HIPAA Education Program

2017-2018

Assurance and Compliance Services

Mount Sinai

HIPAA Training Requirement

This HIPAA Training Program is intended for and will satisfy the training requirement for the:

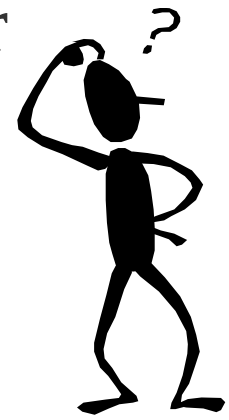
- Mount Sinai PPS, LLC and its Partners
- Mount Sinai Health Partners

What is HIPAA ?

- Official Name – Health Insurance Portability and Accountability Act of 1996

- Effective Date: Privacy Standards: April 2003
  Security Standards: April 2005

- Established National/Federal Standards for Safeguarding Patient Information
  -Applicable to Covered Entities, such as Hospitals, Nursing Homes, Health Plans, Physicians, etc.)



Legal Foundations of Patient Privacy

Where do we Find our Obligation to Protect Patient Information?

- Federal Law – HIPAA Legislation & Medicare Conditions of Participation
- New York State Law – Patients' Bill of Rights, New York State Public Health Law
- Joint Commission Standards – Minimum Standards

HIPAA Privacy Rule

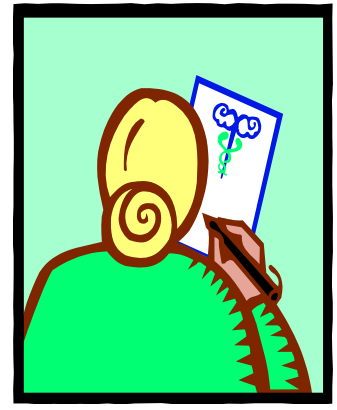
- **HIPAA Privacy Rule**:
  - Imposes Restrictions on the Use and Disclosure of Personal Heath Information
  - Gives Patients Greater Access to Their Medical Records
  - Gives Patients Greater Protections of Their Medical Records

Protected Health Information

Protected Health Information (PHI) is any information relating to a patient (demographic, financial, social, clinical) that is attached to an Identifier.

All of the following are examples of I**dentifiers:**

Name; Address; Zip Code; Email/IP/URL Addresses; SSN; MRN; Telephone/Fax #; Date of Birth; Date of Service; Date of Death; Account Numbers (health plan, credit cards); Images (full face, dental x-rays, tattoos); as well as ANY other unique identifying characteristic(s)

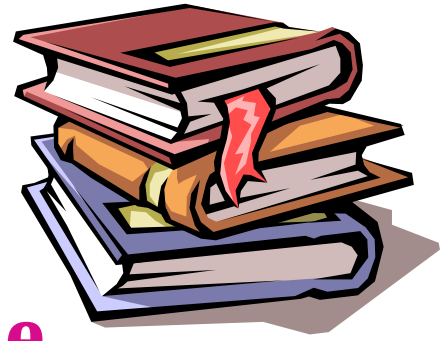


PHI: can be Oral, Paper, Electronic

Examples: Diagnosis, Prognosis, Appointment Dates; Admission/Discharge Dates; Billing Information; Lab Results, Etc.

ePHI: Electronic Protected Health Information

Disclosure of PHI



When are you Permitted to Disclose PHI Without Specific Patient Consent?

- **For Reasons Related to: T P O**
  - Treatment – Managing, Coordinating and Providing Health Care
  - Payment – Activities Relating to Obtaining Payment for Services
  - Healthcare Operations – Administrative, Financial, Legal and Quality Improvement Activities

Disclosure of PHI (Cont'd)

- **Public Interest Disclosures are Also Permitted Without Patient Consent. These Include the Following Purposes:**

  - Public Health Activities
  - Reporting on Victims of Abuse, Neglect, Domestic Violence
  - Judicial Proceedings
  - Law Enforcement Purposes
  - Coroners, Funeral Directors, Medical Examiners
  - Information for Organ Donation
  - To Avert a Serious Threat to Health or Safety
  - Workers' Compensation

Disclosure of Specially Protected PHI

Certain elements of PHI have protections additional to those provided under HIPAA. These elements include HIV related, psychiatric/mental health treatment, alcohol/substance abuse treatment and genetic information.

The patient has to specifically authorize the release of Protected Information by checking a specific box on a general HIPAA authorization form or using a special authorization form specific to the Protected Information. If the specific authorization is not provided, you may not disclose the information.

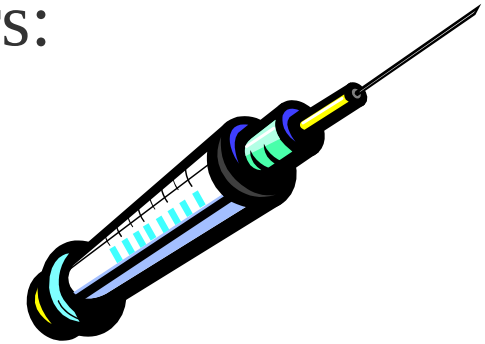
Exceptions to authorization to disclose HIV related information include:

- for treatment purposes ***only*** as needed to provide necessary care
- with an insurance company ***only*** if necessary to obtain payment
- with authorized corrections staff if the person is in jail or on parole
- under certain circumstances when there is an occupational exposure
- with health oversight agencies for the purpose of surveillance and public health (including partner notification)

Business Associates Agreements

- Vendors and Contractors who are Engaged by the Covered Entity to Perform a Service on the Covered Entity's Behalf with Whom the Covered Entity Shares PHI Must Enter Into a Business Associate Agreement Whereby They Agree to Follow the HIPAA Regulations.

- Examples of Business Associate Vendors:
  - Billing Companies
  - Transcription Services
  - Malpractice Law Firms



Notice of Privacy Practices

- Written Notice That Is Provided to Patients Upon Their 1st Treatment Encounter
- Informs Patients Of Their Rights Regarding Use And Disclosure Of Their PHI
- Informs Patients Of Our Organizational Obligation To Protect/Safeguard Their PHI
- Must Be Posted In Patient Registration Area And Web Site
- Provides Avenue for Redress of Patient Complaints
  - Privacy Officer
  - Office for Civil Rights (OCR) – Dep't of Health & Human Services (HHS)

Patients' Rights

Patients Can Request:

- That Their PHI be Shared With Family/Friends
- Confidential Communications – (i.e., Only Send Bills/Letters to Home/Work/Etc.)
- Not Receive Fundraising Communications
- Not be Listed in Inpatient Facility Directory Listing
- An Accounting of Disclosures – to Whom did we Send Their PHI to Without their Authorization

Patients' Rights (Cont'd)

Patients Also Have the Right To:

- Access Their Medical Records (Either Receive a Copy or View Original Record Under Supervision)
- Request an Electronic Copy of an Electronic Record
- Request an Amendment to Their Medical Record
- Request Limits on Disclosure, Including Not Disclosing to an Insurance Carrier if the Encounter is Paid for in Cash.

Access, Use, and Disclosure

- You May Only **Access** The Information You Need To Do Your Job
- You May Only **Use** Information For The Purpose Of Completing Job Related Tasks
- You May Only Share/**Disclose** Information With Those Who Are Authorized To Receive It

Only the Minimum Necessary Information Can be Accessed, Used or Disclosed

Minimum Necessary Standard

- **Two (2) Aspects:**
  - Health Care Staff Should Only Access, Use or Disclose the Least Amount of PHI Necessary to Carry Out a Particular Purpose or Function
  - Staff Should Only Access PHI if They Have a Job-Related Need to Know It

- **Example**: A Patient Who Uses a Wheelchair is Admitted for a Same Day Procedure on her Knee. Her Neighbor Picks her Up and Drives her Home. The Neighbor will Not be Giving the Patient Medications or Changing Her Dressings – She is Just Providing a Ride.

  In this Situation, Minimum Necessary Would Include Instructions on Safe Transfer Into the Car and Assistance with Getting Out of the Car and Into her Home. Sharing the Details of the Procedure, Diagnosis, Medications, Follow-Up Appointments, etc. is not Necessary for the Neighbor to Assist the Patient in Getting Home.

Roxanne Registration Scenario

- Roxanne is Checking in at Registration Desk for her Appointment
- Roberta the Registrar is Asking Roxanne to Verify her Insurance and Change of Address
- Penelope, the Next Patient in Line Behind Roxanne can Overhear the Verbal Exchange of PHI Between Roxanne and Roberta

–Is This a HIPAA Issue/Concern?

Incidental Disclosure

YES, It Is A Concern!

Incidental Disclosure is When PHI is Unavoidably Disclosed in the Course of Taking Care of a Patient.

Staff are Required to Take Reasonable Safeguards to Avoid Inadvertent Disclosures:

- Ask Penelope to Have a Seat and She Will be Called When you are Finished with Roxanne
- Do not Discuss Patients in Public Places Including Hallways, Elevators, Cafeteria
- When Discussing Patients, Close Curtains/Doors
- Be Aware of who is Around you Before you Start Speaking - Especially When Using Your Telephone or Other Communication Devices
- Be Attentive to Volume and Tone When Speaking: Voices Carry.

One More HIPAA Hypothetical

- Applicable to Inpatient or Outpatient Location
  - Physician Needs to Speak to the Patient About Their Care
  - PHI will be Part of the Discussion
  - The Patient Has Family Members in the Room With Her
- What is the Best Means of Speaking With the Patient About Her Laboratory Test Results/CT Scan, Etc.?

Special Circumstances

- **Dealing with Family Members**

  - Ask Visitors to Step Out. Confirm with the Patient Privately What can be Shared and with Whom.
  - Alert/Invested Patients Determine Who May Know What
  - Even Alert Patients are Subject to Subtle Pressure
  - By Law We Must Provide Professional Translators (Family Translators are the Last Resort)
  - **Family Politics are a Potential Minefield!**

Privacy Breaches

- **Since 2003 – Over 91,000 Reported Allegations of PHI Breaches**
- **Unauthorized Access or Disclosure of PHI**
  - **Misdirected Fax, Email, Snail Mail**
  - **Loss or Theft of Unencrypted Data on Computer Hardware**
  - **Mishandling of Confidential Waste**
- **$$$ Fines – Up to $1.5 Million**
- **Adverse Media Publicity**
- **Additional Federal Oversight – (i.e. Audits)**

HIPAA Security Compliance with Computer/Devices Policies

- Encryption Policy – PHI That is Electronically Transferred Needs to be Encrypted
- User IDs and Passwords – Sharing of User IDs and Passwords is Not permitted
- Logging off of PCs/Workstations When Done is a Must

Data Security: Workstation Security

- **Use Strong/Unique Passwords** (at Least 8 Characters, Upper and Lower Case Letters, Numbers, Special Characters). Do Not Use the Same Password For Your Personal Accounts and Your Workstation System Access.
- **Never Share Your Password** or Allow Someone to Access a System Using your Log-On Credentials. Lock your Workstation or Log Out of Applications When you Step Away.
- **Don't Let Someone Watch You Enter Your Password**
- **Don't Write Your Password** Where Others Can See It – Memorize it
- **Always Log Out or Lock Your Workstation** When You are Away From It

Data Security: Workstation Security

- **Privacy Screens** Should be Used When a Workstation is in a High Traffic or Public Facing Area.
- **Do Not Download/Install Unapproved Applications** Such as File Sharing or Software.
- **Contact Your IT Administrator** if you are Concerned Your Password has Been Compromised or Your Workstation has Been Infected With Malware.

MSPPS Partner and MSHP Expectations

- **Appoint a HIPAA Privacy Officer and Security Officer**
  - Duties Include the Overall Oversight of the HIPAA Program and Follow-Up on Complaints
- **Partner Employees' Responsibilities:**
  - Protect PHI From Improper Disclosure
  - Ensure you Access PHI Only for **TPO** Purposes
  - Protect and Do Not Share Computer Passwords
  - Do Not Discuss PHI in Public Areas
    (i.e. Elevators, Cafeteria, Public Areas, etc.)
  - Report Issues/Concerns to Management or to Privacy/Security Officer

Responsibilities

It is the Responsibility of Every Mount Sinai PPS and MSHP Workforce Member to Protect the Privacy, Integrity and Security of Patient Information.

You Should Notify the HIPAA Privacy Officer or Your Manager if You:

- Become Aware of a Misdirection (Electronic or Paper) of PHI
- Find Unsecured PHI.
- Become Aware of Any Unauthorized Disclosure or Access of PHI.
- Are Notified by a Regulatory Agency or Patient/Family of a Privacy Complaint

You Should Protect Information By:

- Accessing only the Minimum Necessary Information to do Your Job
- Disclosing Only the Minimum Necessary Information to Authorized Individuals
- Securing Hard Copy PHI and Disposing of it Properly
  - Shredder, Confidential Bin
- Using Encryption and Secure Emails
- Accessing Websites, Links, and Attachments Only From Trusted Sources

Questions