HIPAA: Overview of Use/Disclosure of Patient Information, Data Security and Integrity, and Patient Rights

Presenter Heather Chamides

New Provider Education

HIPAA Compliance Program
Assurance & Compliance Services

Mount
Sinai

The HIPAA Compliance Program at Mount Sinai is responsible for:

- Development and implementation of HIPAA related policies and procedures
- HIPAA Training and Education
- Investigation of privacy and security breaches and/or complaints
- Auditing and monitoring of system access
- Management of ID theft program

HIPAA Compliance Contacts

MSHS Privacy Officer, VP Compliance

Louis Schenkel
Louis.Schenkel@mountsinai.org

Director, HIPAA Compliance

Heather Chamides
Heather.Chamides@mountsinai.org

HIPAA Security Officer

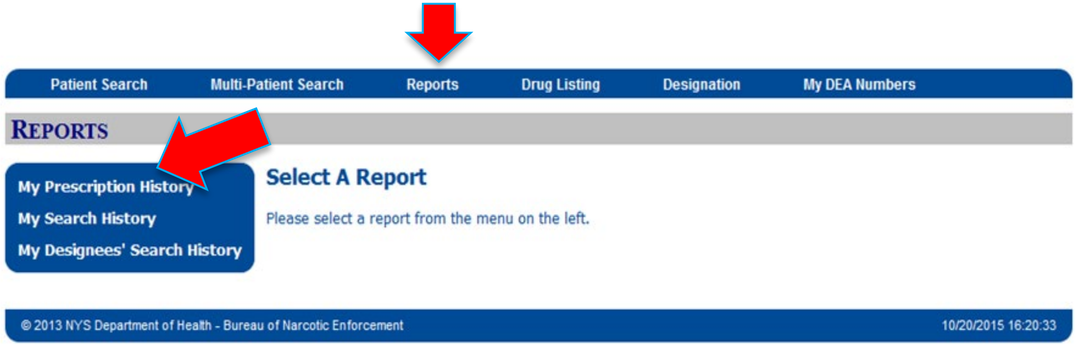
Raymond Shelton
Raymond.Shelton@mountsinai.org

Provider ID Theft / Drug Diversion

Providers are at growing risk for ID Theft related to drug diversion. Simple actions you can take to protect yourself:

- Run report in iSTOP on activity/orders attributed to your DEA # at least twice a year. (see next slide)
- Do not order prescription pads with your DEA # pre-printed.
- Keep your prescription pads/paper secure at all times.
- Use one pad at a time and keep track of the numbers on each pad, which pads you have completed, and the numbers of prescriptions you have written. If you learn your pad or prescriptions may have been stolen / misused you will need to report to Narcotics Enforcement the specific prescriptions that have been compromised or stolen.

In addition to the patient-focused search, you can view other reports, including one presenting the narcotics prescriptions ISTOP attributes to your DEA number.



Select A Report

Please select a report from the menu on the left.

© 2013 NYS Department of Health - Bureau of Narcotic Enforcement
10/20/2015 16:20:33

Select “My Prescription History.”

When search activity related to your DEA number, there is no limitation on the time period you can review.

Data Integrity: Impact to Patient Safety

- Patient may receive inappropriate care based on incorrect info or lack of access to correct info;
- Patient identification and verification is affected;
- Inaccurate Epic alerts can be triggered/not triggered;
- Can cause delays in obtaining prior approvals for needed services;
- Can negatively impact the patient accessing care in the community (such as filling prescriptions).

Comingling

Commingling occurs when information about more than one patient is associated with a single MRN.

Red flags:

- Name, DOB and/or sex discrepancy
- Clinical information on file is inconsistent with exam or history provided by the patient
- The patient reports significantly incorrect information is in their record including encounters/visits that do not belong to them.

Comingling: Registration Error

What to do:

- Notify the CNM/AOD and the clinical team; ask all staff to close the patient’s record in Epic and use downtime procedures;
- Staff will call the **Help Desk** for a **High Severity Ticket** that an active patient is registered to a wrong MRN
- *** EMPI staff will follow up on the ticket and will walk the floor through the rest of the process which depending on when and where the error is identified**

Duplicate MRNs

Due to issues with how some clinical systems process merges, we ***CANNOT*** merge two MRNs while the patient is active inpatient.

What to do:

- Immediately report the duplicate records to **EMPI team using the web tool below** so both records can be flagged in Epic. https://erap.mssm.edu/public/empi_merge_tool.aspx

  Intranet, → Applications Web Based, →I, J, L, M, -> MRNMerge.
- The records will be merged once the patient is discharged
- When you complete the form, indicate it is an **urgent request** and choose "Patient is active Inpatient" from the drop down for reason.

Unidentified Patients

Registered as :

- **Last Name**: Unknown
- **First Name**: A word from a set list assigned to each ED
- **DOB**: Day and month of presentation (e.g. 8/23); year is always 1900
- **Address:** The address of the ED that received the patient

What to do:

Notify the BA/Unit clerk if you are able to obtain the patients name, DOB or identify a previous MS MRN for the patient

Staff will:

- ▶ Update registration info once the patient is identified with a reasonable level of reliability
- ▶ If the patient has a pre-existing MS MRN, notify EMPI to mark for merge.
- ▶ Alert the clinical team of any other steps such as drawing a new Type and Screen specimen if one was previously sent using the place holder information.

HIPAA

(Health Insurance Portability and Accountability Act of 1996)

The purpose of the HIPAA regulations was to improve efficiency in healthcare billing, prevent fraud and abuse, protect patient privacy and afford patient additional rights and prohibit exclusion from healthcare coverage based on a preexisting condition when transferring from one job with healthcare coverage to another.

- Privacy Rule - April 14 2003
- Portability of Health Insurance – Dec 2004
- Security Rule - May 23 2005
- National Provider Identifier – May 2007

ARRA/HITECH/Omnibus

(American Recovery and Reinvestment Act of 2009)

- Direct Accountability for Business Associates – Feb 09/Sept 2013
- Notification of Breach – September 30 2009
- Enforcement – November 30 2009
- Interoperability – December 2009
- Patient Right to an Electronic Copy of Medical Record – Sept 2013
- Patient Right to Request Limitations on Use/Disclosure – Sept 2013

21st Century Cures Act

The 21st Century Cures Act addresses “data blocking” in terms of how Health Information Technology vendors develop their products as well as how health care providers, insurance plans, and health information exchanges (HIEs) use the technology to exchange data.

Providers are required to be able to exchange health information with patients and other authorized parties, such as other providers and health plans, in real time. The regulation does provide for some limited exceptions where withholding the information would be permissible.

These exceptions include:

- Privacy: patient consent is required or provider agreed to a request from the patient for a limitation on use/disclosure for a permitted purpose
- Preventing harm: there is an imminent risk for serious harm to the patient, others, or to public safety that would be substantially reduced if the information was withheld
- Infeasibility: the information is not maintained in a form/format where it is feasible to exchange as requested.

Mount Sinai uses various health information exchange/interoperability platforms to meet the requirements of this regulation.

Family Health Care Decisions Act (2010)

In the absence of a signed proxy if the patient lacks capacity the individuals below may make decisions and have access to the information necessary to do so in the following order:

- Court-appointed guardian
- Spouse or domestic partner
- Adult child
- Parent
- Brother or sister
- Close friend

Definitions

Organized Health Care Arrangement (OHCA) – components of the organization that may share PHI without authorization if appropriate. *(Icahn School of Medicine Doctors Faculty Practice, New York Eye and Ear at Mount Sinai, Mount Sinai Doctors Network Practices, Mount Sinai Beth Israel, Mount Sinai Brooklyn, Mount Sinai Hospital, Mount Sinai Morningside, Mount Sinai Queens, Mount Sinai South Nassau, and Mount Sinai West.)*

Designated Record Set (DRS) – the totality of information used to make a clinical or financial decision about a patient including documents that are not generally including in the "Medical Record" e.g., x-rays, video /images of a procedure, billing correspondence, external records

Personal Representative - A personal representative, is someone other than the patient, who has the same rights as the patient regarding access and authorizing disclosures of the patient's information. A personal representative can be a patient's legal guardian, health care agent designated in a health care proxy form or other advanced directive(in active status), parent of a minor (some exceptions for adolescents), or surrogate identified as per Mount Sinai's Family Health Care Decisions Act policies.

What is PHI?

PHI (Protected Health Information) is any information regarding an individual (demographic, financial, social, clinical) that we receive, create, maintain in the course of providing the individual a service; in any format – verbal, hard copy, electronic

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

►Name

►MRN

►SSN

►Address

►Telephone/Fax Numbers

►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) including biometrics.**

What is a Limited Data Set and Very Limited Data Set?

A **Limited Data Set (LDS)** 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.

Both are still PHI, but have less stringent rules on use and disclosure for research purposes.

- ~~Name~~
- ~~MRN~~
- ~~SSN~~
- **Address:** ~~house #,street,apt#,~~ **city, state and ZIP CODE**
- ~~Telephone/Fax Numbers~~
- ~~Email/ IP /URL addresses~~
- ~~Serial Numbers (VINs, device numbers)~~
- **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)~~
- ~~Biometric identifiers (finger print, voice print, dental x-rays, etc)~~
- ~~Images such as photos including full face or unique physical characteristics~~

Permitted Uses and Disclosures

You may share PHI within the OHCA without authorization for **Treatment, Payment, Operations** (TPO) for the purpose of doing your job as follows:

- With other care givers within the OHCA who are involved in the patient’s care (**T**), to make a referral, to respond to a referral, for transition of care and coordination of care with the patients PCPs.
- To enable payment of a bill (**P**)
- For hospital operations within the scope of your responsibility (**O**)
- In response to a valid authorization to disclose
- As mandated by law (e.g., to report immunizations, etc)

You may only view information needed to care for your patients or to perform your job. Accessing unauthorized records will result in disciplinary action up to and including TERMINATION.

PHI may not be shared with anyone who does not have an official need unless that person has been authorized to have access by the patient or his/her personal representative.

Research

- You may access a patient record for research as follows:

  -With IRB approval and patient authorization

  -With an IRB approved waiver of consent, without authorization, unless
    - **the patient is known to you**
    - **the patient is a public figure**
    - **the patient is an employee**

  -Before IRB approval, if you are screening your own patients preparatory to research

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.

Patient Directory

- Includes patient's name, location, and condition

- Directory information is public information while the patient is here unless s/he opts out

- Patient may opt out of both name and location or just location

Special Privacy Concerns

A patient who may be a very public figure or well known to members of the Mount Sinai community may have special concerns about their privacy and the confidentiality of their records while they are receiving care at Mount Sinai.   If you have a patient who has specific concerns, contact HIPAA Compliance to discuss additional options , including the use of a temporary or permanent alias.

Family and Friends

- Interacting with family members
  - Alert patients determine who may know what
  - Even alert patients are subject to subtle pressure
  - Ask visitors to step out. Confirm with the patient privately what can be shared with who.
  - By law we must provide professional translators (Family translators are the last resort)
  - Family dynamics are complicated

Incidental Disclosures

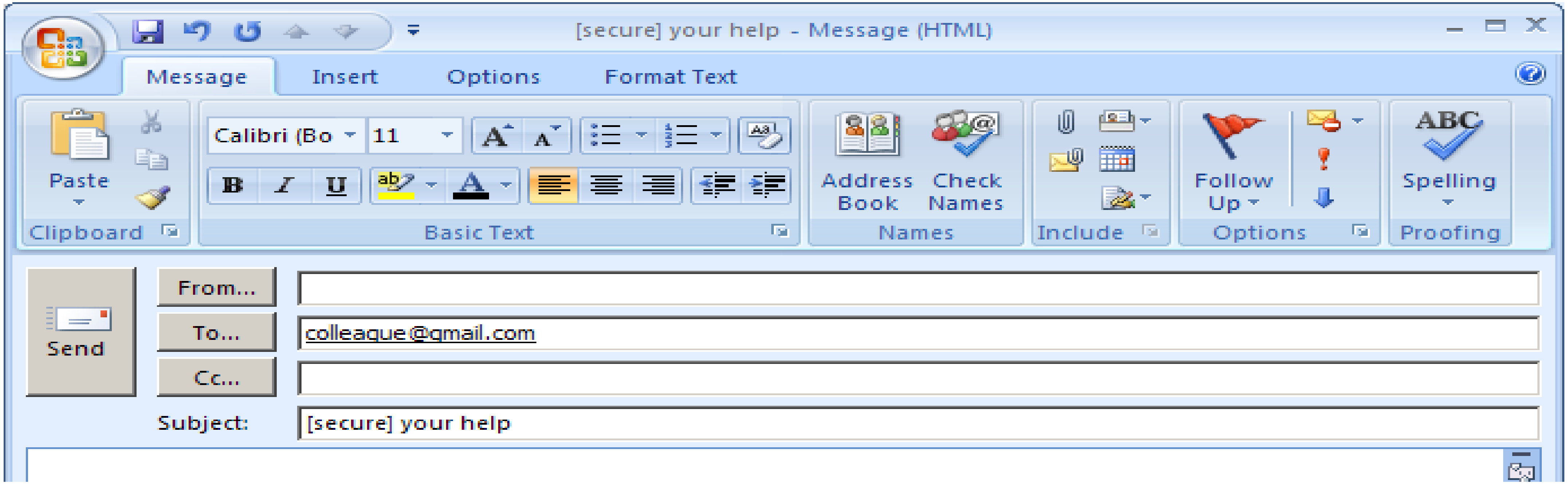
Incidental Disclosure is when patient information is unavoidably shared with someone not authorized to receive the information in the course of providing care to the patient. Incidental Disclosures are acceptable as long as reasonable steps were taken to protect the information.

- Don't discuss patients in elevators, shuttles, the cafeteria or other public places
- Before starting a conversation about a patient over mobile phone or Vocera, ask if they are in a private place and can speak; Let callers know that you need to call them back if you are not in a private space.
- When discussing patients at bedside or rounding close curtains
- Take note of visitors and other patients who may be near enough to overhear your discussion
- Speak in low volume
- Limit discussions to the minimum necessary information and if possible avoid statements about particularly sensitive information until in a more private area.

Communicating Via Email

Email is one of the most common and preferred ways to communicate.   When communicating via email about patients you should :

1) Only use your Mount Sinai email account to communicate about patients.
2) Remember that email , by its nature, is the not most secure way to communicate. Information in an email can be printed and forwarded without your knowledge or control. Adding an unintended party is easy. So when discussing patients, even internally, limit the identifiers used and don't put patient names or DOB in the subject line. Consider password protecting attachments or using a different more secure way to share attachments with lots of patient information.
3) If you need to communicate patient information with someone who does not have a Mount Sinai email, you must use the Mount Sinai secure email portal which is triggered by adding [secure] to the email subject line



[secure] your help - Message (HTML)

From...

To... colleague@gmail.com

Cc...

Subject: [secure] your help

Communicating with Providers/Staff : Texting

Epic Secure Chat is the only approved messaging platform for communicating about patients. If Secure Chat is unable to meet an urgent, immediate patient care need, SMS/ text messaging may be used as follows:

- As a way to initiate contact ("Need to talk to you about JD on 7E call me @..."; "Need you to look at something urgently; check your email").

- In an emergent patient care treatment situation if texting is the only means available to communicate PHI, texting is permitted. Take care to:
  - Include the minimal amount of potentially identifying information try to use patient initials, medical record number, room number
  - Limit the content until a more secure communication can be established
  - Delete the texts as soon as the information is no longer needed for the emergent patient care.

As part of Joint Commission Patient Safety Standards the communication of orders via Epic Secure Chat or other SMS/text/DM platform is prohibited. You must use the verbal order process or place the order directly in the EMR.

Epic Secure Chat is not maintained as part of the medical record. You need to document in the patient's medical record communications via Epic Secure Chat or other text/DM platforms as appropriate.

USE OF WHATS APP OR SIMILAR APPS TO COMMUNICATE /SHARE PATIENT INFORMATION OR IMAGES (even de-identified) IS PROHIBITED.

General Faxing of Patient Information

Patient information should only be faxed when more secure alternatives are infeasible to meet the immediate patient care needs. Only the minimum necessary information should be faxed.

All policies regarding processing requests for patient information should be followed.

Sensitive or specially protected information, such HIV-related, psychiatric/mental health treatment, or substance abuse treatment information should not be faxed unless required for medical care. Faxing for any other purpose must be approved by a manger/supervisor.

Prior to sending the fax you should confirm the fax number with the authorized recipient.

A fax cover sheet that contains a confidentiality statement, as well as the prohibition on re-disclosure if specially protected information is included, must be used.

Any misdirection of a fax must be reported to the Privacy Office and your supervisor.

Preventing and Mitigating Misdirection

To Prevent/Mitigate Misdirection of Electronic or Hard Copy Documents/Communication:

- Validate email addresses, names, mailing addresses, fax numbers to send the document
- Always include a return address with your name and box number or floor/suite
- Always use an email signature that includes your role, department, telephone number and a Confidentiality Statement
- Always use a fax cover sheet that includes your name, department, telephone number and Confidentiality Statement

If You Identify That a Hard Copy Document has Been Misdirected:

- make arrangements for them to return the original documents which can include sending a self addressed/postage paid envelope

If You Identify That an Email or Electronic Communication has Been Misdirected

- send a separate message asking the recipient to completely delete the communication from their email account/systems
- get written confirmation that they have done so and have not shared the information with anyone.

Health Information Exchanges (HIE)

Mount Sinai Health System participates in several platforms that facilitate Mount Sinai's ability to exchange (both send and receive) health information electronically with the patient and their non-Mount Sinai health care / health services providers in order to improve coordination of care, quality of care, and improve health outcomes.

Epic Interoperability

Epic CareLink – provisioned non-Mount Sinai referring and primary care providers can view their patients' Epic records and make referrals

Epic CareEverywhere – Allows an Epic user at a participating facility to view a patient's Epic record at another participating facility.

My Chart – Patient Portal where patients can schedule and check into appointments, message providers, upload information, and pay bills.

Carequality – is an interoperability platform that allows sharing of data between different EMR systems leveraging their native interoperability functionality. Not all EMR vendors participate. Prospective consent needs to be obtained by the custodian of the patient record. MSHS participates has implemented EIE consent form to collect prospective authorization for the sharing of Epic records.

Healthix – a state managed HIE in which Mount Sinai is a member (formerly NYCLIX and LIPIX). Allows providers to view clinical data from other participating facilities

Information Exchange

Some of these exchanges are permitted without the patient's authorization as part of treatment, payment, and health care operations activities. Some fall under an exemption to consent such as

- Public Health surveillance including monitoring disease trends, epidemics, and public health emergencies
- Disaster Management for the purpose of locating patients during an emergency event
- Organ procurement
- Office of the Medical Examiner
- With Health Plans and payers for quality reporting such as calculating HEDIS and QARR measures.

Most exchanges require patient consent.

The Mount Sinai Enterprise Information Exchange (EIE) consent form is one way we engage patients prospectively about data sharing on specific platforms Mount Sinai participates in.

There are also opportunities for the patient to consent at the point of care with their non-Mount Sinai providers or to use tools within the patient portal to share their information with their family, care partners, and providers.

Mount Sinai Enterprise Information Exchange (EIE) Consent Form

The Mount Sinai EIE consent form addresses patient consent choice regarding how their information will be exchanged on four platforms: Healthix, Epic Care Everywhere, Carequality, and Mount Sinai HIE.

An adult patient, or the personal representative of a child (ages 0-11) or incapacitated adult (age 18 or older), can choose one of four consent options which will be applied to all four platforms based on the platform's functionality:

I GIVE CONSENT

I DENY CONSENT, EXCEPT IN AN EMERGENCY

I DENY CONSENT, EVEN IN AN EMERGENCY

I DO NOT WISH TO MAKE A CHOICE AT THIS TIME

For a child, when the patient turns 12 years old, any consent choice made previously by their parent/guardian is updated to what is functionally "I DO NOT WISH TO MAKE A CHOICE AT THIS TIME". If the patient presents to Mount Sinai on or after their 18th birthday , they or their personal representative, will have the opportunity to complete a new EIE form. Adolescents (ages 12-17) and their personal representatives have opportunities at the point of care with their non-Mount Sinai providers to provide time limited, specific authorizations.

Other than for children the consent choice is durable and does not expire. Adult patients and the personal representatives of an adult or child 0-11, can change their consent choice at any time by completing a new EIE form with their new consent choice.

If a patient wants to opt out of all participation in any of these platforms, including those that are permitted without patient consent, they can submit the request to be non-participating / limit permitted use and disclosure of their information in writing to the Mount Sinai Privacy Office.

EIE consent forms, like other documents that are part of the patient's medical record, must be retained as per Mount Sinai Medical Record Retention Policy – a minimum of 10 years for adult patients or for minors until their 21st birthday or 10 years, whichever is the longer.

Patients always have right to receive a copy of any form they sign, including the MS EIE consent form.

Healthix

Healthix is a regional health information organization (RHIO) that is part of a larger State Health Information Network (SHIN-NY) that is overseen by the NYS Department of Health.

Mount Sinai, as a participant in Healthix, is required to ensure only authorized users within Mount Sinai have access to Healthix information and only that appropriate for their role, that we report to Healthix without delay any impermissible use or disclosure of patient information that we received/accessed from Healthix, and that we implement appropriate sanctions for a violation. Healthix in addition may independently seek out sanctions on the user or Mount Sinai as an organization.

Patient consent is not required for a health care organization to share patient information with Healthix but written patient consent is required for an organization to access a patient's health information in Healthix. This would be a consent election of **I GIVE CONSENT** on the MS EIE form.

Healthix takes additional precautions to protect sensitive information for minors (0-17), including excluding 42 CRF Part 2 data (health information from facilities that provide Substance Abuse/ Chemical Dependency specific treatment) from disclosures authorized by a parent/guardian.

Minors ages 10-17 can themselves grant a one time consent, at the time of visit for a provider of Minor Consented Services to view their complete record.

If on the MS EIE form a patient makes a consent choice of

- **I DENY EXCEPT IN AN EMERGENCY** , Mount Sinai Emergency Room providers will be able to access the patient's information in Healthix. However if the patient makes an election of **I DENY EVEN IN AN EMGERGENCY**, Mount Sinai providers will not be able to access information.
- **I DO NOT WISH TO MAKE A CHOICE AT THIS TIME**, Mount Sinai Emergency Room will allow Emergency Room providers to "Break the Glass" to obtain emergency access to see all the patient's information one time only. The patient's Mount Sinai providers and care coordinators will also be able to receive alerts limited to essential information. Alerts will exclude information related to 42 CRF Part 2 facilities

Additionally, a patient can also request that no organization participating in Healthix should ever have the ability to view their information. A patient who wants to make an **I DENY ALL** consent choice should contact Healthix directly at compliance@healthix .org.

A patient can also request from Healthix directly (email compliance@healthix.org) a list of all Healthix participant organizations whose employees accessed their health information via Healthix.

If a patient wants to request that Mount Sinai not share any of their data with Healthix, they can make a request in writing to the Mount Sinai Privacy Office to be non-participating.

Epic Care Everywhere and Carequality

Epic Care Everywhere is the interoperability platform in Epic, the MSHS EMR, that facilitates health information exchange between other provider organizations that also use Epic as their EMR.   MSHS also uses Epic Care Everywhere functionality to incorporate external health information we receive into Epic so it can be more readily be used by providers and care coordinators.

Carequality is a framework that facilitates health information exchange between provider organizations who use one of several certified EMRs by leveraging the EMRs native platform.

Data exchange on these platforms is facilitated by the participating organizations allowing " auto matching" which does not require patient consent. If a patient matches between two organization, that organization will appear in the interoperability workflow as having provided a service to the patient, but no information about the services or any other information about the patient is available. Mount Sinai opts to not allow matching for any patient who has only received services in confidential departments.

An "I GIVE CONSENT" consent election on the MS EIE consent form permits MSHS to allow any provider organization that also participates in Care Everywhere or Carequality to query/access information from the patient's MSHS Epic record. If a patient with this consent election "auto matches" , the external provider will be able to view clinical summary information and a list of encounters and will be able to query other documents and results directly from their EMR.   MSHS opts not to share encounter specific information for our confidential departments through these platforms.   However all information about medications, diagnosis and test results will be available.

Any other consent choice will require at the point of care the non-Mount Sinai provider attests that they have obtained written authorization from the patient/personal representative , or it is a medical emergency and access to the information is necessary to avoid harm to the patient, to query information.   This attestation will allow the provider organization to query the patient's record for only that one encounter.

If a non-Mount Sinai organization requires patient consent, Mount Sinai providers must obtain written authorization from the patient or their personal representative before they attest in Care Everywhere they have obtained consent. The written consent must be scanned into the patient's record using the appropriate Care Everywhere document type.

If a patient does not want Mount Sinai to exchange any data via Epic Care Everywhere or Carequality, they can make a request to be non-participating in writing to the Mount Sinai Privacy Office.

Mount Sinai HIE

The Mount Sinai HIE is a Mount Sinai application that facilitates the collation of patient data from across Mount Sinai clinical/EMR applications and data we receive externally about patient's health care.

The Mount Sinai HIE also facilitates sending patient information to Healthix and other data sharing for treatment, payment and health care operations purposes that does not require patient authorization.

However the MS HIE does have the ability to function an a data exchange platform with our clinical partners and therefore it is also included in the MS EIE consent form.

An I GIVE CONSENT election permits MS HIE to disclose the patient's data it holds with participating partners and to use/disclose internally external data received.

Any other consent election will limit information use or exchange to only that permitted without patient authorization.

My Mount Sinai / Epic My Chart and Happy Together

My Mount Sinai / My Chart is the patient portal in use at Mount Sinai Health System.   This facilitates patients, their personal representatives, and others that they may authorize, to view health information, as well as message providers, upload information, schedule appointments, complete check in to appointments, and pay bills.

My Mount Sinai / My Chart does not currently provide access to the patient's entire/complete medical record (for example information that is not directly maintained in the Epic EMR) therefore may not meet the patient's right to access provided by HIPAA and NYS regulations.   If a patient cannot see information in My Chart they should be directed to the appropriate Medical Records resource to request either paper or electronic versions of the information.

However most of the patient's Mount Sinai record maintained in Epic is shared with the patient, and those they authorize, including provider notes.   By default, all results, all clinical and nonclinical notes written by staff will be shared with patients at set times after the result is finalized or the encounter closes. These include abnormal results, narrative results (such as pathology or radiology reports), behavioral health notes, chaplain notes, social work notes, nursing notes, etc.

Happy Together is a functionality in My Chart that will allow a patient to link their Epic My Chart accounts from all of their providers who use Epic so they can view all of the information their providers make available through My Chart in one account. This does not affect what Mount Sinai or their other providers can view via Care Everywhere.

Epic Care Link

Epic Care Link is a web based portal for providers that are part of the Mount Sinai Clinically Integrated Network (CIN) or are community providers whose patients utilize Mount Sinai for emergency, acute, or specialty care.

This data exchange is not part of the EIE consent. Instead Mount Sinai enters into agreements with these community providers and these providers collect specific consents from their patients.

This portal allows community providers to make referrals to Mount Sinai, including physician to physician e-consults, and for Mount Sinai to make referrals to the providers. It facilitates sharing health information for consults, transitions of care, and care coordination.

Use of Cameras and Video/Audio Recording Devices

Staff use of cameras and recording devices in patient care areas is prohibited unless it is for:

- Treatment or internal training/education purposes. Patient consent is needed if any identifiable features (full face, tattoos, unique wounds or markings, voice recordings) will be captured.
- Security purposes.
- An activity approved by the Marketing and Communications Office for purposes of the MSHS Archives, media or marketing/promotional purposes. Patient consent and authorization is required prior to any photos or recordings of patients even if the patient is not recognizable. Care should be taken that no patients, visitors or PHI are captured in the background.
- Social purposes, such as staff celebrations, that are approved by the   unit/department manager and ensure that no patient information or images are captured in the background – such as monitors or patients/visitors in the background.

Social Media / Media Interactions

- **All MSHS policies apply to use of 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.

  - 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 MSHS information of any kind, contact the Press Office, a division of the Marketing & Communications Department, at (212) 241-9200 or newsmedia@mssm.edu

  - You may not comment on patients/patient events without written authorization of the patient even if information has been made public

Medical Students interacting with Patients

- Patients should be asked if they consent to have a student present during a history and/or physical examination

- Observers or shadows must have permission of the Department Chair or Division Chief and must comply with Institutional Observer Policy. If they have actual patient contact the patient must consent.

Medical Records

- Original records may NOT be taken off the premises at any time

- You may NOT take any original MS medical records if you terminate your relationship with Mount Sinai

- You may take copies only if you have a valid authorization from the patient.

Patients 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 a record
- Request limits on permitted uses and disclosures of their information, including not disclosing to a carrier if the encounter is paid for in cash.
- A copy of the designated record set (DRS)
- Request an Accounting of Disclosures
- Request confidential communication

Request to Amend

There has been a significant increase in patient requests to amend their records since the implementation of the electronic medical record (EMR). The process to amend the record in the EMR is much more complicated than in the paper world.

Incorrect Information

In the EMR a documentation error not only affects the original provider's documentation but may affect subsequent provider notes through the use of shared problem and history lists, template notes, and use of smart text.

Sensitive Information

Patients often share sensitive information about themselves or a family member with a provider but do not want it documented in the EMR concerned that others who do not need this information will have access or feel it should not be part of the medical record at all.

Contact the HIPAA Compliance Office if a patient requests an amendment or requests that you exclude information from your documentation.

Use of Copy Forward, Smartphrases, Smartlinks, and Copy/Paste

Documentation in the EMR is time consuming and there many requirements regarding what should be included in your documentation.

While there are tools available in the EMR to assist with compliance and decrease the documentation burden, you need to use the tools in an appropriate way and follow MSHS policies for documentation.

The **Copy Forward** function in Epic can be time-saving and helpful, but can lead to inaccuracies. Be sure to accurately describe in your note what you discussed with the patient, the exam findings for that particular day, and your evolving plan. Notes that copy forward exam findings and plan items from prior days are risky if you don’t review and update them each time.

Smartphrases (also called dot-phrases) are powerful ways to generate canned sentences or paragraphs with a few keystrokes. Using smartphrases is generally acceptable but caution is needed that you are editing for the specific encounter and patient as needed.

Smartphrases can include **Smartlinks** to “pull in” data from other parts of the chart such as history, vital signs or lab results. You should not use smartlinks (or other macros) to pull in data that you have not verified as accurate – this is especially important for previous medical history, social history and SOGI related information.

Puling in data injudiciously leads to:

- note bloat (making the note hard to follow)
- potential error (if say there are missing or erroneous entries in past medical history, for instance)
- potential confusion (if, say, the lab results are out of date by the time the note is signed).

What’s more, these smartlinks may not be necessary from a billing perspective or even to communicate among colleagues. If you’re compelled to pull in blocks of data, try to limit it to the past 24 hours (for inpatient) and limit to pertinent findings.

There is also the temptation to copy/paste relevant information from another provider’s note. You must attribute in your note where the data originated from. Again you need to be cautious not to replicate a documentation error.

In general copy/pasting from a different patient’s record is not permitted.

Documentation Tips

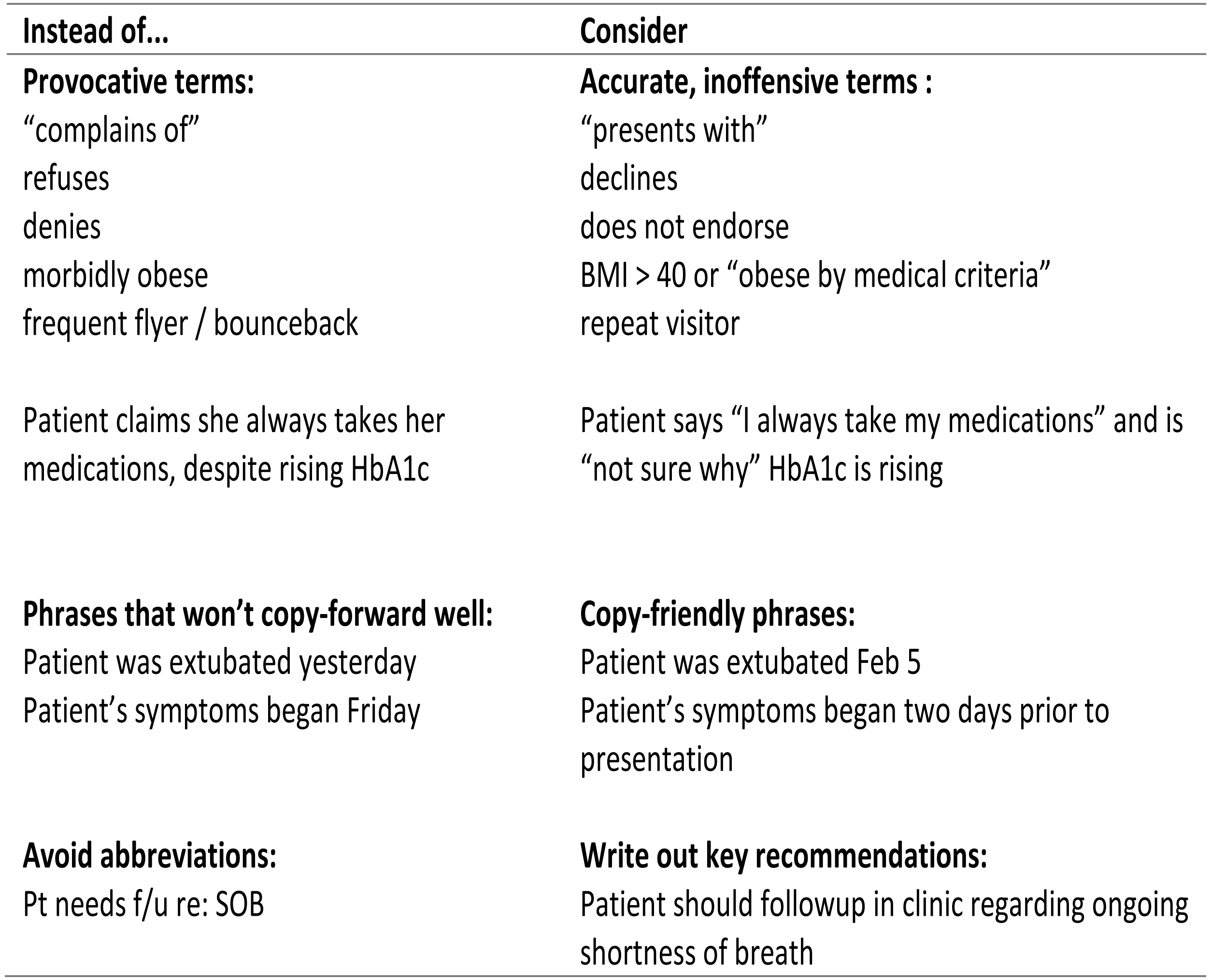
Here are some quick, simple suggestions. This will help fellow clinicians reading the note, won't affect coding and billing, will avoid medico-legal pitfalls and will be appreciated by patients.

Remember, patients who spot errors, or read something confusing or unexpected, may make requests for corrections/amendments. So it's in your best interest to write notes that are clear, accurate - and avoid potentially awkward phrasings.

Every note should have a short, easy-to-find nugget of readable prose that succinctly recaps relevant new info, as well as your medical decision-making and recommendations. This capsule summary, especially if placed at the top of the note, would really help your colleagues and patients reading the note.

- Avoid potentially inflammatory terms - choose language that conveys the same meaning but is less likely to provoke the patient
- Patients may sometimes say implausible or extraordinary things. Make use of quotation marks in these circumstances; there's no editorial judgment involved (unlike paraphrasing).
- Don't write notes with relative dates, Notes become confusing and inaccurate when that phrase gets copied and pasted in consecutive progress notes. Instead, use absolute dates (see below)
- Be mindful of abbreviations or medical terminology that can be misinterpreted.
- Don't include phone numbers of treatment team members in your note or signature. Sure, listing a number may be helpful for colleagues – but a patient reading that note may feel it's ok to dial it and ask questions. Refer colleagues to a call schedule (eg Amion) or Epic Secure Chat, instead.
- Don't document things that didn't happen. This takes many forms (attesting to being present for something when you were absent, or documenting a negative exam when one wasn't done) but it's always wrong, and with patients now reading notes, more verifiably wrong.
- Don't use the chart to document disagreements with other services ("Consulted xx service again, but as usual they never return calls").
- Don't document discussions with risk management (or the involvement of risk management) in the chart.

Instead of…… Consider



Instead of...	Consider
Provocative terms:	**Accurate, inoffensive terms :**
“complains of”	“presents with”
refuses	declines
denies	does not endorse
morbidly obese	BMI > 40 or “obese by medical criteria”
frequent flyer / bounceback	repeat visitor
Patient claims she always takes her medications, despite rising HbA1c	Patient says “I always take my medications” and is “not sure why” HbA1c is rising
Phrases that won’t copy-forward well:	**Copy-friendly phrases:**
Patient was extubated yesterday	Patient was extubated Feb 5
Patient’s symptoms began Friday	Patient’s symptoms began two days prior to presentation
Avoid abbreviations:	**Write out key recommendations:**
Pt needs f/u re: SOB	Patient should followup in clinic regarding ongoing shortness of breath

Data Security

- Never share your computer system logon ID and password; Do not allow another person to use an application while you are logged in; Lock or log out of applications /workstations when you step away. Audit trails will hold you responsible.

- To access Mount Sinai systems remotely use approved portals and VPN; if you must transport data via a portable device (e.g. laptop, flash drive, etc.) it must be encrypted and a back up copy must exist.

- If your smartphone, tablet, Blackberry, etc... contains PHI it must be encrypted and password protected.

- Confidential Waste must be placed in secure bins/shredders.

- Always use a box number on internal mail and in your return address on all outgoing mail.

Data Security

- Full Disk Encryption is required on all portable devices owned by Mount Sinai and any other portable devices (including privately owned laptops) that contain Mount Sinai confidential information on its local hard drive.
- External USB drives that contain PHI or other confidential information must also be encrypted.
- Although encryption protects the privacy of the data, it does not help with the recovery of the information should a device be lost or stolen.
- To prevent the loss of data, "back it up" in case an unforeseen computer issue occurs.
- Public cloud based services (dropbox; googledocs) are not approved for the storage of unencrypted Mount Sinai PHI or other confidential information.
- Your department would need to follow the Purchasing Policy to engage any private cloud services and request a Risk Assessment /Review of the vendor/application from Mount Sinai Information Security if the vendor/application is new to Mount Sinai.
- Contact IT Security for other issues at : DTPSecurityOperations@mountsinai.org

Cyber Attacks: Malicious Software

Malware is software designed to cause harm to the user or the system. It can infect devices through attachments, links/URLs, webpages, and pop-ups. From the initial infected device/workstation, malware can spread throughout the MSHS network affecting workstations, servers, and applications.

- Ransomware restricts access to a computer system or data until a ransom is paid.
- Viruses cause damage to the core functionality of systems, corrupting files and locking users out.
- Spyware collects information such as logon credentials and other confidential information.
- Remote Access Tools allow the computer to be remote controlled by an unauthorized party.

Cyber Attacks: Phishing

Phishing attempts use electronic communications (email, IM/DM, text) that appear to be from trusted or legitimate senders in order to obtain from users confidential information such as logon credentials, personally identifying information, and banking/credit card information. This can be a direct request for information or by using attachments or URLs with malware.

- Spear Phishing – uses information about the target to increase the likelihood of success
- Whaling – targets senior executives and high profile individuals
- Clone Phishing – a legitimate email to the target (obtained because either the sender or target was already hacked) is cloned by the attacker. The second communication will claim to be a resend or update.
- Business Email Compromises – email that looks to be from a person of authority or trusted colleague that directs the recipient to perform some business or financial transaction, including the purchase of gift cards.

Mitigating a Cybersecurity Event

Report suspicious emails by forwarding them as an attachment to ReportSpam@mountsinai.org

If you believe you have responded to a phishing email, clicked on a suspicious link or attachment, or that your workstation or server has been compromised by malware, contact your Helpdesk or email DTPSecurityRisk@mountsinai.org

If you believe your logon credentials have been compromised or have been used by another individual, use the self service tools to reset your password and report the issue to DTPSecurityRisk@mountsinai.org

Telecommuting: Secure Your Home Network

Use a wireless router that includes a built-in firewall; most modern wireless routers have this feature.

Enable automatic updates on the wireless router to ensure its software is being updated to fix vulnerabilities that are identified by the manufacturer.

Activate wireless network encryption. Encrypting your wireless data prevents anyone viewing your data. Use a wireless router that supports WiFi Protected Access (WPA, WPA2, or WPA3; WPA3 is the latest version). Wired Equivalent Privacy (WEP) should NOT be used.

Change the name of your wireless router (referred to as the SSID or ESSID) from the default name to something unique to you and not easily guessed by others. Do not use your name or the name of others in your household.

Change the password from the manufacturer's default which can be easily found online. The new password should be at least 12 characters long. Passwords should be changed periodically - once a year or when the clocks change or if you think your wireless network has been compromised.

If your router allows for a separate guest network or account, set it up for guests to use. The guest account will protect your primary network/account from misuse by others.

Disable remote administration. This will prevent others from changing your wireless router's settings.

Telecommuting: Securing Your Devices and Paper

Make sure all of your devices that connect to your home network – personal or issued to you by Mount Sinai – are up-to-date on the patches and updates to the OS (operating system), malware and antivirus software, and applications. Unsupported or unpatched software can have vulnerabilities that can be exploited.

Do not allow others (friends, children, spouse) to use your MSHS work issued devices to avoid inadvertent deletion or alteration of information, or accidently allowing malware onto your device.

Limit your own use of devices provided to you by MSHS to legitimate work purposes. Use your personal devices for your personal use.

If you need to print or create information on paper at home, secure it in a locked desk or cabinet. If it is no longer needed, it should be shredded or otherwise made unreadable before being put in the trash/recycle.

Cyber Security Reminders

Think before you click!

- Email is the primary attack method for cyber criminals. If you are not sure about the legitimacy of a message, call the sender to verify or go directly to the senders website rather than use the link in an email.

Know how to recognize a secure site!

- Check the URL address. Secure sites are indicated by a Web address that starts with “https” (instead of just “http”) and a padlock icon at the top or bottom right of your browser window. Check for misspellings, added letters or numerals, transposed letters in the URL.

Think before you connect!

- Telecommuting employees should only connect through VPN and not use public Wi-Fi.

Guard your mobile devices!

- Never leave your phone, tablet, laptops, USB or external storage devices unattended in a public place. Turn on device encryption.

Use strong passwords!

- Use strong passwords and change them regularly. Do not share your password with anyone. Passwords are the first line of defense in preventing unauthorized access to any computer or network.

UPDATE your computer and devices!

- REBOOT your centrally managed computer on a regular basis to allow security patches to be applied to the system. Update your unmanaged workstations and devices when new patches are announced.

Software Asset Management (SAM)

What is SAM?

A Software Asset Management (SAM) program allows you to minimize software cost, be in compliance with license terms, and ensure that software assets are managed according to the MSHS strategy.

Our Policy

All employees must comply with the MSHS Software Licensing Policy, which defines the standards, procedures, and restrictions for users regarding the procurement, deployment, use, compliance, and security of software (e.g. Acrobat, MS Office, etc.). You can read the MSHS Software Licensing Policy on the policy management system found on the intranet.

SAM
Do’s & Don’ts

- Users may maintain only legally licensed software on MSHS computers, workstations, laptops, servers, tablets, and other computing and storage devices.
- Users must not distribute, duplicate, copy, or transmit copies of MSHS-licensed software to third parties.
- Users must ensure that all acquired software versions used are still supported by the vendor.
- Users may not download or install personally licensed/personally owned software, “Freeware,” or “Shareware” on MSHS computers or networks.
- Users must obtain valid proof of licensing when installing software applications on new or replacement MSHS devices.
- Users are also responsible for retaining copies of licenses as proof of purchase for software

Contact

All questions and concerns related to SAM and the MSHS Software Licensing Policy should be directed to the SAM Administrator at softwareassetmanagement@mountsinai.org