Privacy and Security for the Medical Student

HIPAA Compliance
Audit and Compliance Services
Mount Sinai Health System

Mount Sinai

Table of Contents

Confidential and Protected Information

Confidential and Protected Information

Confidential Information is information that is considered intellectual property of Mount Sinai; that Mount Sinai has proprietary(ownership) interest in; or is protected by contractual obligations. Examples are grants, contracts, payment agreements, information on the internal workings of Mount Sinai.

Protected Information is information that is protected by law or regulation. This includes information about employees and students, quality assurance work products, certain business information, and of course patient information **(PHI)**.

What is PHI?

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

ALL of the following identifiers would need to be removed for patient related information to no longer be considered PHI:

- ►Name
- ►Address
- ►MRN
- ►Telephone/Fax Numbers
- ►SSN
- ►Email/ IP /URL addresses
- ►Serial Numbers (VINs, device numbers,)
- ►All elements of dates other than year (date of birth, date of service, date of death)
- ►Account Numbers (health plan, credit card, bank, invoice, visit, or accession #s)
- ►Images (full face, dental x-rays, unique physical characteristics such as tattoos, clothes, abnormalities)
- ► ***ANY*** **other unique identifying characteristic(s)**

Access, Use, and Disclosure

Access and Use

You may access or request only the minimum necessary Protected Health Information (PHI) or Protected Information to complete a task.

You may not use PHI or Mount Sinai Protected Information or Confidential Information you have legitimate access to for any other purpose than to take care of your patient or perform your responsibilities.

You may only share PHI and Protected Information with individuals who are authorized to receive such information.

HIPAA: Privacy Rule

The Privacy Rule establishes standards on how to protect the confidentiality and privacy of patient information (PHI) and identifies permitted uses and disclosures of PHI.

The Privacy Rule also provides for patients' rights related to PHI including:

- Patient Access
- Request a correction
- Limit Uses and Disclosures of PHI

The Mount Sinai Health System Notice of Privacy Practices (NOPP) is provided to patients to inform them of how Mount Sinai will use and disclose their information and their rights related to their PHI.

Disclosure

PHI may be shared with anyone the patient or the patient's Personal Representative authorizes to receive it.

- the patient must consent to an observer being present; patients can decline having a medical student present.
- ask visitors to step out unless the patient indicates they can be present
- make sure you know what information can be shared and with whom
    - get authorization in writing using an approved form
    - if only verbal consent can be obtained, it must be documented

PHI can be disclosed without authorization for the purposes of Treatment, Payment and Health Care Operations (TPO). Only the minimum necessary information should be disclosed.

If a patient has paid for services in cash and requests that information related to that service is not disclosed to their insurance carrier, we are required to honor the request.

You may not disclose PHI to anyone who is not directly involved in the care of the patient or is not authorized by the patient/personal representative.

Special Circumstances: 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)

Special Circumstances: Incidental Disclosure

Incidental Disclosure is when PHI is unavoidably disclosed in the course of taking care of a patient.

Everyone must take reasonable steps to avoid inadvertent disclosures:

- do not discuss patients in public places including hallways, elevators, shuttles, cafeteria
- when rounding/discussing patients close curtains/doors
- be aware of who is around you before you start speaking – especially when using your phone or other communication devices
- be attentive to volume and tone when speaking: voices carry.
- unless you are aware a patient has agreed to having detailed messages left at a preferred number, only include enough information for a call back when leaving a message.

Special Circumstances: Public Domain

You may not discuss PHI in public without patient authorization even if the patient has spoken publicly.

Case studies of well-known cases or patients require authorization even if the name is not mentioned.

Special Circumstances: Social Media

- Protected Health Information (PHI), including photos of patients, should never be posted on your personal social media site.

- Patient authorization is needed for use of patient information/photos on professional sites.

- Where your connection to Mount Sinai is apparent, make it clear that you are speaking for yourself and not on behalf of Mount Sinai.

- If you communicate in social media about Mount Sinai, disclose your connection with Mount Sinai and your role within the Health System.

- Consult with the Marketing & Communications Department if you have any questions about the appropriateness of materials you plan to publish.

- If you are contacted by a member of the media about a Mount Sinai-related blog posting or MSHS information of any kind, contact the Press Office, a division of the Marketing & Communications Department, at (212) 241-9200 or newsmedia@mssm.edu

Special Circumstances: Social Media Use in General

Protect your Privacy. Customize the privacy settings on the sites you use and limit the amount of identifying information you include in your profile or posts. Information on social media sites can be collected and used to steal your identity or locate you in the real world. Read the privacy policies for the site, they may be sharing your information with third parties.

Think Before You Post. Once you post something, even if you remove it, the information is still somewhere on the internet. You are responsible for the material you post. Be courteous, respectful, and thoughtful. Inaccurate, inappropriate, threatening, harassing or poorly worded postings may be harmful to others. Think about how a picture or comment could affect others or affect how people think about you. If you would not want your mom, boss or patient to see it, don't post it.

Data Security

HIPAA Security Rule

The HIPAA Security Rule sets standards to ensure the security, confidentiality, integrity and availability of all electronic PHI (ePHI) we create, receive, maintain or transmit.

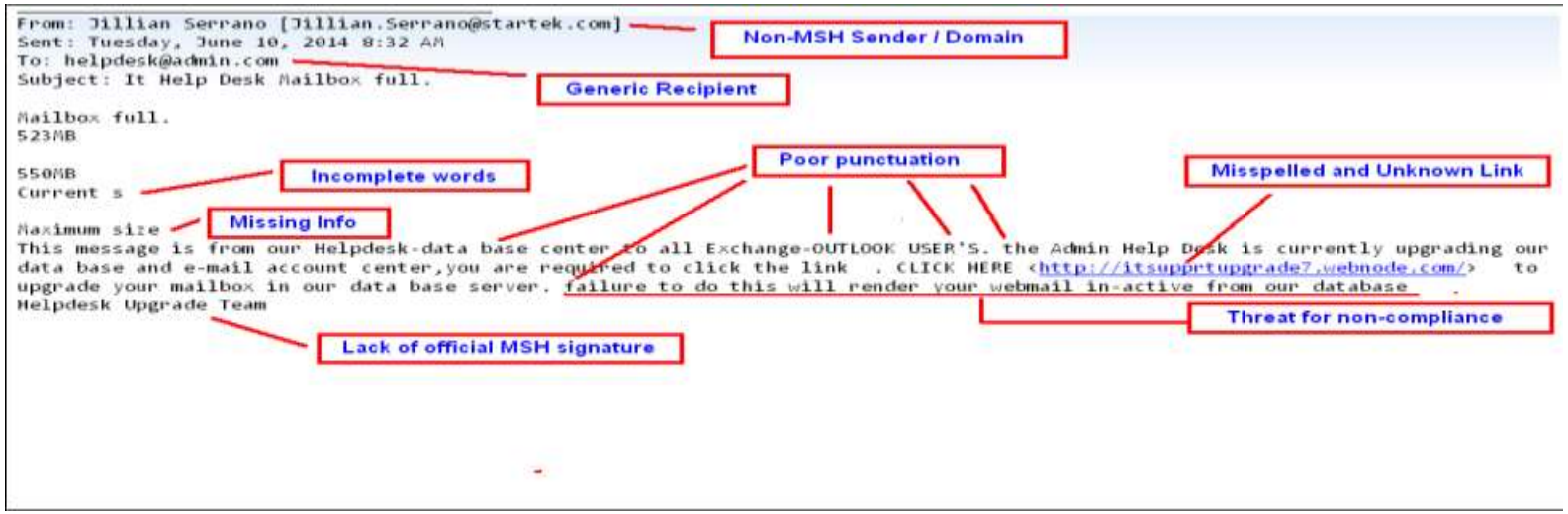
These same concepts are applicable not only to ePHI but other electronic Confidential and Protected information maintained by Mount Sinai.

Data Security: Workstation Security

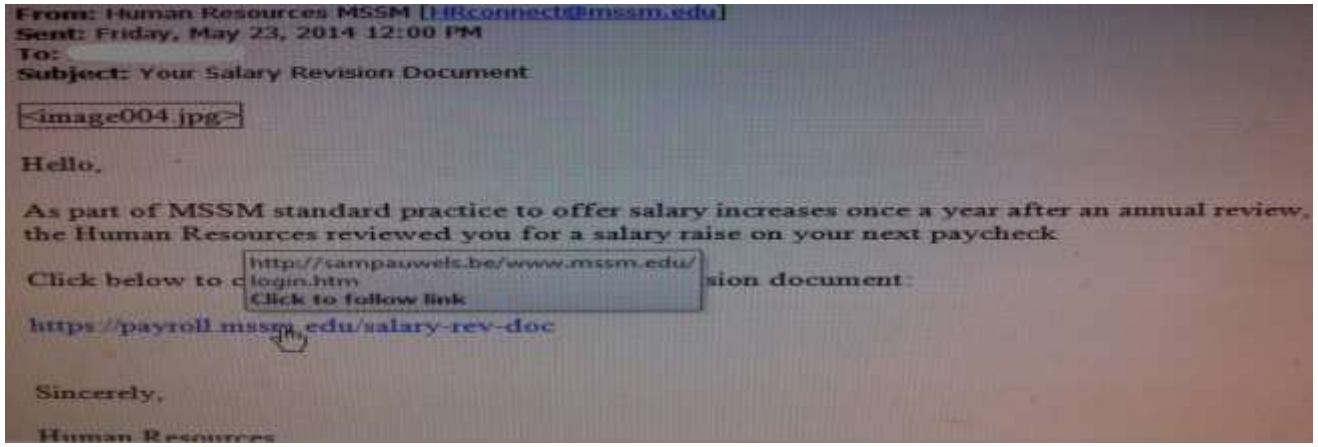
- **Use strong Passwords (8 characters, upper and lower case letters, numbers, special characters). Do not use the same password for your personal accounts and your Mount Sinai system access.**
- **Never share your password or allow someone to access a system using your logon credentials. Lock your workstation or log out of applications when you step away.**
- **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 on MSHS devices.**
- **Keep your workstation and laptop up-to-date with software patches and virus protection. On centrally managed workstations, shutting down will update the software.**
- **Contact IT Security if you are concerned your password has been compromised or your workstation has been infected with malware.**

Data Security: Internet Safety

- **Be alert to malware and phishing attempts. Do not open attachments or links from unknown senders or in suspicious emails. Do not access untrusted websites.**



- **Use the Hover feature of Outlook and most web browsers to verify the destination of web links.**



Data Security: Use of Email

Use caution when choosing to email Protected or Confidential Information.

- Only use your Mount Sinai email account when emailing PHI or Mount Sinai confidential or protected information.
- Emails containing PHI or Mount Sinai protected or confidential information may not be forwarded to your personal email account.
- Be extremely careful when “replying to all” or forwarding emails and attachments. Review To, Cc, and Bcc fields before sending an email.
- Always use secure email when sending PHI or Mount Sinai protected information to a non-Mount Sinai address.
- Password protect attachments containing protected information or PHI and send the password in a completely separate email.
- Limit the identifiers and/or the content when emailing PHI to the minimum necessary – even when communicating internally or using password protection.
- Immediately notify HIPAA Compliance if an email containing PHI is misdirected.

Remember: Once you send an email, you no longer control the information in it.

Secure emails

- All communications sent from your Google Apps account (@icahn.mssm.edu) to recipients within the Mount Sinai Health System (@mountsinai.org, @mssm.edu. @chpnet.org, @nyee.edu) are secure and meet HIPAA compliance standards. No action is needed on your part to ensure that these messages are protected.

- To send secure messages to recipients outside of the Mount Sinai Health System, you need to use an email add-on called Virtru. A learning module for using Virtru on an iPhone has been placed on Blackboard. To access it, log onto Blackboard and under “My Organizations”, select “Google Apps for Education”.

- To send secure messages from an @mountsinai.org or @mssm.edu account, include **[secure]** in the subject line.

Data Security: Use of Texting

At MSHS there is currently no information technology platform for secure, encrypted, HIPAA-compliant text communication.

In your current role as a medical student, you should not be texting PHI.

Data Security: Encryption and Electronic Data

- **All Mount Sinai purchased (including from grants or contracts) portable devices (USB drives, laptops, tablets) must be encrypted even if you do not intend to store Confidential or Protected Information.**
- **Encryption is required for any local storage (desk top, local drive/hard drive, USB drives, CD/DVD), including personal devices, of protected information/PHI. If the device cannot be encrypted the *file* containing the information must be encrypted.**
- **Only use approved portals for remote access to PHI or Mount Sinai protected or confidential information. Unapproved applications that share files or sync your workstation with another computer are prohibited.**
- **PHI, including appointments or schedules, may not be stored on public/free cloud services. Not all institutional /private cloud services are appropriate for use with PHI. Ask before uploading/transmitting PHI.**

Data Security : Physical Security and Disposal

- **Hard copy PHI and Mount Sinai protected information must be stored in a locked cabinet or desk. Hard copy PHI may never be taken home.**

- **Workstations that are not encrypted must have a security cable. (Contact your local IT support if you are not sure if your workstation requires a cable).**

- **PHI and Protected Information in any format (paper or electronic) that is no longer needed, and does not need to be maintained, should be disposed of in an appropriate manner.**

- **Dispose of hard copy PHI and protected/confidential information by placing it in a confidential bin or by shredding. If it cannot be properly disposed of immediately, it must be stored securely.**

- **Contact IT Security for proper disposal of any digital media (CD/DVD, diskettes, floppy discs, memory cards), USB devices or other hardware that may contain PHI or Mount Sinai protected / confidential information.**

Research and QI/PI

De-Identified Data

ALL of the following identifiers would need to be removed for patient/subject related data to be considered De-Identified and therefore no longer considered PHI.

- Name
- MRN
- SSN
- Address
- Telephone/Fax Numbers
- Email/ IP /URL addresses
- All elements of dates other than year (date of birth, date of service, date of death)
- Account Numbers (health plan, credit card, bank, invoice, visit, or accession #s)
- Serial Numbers (VINs, device numbers)
- Certificate/License Numbers
- Biometric identifiers (finger print, voice print, dental x-rays, etc)
- Images including full face or unique physical characteristics
- **ANY other unique identifying characteristic(s)**

Limited Data Sets and Very Limited Data Sets

- ~~Name~~
- ~~MRN~~
- ~~SSN~~
- **Address:** ~~house #,street,apt#,~~ **city, state and ZIP CODE**
- ~~Telephone/Fax Numbers~~
- ~~Email/ IP /URL addresses~~
- **All elements of dates (DATE OF BIRTH, date of service, date of death)**
- ~~Account Numbers (health plan, credit card, bank, invoice, visit, or accession #s)~~
- ~~Serial Numbers (VINs, device numbers)~~
- ~~Certificate/License Numbers~~
- ~~Biometric identifiers (finger print, voice print, dental x-rays, etc)~~
- ~~Images such as photos including full face or unique physical characteristics~~

A **Limited Data Set** is a data set that excludes **MOST** of the 18 identifiers defined in HIPAA, leaving only dates and limited address information.

A **Very Limited Data Set** excludes **ZIP CODE** and **DATE OF BIRTH** as well.

Access to PHI for Research

To access PHI, outside of a **Limited Data Set** or **Very Limited Data Set**, for the purpose of Research:

1) Need IRB approval and patient consent
2) Need IRB approval and a waiver of HIPAA authorization from the IRB
    a) the waiver of HIPAA authorization does not cover
        i. a person personally known to the researcher
        ii. a person who is MS employee
        iii. a person who is identified as “Public Figure”
3) In preparation to research a researcher can review the records of his/her ***own*** patients without specific authorization or waiver.
4) If you are accessing PHI with waiver, you need to request the data from the HIM/MR department or data base owner so that patients who are not covered are excluded and the disclosure can be tracked appropriately in case an **Accounting of Disclosures** is requested.

Access to Limited and Very Limited Data Sets for Research

Limited and Very Limited Data Sets are still PHI.

1) At Mount Sinai the IRB acts on behalf of the Privacy Office to review and approve requests for Limited Data Sets

2) A Data Use Agreement (DUA) is needed, even internally. The DUA:
    a) prohibits attempting to identify the individuals or contacting them
    b) prohibits using the data for any other purpose than indicated in the DUA
    c) prohibits disclosing the data to any one not named in the DUA
    d) requires the use appropriate safeguards to prevent use or disclosure not provided for by the DUA
    e) requires reporting of any use or disclosure not provided for by the DUA
    f) requires the recipient ensure that any of their agents/subcontractors agrees to the same restrictions.

Research vs Quality Improvement/Performance Improvement

HIPAA permits the use and disclosure of PHI for the purpose of Health Care Operations without patient consent. Only the Minimum Necessary information should be requested or disclosed. QI/PI activities fall under Health Care Operations.

The difference between Research and QI/PI activities can be subtle and in some cases QI/PI can also be Research, especially if there is a plan to publish findings. The issue of generalizability of results is key in the definition of research.

Whether or not the QI/PI activity is research or not, you should have a data security plan in place that is consistent with IRB requirements.

Responsibilities and Resources

Responsibilities

It is the responsibility of every Mount Sinai workforce member to protect the privacy, integrity and security of patient and Mount Sinai information.

You should notify the HIPAA Compliance Office or your preceptor 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
- Using encryption and secure emails
- Accessing websites, links, and attachments only from trusted sources

HIPAA Office

Privacy Officer

Louis Schenkel, VP Compliance

Security Officer

Raymond Shelton
646-605-7124

Directors

Heather Chamides
646-605-7130

Norman Werner
646-605-7140

Resources

Academic IT Support Center

ASCIT@mssm.edu

212-241-7091

MSHS IT Security

#secadmin@mountsinai.org

HIPAA Compliance: Policies and Forms

http://intranet1.mountsinai.org/compliance/hipaa_security_policy.asp

IT Security Intranet Page

https://wiki.mssm.edu/display/DS/Data+Security+Wiki

Department of Health and Human Services Office of Civil Rights

http://www.hhs.gov/ocr/privacy/index.html

PPHS/IRB: Polices, Forms, Education

http://icahn.mssm.edu/research/resources/program-for-the-protection-of-human-subjects