefits, the potential pitfalls are not always obvious. Even a seemingly innocent post on social media could have disastrous repercussions if you were to disclose a consumer's PHI without consent. This is a direct violation of HIPAA and Department regulations.
- Don't assume that any posts are "private" or have been deleted and cannot be viewed, shared, or saved by others.

Safeguarding PHI

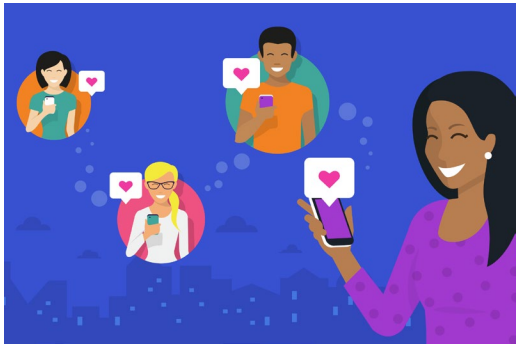
Social Media Examples

Examples of common social media violations include:

- Posting of images and videos of consumers without their consent
- Posting "gossip" about a consumer, even if their name is not disclosed
- Posting any information that could allow an individual to be identified
- Sharing photographs or images taken inside a healthcare facility with consumers or PHI visible
- Sharing photos, videos, or text within private groups
- Sharing a seemingly innocent photo of your lunch, which happens to include a visible consumer file beneath your sandwich

Question 2 True or False

Your facility is having a summer picnic for staff and patients on the floor where you work. While at the event your co-worker takes a picture with you. A few patients can be seen in the background. She should post the photo on social media with the caption "Having a great time with House 8!" so that everyone can see how great your work treats the staff.



Question 2 Answer

False

- **Although the PHI in the photo is accidental and your co-worker meant no harm, someone viewing the photo may recognize the one of the patients and now knows the individual is a patient in the facility, which is a breach of the patient's privacy.**
- **The best way to prevent accidental exposure of PHI on social media is to not take photos in the workplace and to not post anything related to the patients at the facility where you work.**

Question 3 True or False

A hospital billing department employee sees her son's girlfriend has been admitted to the same hospital. The employee is concerned about the girlfriend. The employee should look up the girlfriend's medical record to find the diagnosis and text her son the information.

Question 3 Answer

False

- **The billing department employee should refrain from looking up the patient's medical record.**
- **The employee does not have a need to know as she is not directly involved in the patient's care.**
- **The employee cannot disclose any information she sees or overhears at the hospital regarding the patient to her son or any other parties as this would be a breach of the HIPAA Privacy Rule.**

Social Security Administration (SSA) Federal Standards

- The following are the requirements and procedures for the exchange of electronic information with the SSA.
  - The SSA is required by law to oversight of the protected information it provides to the Department of Mental Health (DMH) and is utilized by department employees, contractors and providers.
  - All DMH employees, contractors and providers who access SSA-provided information must be trained as to the sensitivity and protection of SSA-provided information.
  - DMH employees, contractors and providers are subject to and must comply with the Privacy Act of 1974, the Federal Information Security Management Act (FISMA) and relevant policy issued by the National Institute of Standards and Technology (NIST) when accessing or using SSA-provided information.

Safeguard of SSA-Provided Information

- All DMH employees, contractors and providers agree to:
  - Protect SSA-provided information with efficient and effective security controls.
  - Only use SSA-provided information for a legitimate work purpose. Viewing and copying of SSA-provided information for a non-work purpose is prohibited.
  - SSA-provided information shall be disposed of properly and timely when no longer needed.
  - Report a breach or loss of SSA-provided data immediately to a local DMH Privacy Officer.
  - Follow procedures to protect the network from malware attacks, spoofing, phishing and pharming, and network fraud prevention.
- Misuse of SSA-provided information may lead to criminal, administrative, and civil sanctions, contract termination, and/or employee discipline.

MISSOURI DEPARTMENT OF MENTAL HEALTH

What is protected SSA-Provided Information?

- The Electronic Information Exchange (EIE) is an electronic process in which PII under SSA control is disclosed to a third party. DMH uses SSA-provided information to verify and add client information in CIMOR.
- The information includes personally identifiable information (PII) defined as information used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with another personal or identifying information, that is linked or linkable to a specific individual, such as date or place of birth, mother's maiden name, etc.

CIMOR Access

- By accessing CIMOR, DMH employees, contractors, and providers are acknowledging that they will abide by, not only the DMH department operating regulations (DORs), but all relevant federal laws, restrictions on access, use, disclosure, and the security requirements contained within the department's agreement with SSA.
- A copy of the SSA agreement and related documents are available on the DMH Portal for review.

Summary

Federal law provides that PHI is confidential information and the Department of Mental Health, and their Business Associates MUST protect this information from unauthorized releases.

Access must be limited to the minimum necessary data in performing a person's job.

Federal law has defined a breach of PHI as an unauthorized acquisition, access, use, or disclosure of their unsecured PHI that compromises the privacy of security of such information.

All employees are required to promptly report suspected breaches.

Potential penalties for careless, negligent, and intentional disclosures have dramatically increased.