HIPAA: Health Insurance Portability & Accountability Act

HIPAA Privacy Training Objectives

Section 1. **WHY** HIPAA Matters
- Regulations
- Respect for our Patients’ Rights
- Non-Compliance may result in disciplinary action

Section 2. **WHAT** HIPAA Protects
- Individually Identifiable Health Information (IIHI)- PHI

Section 3. **HOW** We Protect PHI
- Safeguards, Minimum Necessary, Proper Use and Disclosure
- HIPAA is Everyone’s responsibility

Section 4. Tips for **PREVENTING** HIPAA Violations
- Tips for common --BUT PREVENTABLE violations

Section 5. Reporting and Contact Information
- For Complaints, Concerns, General Questions, Policies & Schedule Training

Protected Health Information
Is Information Mission maintains about a patient- it includes:
ALL Types such as: clinical, scheduling, financial, billing, & ANY Form such as: Computer, Paper, Conversations, etc.
HIPAA: The Regulation

The Health Insurance Portability & Accountability Act

Section 1. WHY HIPAA Matters

- It is a Federal law
- Provides Privacy and Security Standards for medical information
- Governed by DHHS - Office for Civil Rights (OCR)
- Rules include: Privacy, Security (e-PHI), Breach Notification & Enforcement (Penalties)

The Privacy Rule

Defines Patients’ Rights concerning their PHI.
Outlines Our Responsibilities related to Use & Disclosure of PHI.

Non-compliance with HIPAA may result in:
Significant Fines; Criminal Charges; and/or Corrective Action up to and including possible Termination of employment.

⚠️ Last year 309 team members were subject to disciplinary action due to HIPAA non-compliance; 14 team members were terminated.
HIPAA: Patients’ Rights

Section 1. WHY HIPAA Matters

- It is the **right** thing to do for our patients
- **Mission Health is committed** to protecting our patients’ privacy, which:
  - Creates trust
  - Improves openness, where patients are more likely to share information about sensitive diagnoses
  - Prevents PHI from possibly getting into the wrong hands

**Patients’ have the following rights regarding their PHI:**

- Receive a copy of their PHI (paper or e-medical record)
- Request corrections to their PHI (amend)
- Request confidential communication
- Request limits to our sharing (Disclosure)
- Opt-out of Hospital’s Directory; HIE; & Fundraising
- Request a listing of disclosures (accounting)
- Receive a copy of the Notice of Privacy Practices (NPP)
- Choose someone to act on their behalf
- File a HIPAA Privacy complaint

**Protected Health Information** is information Mission Health maintains about a patient. It includes: **ALL** Types such as: clinical, scheduling, financial, billing, & **ANY Form** such as: Computer, Paper, Conversations, etc.
HIPAA: Patients’ Rights

Section 1. WHY HIPAA Matters

Permissible uses or disclosures of PHI:
1. Treatment,
2. Payment (limit to minimum necessary)
3. Health Care Operations (limit to minimum necessary)

Or
• With A Valid Authorization

For Guidance related to Uses and Disclosures in these, or other areas contact: Privacy, Risk Management, or the Legal Department
• Protected Information, such as Psychotherapy Notes
• Research
• Marketing
• Fundraising
• Employment Records
• Legal Requests- court orders or subpoenas
• Law Enforcement Requests

Protected Health Information is information Mission Health maintains about a patient. It includes: ALL Types such as: clinical, scheduling, financial, billing, & ANY Form such as: Computer, Paper, Conversations, etc.
HIPAA: Protected Health Information

Section 2. WHAT HIPAA Protects

The Privacy of Individually Identifiable Health Information (IIHI)-containing ANY of 18 PHI identifiers.

Related to past, present or future physical or mental health or condition; including treatment and payment.

Examples of PHI: demographics, scheduling, billing, prescriptions, care documents, orders, if it contains ANY of the 18 identifiers.
HIPAA: OUR Responsibilities

Section 3. HOW We Protect PHI

- Safeguards: Securing all PHI whether Paper, Electronic, or Verbal
- Contracts with vendors - Business Associate Agreements (BAA)
- For Violations and/or Breach of PHI
  - Sanctions – Corrective Action up to and including termination of employment
  - Notifications to Patients, Federal & State Agencies, and potentially Media Outlets

- Policies & Procedures
- Training
- EMR - Automated Monitoring and Reporting of user access

Co-Workers
Neighbors
Your OWN record
Family Members
Etc…
HIPAA: OUR Responsibilities

Section 4. Tips for PREVENTING HIPAA Violations

1. Access only information that you "need to know" to perform your job.
   - Access is monitored as required by HIPAA.
   - Do not access your OWN or your child's PHI (request copies from HIM or view through the patient portal).
   - It is inappropriate to access your PHI for TRAINING purposes. Contact IT to receive details for using “test” patients. *this is a violation of the Corrective Action Policy.

2. When asked for patient information, consider:
   - Who is asking for the information? Are they authorized?
   - Why do they need it?
   - How much should be released? Limit PHI to Minimum Necessary unless needed to provide treatment.

3. Communication of Confidential or Patient Information
   - Speak quietly. Be aware of your surroundings. “Who can overhear?”
   - Do not share PHI with others who should not have access, including co-workers or personal acquaintances.

4. Records containing PHI
   - Never leave PHI unattended or visible where accessible to the public. Ex: office doors or desks
   - Do not remove PHI from the facility unless approved by IT.
   - Double-check names on documents PRIOR to giving to a patient (discharge papers, prescriptions, orders).
   - Do not place PHI in the trash. Only dispose it into a secure Shred-It bin.

5. Social Media
   - Never post any reference to a patient on social media or websites, whether private or public.

Access your record through Mission Patient Connect at mission-health.org/patientconnect
HIPAA: OUR Responsibilities

Section 4. Tips for **PREVENTING** HIPAA Violations

6. **Computers and Email**
   - NEVER disclose your user ID or password to anyone.
   - Lock your computer (ctrl-alt-delete) before walking away.
   - Do not allow anyone to use your log-in credentials to access information.
   - EMAIL: Try to avoid using email to communicate PHI.
   - If you must use email, please encrypt by placing the word “confidential” in the subject line.
   - Do not forward emails containing PHI to your personal email address.
   - Do not open suspicious emails or click on links in messages unless you are sure of their authenticity.

7. **Monitors**
   - Turn computer monitors so they cannot be viewed by unauthorized persons.
   - Ask your supervisor for privacy screens if your monitor is viewable to the public.

8. **Printers and copiers**
   - Ensure you are selecting the correct printer, Use the “lock-print” function, never leave papers unattended.

9. **Faxes**
   - Prior to sending, complete verification steps. (See Faxing Policy 2IM.ADM.0019)
   - Remove incoming faxes immediately.

10. **Reporting**
    
    **ALWAYS Report** any suspected or known privacy or security incidents:
    - Lost or stolen devices containing PHI, such as a laptop, iPad, phone, external thumb drive or any other media.
    - Documents given to incorrect patient; Misdirected faxes; Patient complaints about HIPAA or privacy; Co-workers disclosing PHI to unauthorized person, or inappropriately accessing records
    - Prior to sharing PHI with a 3rd party, you must confirm the disclosure has received approval from Legal, Privacy or Information Security.
Section 5. Key Points, Reporting and Contact Info

**Key Points**

- Access only "**need to know**" info to perform your job.
  - *Ask yourself, “Do I need to access this patient’s information to do my job?”*
- Share (**disclose**) PHI only where authorized - to authorized individuals.
- When in doubt, seek guidance from policies, your supervisor, or the HIPAA Privacy Office.
- Violations must be mitigated and could lead to disciplinary action up to and including termination, as well as civil, -- criminal charges - and/or significant fines.
- **ALWAYS** report known or suspected incidents immediately.

**Reporting Information**

**Mission Health’s Privacy Department**

- Executive Director, HIPAA Privacy Officer
  - **Beth Cirillo** (828) 213-8540
- Manager, HIPAA Privacy
  - **Brooke Styles** (828) 213-8536
- HIPAA Privacy Specialists
  - Andrea Budd (828) 213-8541
  - Ellen Rowe (828) 213-8080

**Anonymous Reporting**

- Compliance Hotline 1-877-ETHICS1
- MOD form Online Reporting

**Additional Information**

**Policies:** *Search HIPAA, PHI, privacy, etc*

**MOD Privacy Department page- reporting form**

**Email:** [HIPAA@msj.org](mailto:HIPAA@msj.org)