HIPAA Topics For Research Coordinators

SCORE Meeting

Kathleen Tranelli
Privacy Officer for Research
October 2023

Role of the Research Privacy Officer

- Consultation on RSRB studies
- Advice about contracts (ORPA, Purchasing)
- Data pull questions
- Breach analyses
- Audits of eRecord accesses

WHAT DOES THE PRIVACY OFFICER DO?

Agenda

- Overview of HIPAA
- Bases for Use and Disclosure of PHI in Research
- External uses and disclosures
- Security Considerations
- Common mistakes/ Cautions for Research Coordinators
- Breach response
- International Considerations

HIPAA Overview

- Aims to safeguard health information while allowing a flow of information among providers and payors, and giving patients certain rights regarding their information

- Includes provisions under which a covered entity can use or disclose PHI for research purposes

Privacy Rule =
How PHI is Utilized

Security Rule =
How PHI is Safeguarded

Protected Health Information (PHI)

- Information that is created or received by a health care provider that :

  Relates to the past, present or future physical or mental health or condition of an individual; the provisions of health care to an individual; or the past, present or future payment for the provision of health care to an individual

  AND

  Identifies the individual OR there is reasonable basis to believe that the information can be used to identify the individual

18 HIPAA IDENTIFIERS

- Names
- **Geographic subdivisions smaller than a State (except 1st 3 digits of zip code if…)**
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- **All elements of dates related to an individual (except year) & all ages over 89**
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers
- URLs
- IP addresses
- Biometric identifiers (finger, voice prints)
- Full face photos
- Any other unique identifying numbers, characteristics or code

Research. We may use and disclose medical information about you for research purposes. In most cases we will ask for your written authorization. However, under some circumstances we may use and disclose your health information without your written authorization if doing so poses minimal risk to your privacy. We may also release your medical information without your written authorization to people who are preparing a research project, so long as any information identifying you does not leave our facility. The researchers may use this information to contact you to ask if you want to participate in such research.

URMC NOTICE of PRIVACY PRACTICES

Bases for Using or Disclosing PHI

- Use De-Identified Data (it's not PHI)
- Limited Data Set with Data Use Agreement (DUA)
- Preparatory to Research
- Authorization in Informed Consent
- RSRB Waiver of Authorization
- Research Using Decedent Information

De-Identified Data - Can not include:

- Name
- Street address, city, county, precinct, zip codes (“smaller than State”)
- Dates e.g. DOB, admission date, discharge date, date of death; and all ages over 89
- Social Security number
- Telephone/fax numbers, E-mail addresses, URLs, (IP) address numbers
- Medical record numbers
- Health plan beneficiary numbers, Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying numbers, characteristics or codes

HIPAA BASES for USING or DISCLOSING PHI

Limited Data Sets

- Can be used without subject's authorization
- Permitted HIPAA identifiers: zip code/city/state, dates e.g. DOB, DOS, and unique codes
- Need HIPAA-compliant DUA in order to disclose, and Form 25.6.1
  - Restriction on use (e.g. only for X study, and consistent with protocol)
  - Data safeguard terms, duty to notify of unauthorized disclosure
  - Can't attempt to identify or contact individuals
  - Ensure agents/contractors agree to same restrictions

HIPAA BASES for USING or DISCLOSING PHI

Preparatory to Research

- Examples: Cohort identification, feasibility reviews
- Must use the “minimum necessary” PHI
- Researcher attestation (Form 25.3) required (except if PI/researcher is accessing only records of own patients)
- Use of the PHI to conduct research, contact subjects, etc. requires RSRB approval
- PHI must remain on URMC premises (Remote access is permitted, subject to certain provisos.)

HIPAA BASES for USING or DISCLOSING PHI

AUTHORIZATION:

Excerpts from Bio-Medical Study Informed Consent Template

What information may be used and given to others?

The study doctor will get your personal and medical information. For example: …

- Past and present medical records related to the study, including records of external providers that are available via your electronic health record at URMC & Affiliates
- Results of medical tests

Your information may be given to:

- The Department of Health and Human Services
- The University of Rochester
- Include every organization or individual where data is shared (i.e., sponsors, sponsor agents [e.g., CRO], data monitoring committees, government agencies, foreign government regulatory agencies, companies, coordination centers, data management centers, other research sites, etc. who might receive, and/or use the information)
- The U.S. Food and Drug Administration (FDA) may also need to inspect study records …

HIPAA BASES FOR USING OR DISCLOSING PHI

IRB Waiver of Authorization

- Most common: retrospective review studies
- Subject to the accounting of disclosures requirement
- HIPAA allows reliance on determination of IRB, which documents that standards have been met
  - Minimal risk
  - Adequate plan to protect identifiers, and to destroy identifiers at earliest opportunity
  - PHI won't be reused or disclosed except as required by law or for HIPAA-permitted research

or

HIPAA BASES for USING or DISCLOSING PHI

Accounting of Disclosures

- Required for studies based on waiver of HIPAA authorization, such as retrospective review studies
- PI must complete the Online Disclosure Log
- Also required for disclosures of decedent information (although authorization is not required for research use of decedent information)

ACCOUNTING REQUIREMENT

Issues to Consider with Third Party study supports

- E.g. Home health agency, recruiting or data entry services
- Consent language; protocol modification?
- Security review, and liability for data breaches
  - If sponsor hired the third party: CTA should say sponsor is liable for contractor actions. (Also may impact consent language about 3rd party's data security)
  - Third party vendors will need DTA or BAA; consult Privacy
    - If Authorization doesn't cover vendor, need BAA

THIRD PARTY INVOLVEMENT

Data Transfer Agreements

- Sharing data/collaborating outside the UR
  - **All** data and/or biospecimens shared outside of the institution require the execution of a data use or material transfer agreement via ORPA, including data/biospecimens that have been de-identified

- Leaving the UR
  - Study documentation stays here!
  - As above, data may be shared with new institution, but appropriate agreements must be put into place ***before*** data can be shared
  - OHSP Guideline for Investigators Leaving the Institution

EXTERNAL DATA SHARING

Issues to consider with apps and software

- Do the terms of use or privacy policy say the app developer can use personal information for its own purposes, other than as study team intends?
  - E.g. marketing, independent research
  - Consider consistency with study documents, especially for click-wrap apps
- Impact on consent documents:
  - Disclose particular aspects i.e. collection of location data?
  - Advise subjects to read the app terms and privacy policy?

APPS AND SOFTWARE

Security Rule

Requires covered entities to

- Ensure confidentiality, integrity and availability of all e-PHI that is created, received, maintained or transmitted by the covered entity
- Protect against reasonably anticipated threats to the security or integrity of e-PHI
- Protect against reasonably anticipated unauthorized use or disclosure of PHI
- Ensure covered entity workforce compliance with the rule

Compliance means:

- Access is limited to study team members
- Hard copy documentation is stored securely
- Electronic data is stored on network server, encrypted device (phone, laptop, flash drive), or in approved storage platform
  - Cloud storage (Box.com)
  - REDCap database
- Follow Research Data Security Classification guidance

SECURITY CONSIDERATIONS

Day-to-day use of electronic media:

- Keep all information system passwords confidential
- Log off or lock unattended workstations/computers
- Inventory all assets for proper tracking/updates
- Dispose of broken or unwanted electronic media/devices via the University's Equipment Recovery Program
- Beware of phishing
- Encrypt email with PHI via **"!secure"** in subject line
- Email and texting to subjects requires risk disclosure

See also: Cybersecurity Awareness Month (October) : More info and sessions to "Ask UR Security anything".

Email/Text Messaging Excerpt from Consent Template

"You have the option to receive communications about this study via email and/or text messaging, by indicating your consent at the end of this form. *[Insert purpose as applicable, e.g.: Messages will be limited to appointment reminders]*

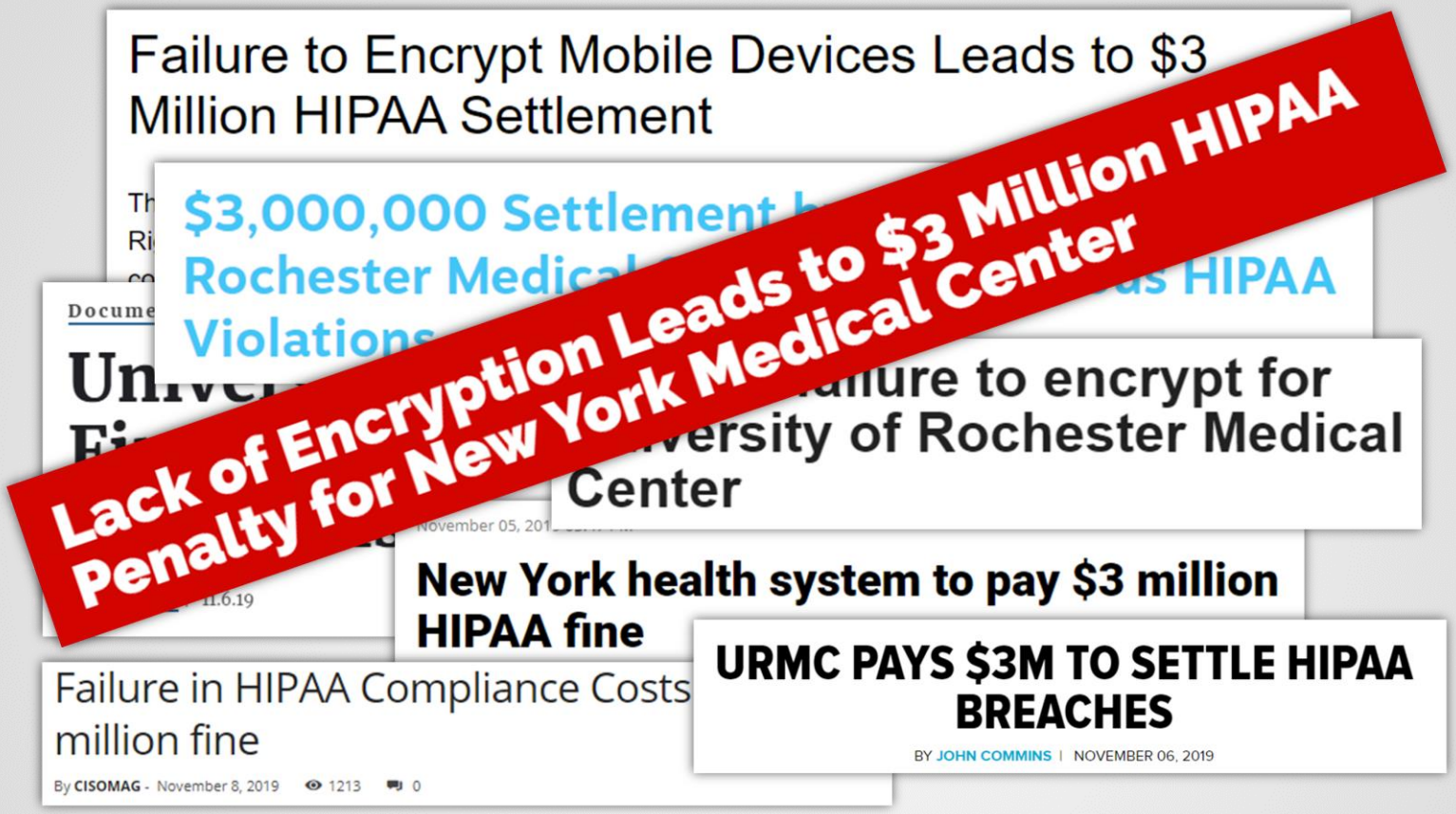
Email and/or text communications may be sent or received in an unencrypted (unprotected) manner. Therefore, there is a risk that the content of the communication, including your personal information, could be shared beyond you and the research team. Your consent below indicates that you understand this risk. The University of Rochester is not responsible for any interception of messages sent through email or texting.

[For email messages add] Email communications between you and the research team may be filed in your research record.

*[For text messages add] You are responsible for any fees charged by your carrier's service plan for text messaging. You may decide not to receive or send text messages with research study staff at any time, in person or by sending the research number a text message that says "**Stop Research Text**". Your consent, and any request to stop email or text messaging, applies to this research study only.*

Email and Text Messages to Subjects

Mistakes Happen



Let's Stay Out of the News :-)

Cautions for Research Coordinators

- Inadvertent Disclosures
- Breach Notification and Response
- Snooping

CAUTIONS FOR RESEARCH COORDINATORS

Inadvertent Disclosures

- Misdirected documents e.g. lab requisition to the wrong patient
- Misdirected email (e.g. “reply to all” without noticing external study monitor is on the group email; sending eRecord excerpt to external rather than internal recipient due to common last name)
- Sending spreadsheet to sponsor that should have been de-identified; column with MRNs was hidden but not deleted
- Pasting care note that included subject’s name, in to email inquiry about dosage change to clinical trial sponsor

Inadvertent Disclosures

Items Provided to Patients:

Lab Kits
Diaries
Study Drugs

Double Check ALL items in kits, on labels, etc.

Conversations:

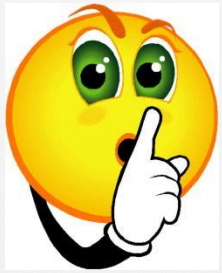
Be aware of your surroundings

Don't discuss other subjects with other participants

Social Media:

Don't post anything about a patient or family, even without identifiers

You NEVER know who will see the post



Watch out!

If you need to send restricted or sensitive information through email remember these important tips!

Send the "minimum necessary" to get the task done.

Send to a single addressee **ONLY**:

- No Distribution Lists
- No List Servs
- Don't "Reply All"

Double-Check:

- Email address of recipient (s)
- Content being sent (incl forwarded email)

Send only to internal URMC address or use !Secure in subject line of external email

Do **NOT** use personal email (Hotmail, Gmail,MSN,etc,) to send anything with PHI

Do **NOT** Auto-Forward any of your URMC email to a personal email account

*PHI sent outside of URMC must be encrypted.

Emailing PHI: Important Tips

Attachments: Removing PHI

Printed Materials:

- Use a **BLACK** Sharpie to "black-out" any PHI:
  - Check the reverse: may need to use marker on back side if PHI visible
- Have a "Buddy" check it over to make sure all PHI is removed
- Scan and Save as "pdf" for submission, storage, etc.

Downloaded Materials:

Chart notes
Lab Reports
Imaging Reports
And so on…..

- Convert document to a pdf document
- Use Tool in Adobe Pro to "Redact" all PHI
- DOUBLE CHECK for PHI: not a 100% foolproof tool

Step by Step instructions on how to redact a pdf document can be found in separate PowerPoint file

What to do if a potential breach occurs

- Contact the Privacy Office, as well as RSRB (Is RNI required?)
- Promptly recall any email that is source of the disclosure
  - Outlook recall is worthwhile but not reliable
- Request secure deletion of the email, document or information sent/uploaded in error
  - Investigate, with Privacy Office guidance, the scope of the disclosure, e.g. who saw it, how many, did they download/export/forward, etc.
  - Request written confirmation that the document has been **deleted from all devices and systems, including email, backup and file storage**
- Other breach types may require additional remediation/corrective action

Breach Response

- Information to include in communication with Privacy Officer
    - Description of event including incident date, discovery date, name/MRN of affected subject(s)
    - Copy of consent forms (if applicable)
    - Communication/emails showing PHI breach.
    - ClickIRB #
    - Is the recipient/organization a covered entity under HIPAA?
    - Does the recipient /organization have a contractual commitment of confidentiality?

- After investigation/analysis, Privacy Office may need to notify affected subjects of the disclosure, as well as the Office of Civil of Rights (part of Health and Human Services)
    - Fact –based determination depending in part on nature and extent of PHI disclosed

Breach Response

If in doubt, report !

- HIPAA Policy 30 creates a duty to report
- Notify your supervisor. You or your supervisor should call the URMC Integrity Hotline at 585-756-8888 or contact a Privacy Officer. Calls to the Hotline may be made anonymously.
- Prompt reporting is critical. If the event is a breach, there are strict deadlines for reporting it to authorities and notifying affected patients.

Duty To Report Unauthorized Use Or Disclosure

Snooping

You must have a **job-related reason** to use or disclose PHI

Don't

- Look up your colleague's record because she has been out ill and you are concerned
- Review a neighbor's chart because your Mom heard he was taken to the ED
- Check on someone who failed to qualify for your study several months later, because he seemed like a nice guy

Your accesses are audited – "electronic footprint"

Snooping : No job-related reason

You must use or disclose only the **minimum necessary** information

- Protocol defines what is the relevant medical record information, e.g. exclusion criteria
- Examples of more than Minimum Necessary:
  - Reviewing mental health notes about a subject in a stroke study
  - Reading encounter note when only demographic or contact information was necessary

Minimum Necessary Rule

Outside the United States: GDPR and more

European Union General Data Protection Regulation (2019):

- Gives various rights to European data subjects, including copies of data, accounting of accesses
- Applies to any entity, including non-EU entities, which collect or process data of subjects residing in the EU
- Even if UR just processes (e.g. does analysis of) EU subject data, GDPR has indirect impact
    - EU entity that collected and controls the EU subject data has obligations which it must pass on to UR

INTERNATIONAL IMPLICATIONS

GDPR Compliance

- Requires implementation of technical and operational measures
- Must give EU subjects notice of their rights (usually paired with Informed Consent)
- May need to enter “standard contractual clauses” specified by EU regulators, with the EU collector (“controller”) of the subjects’ data
- Caveat: GDPR applies even to coded data (called “pseudonymized”), but it does not apply to fully anonymized data

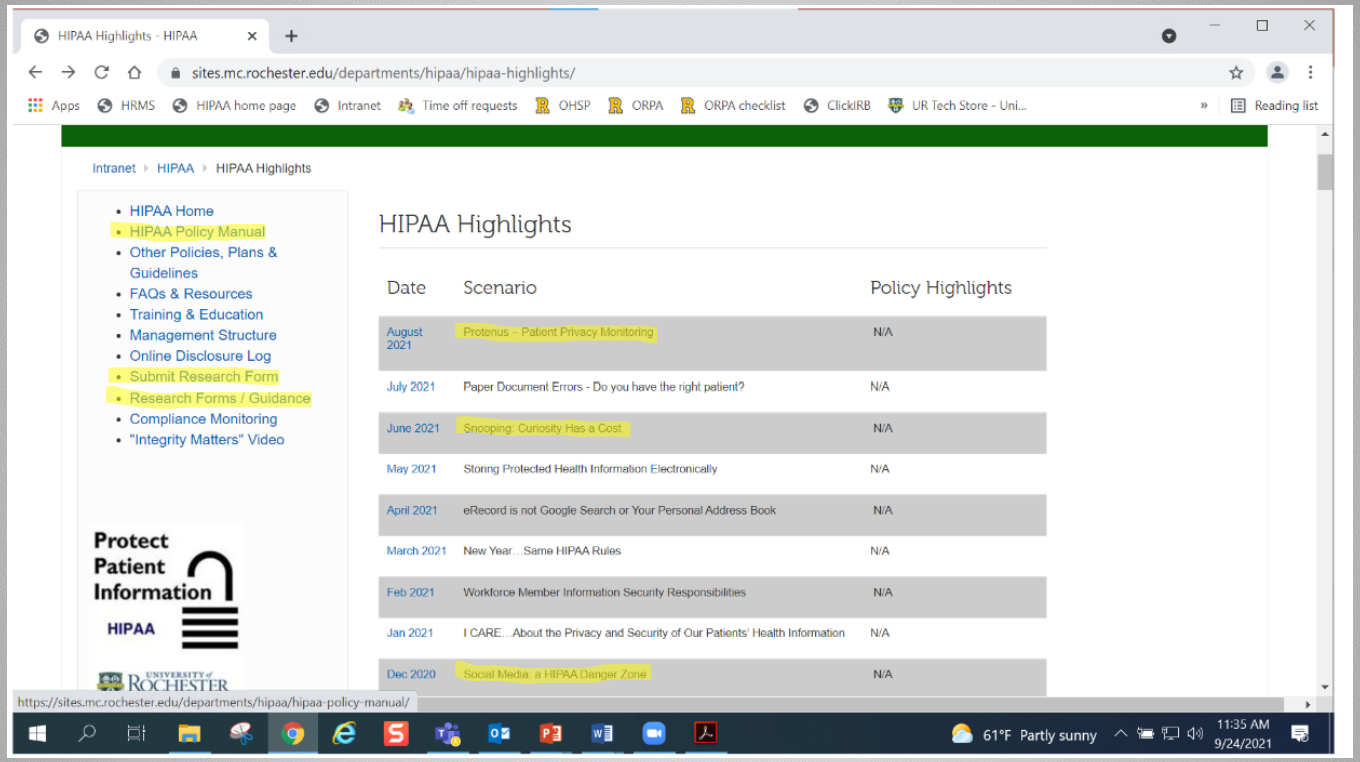
More: China has a similar law. PI is responsible to comply with local law; this may require use of outside counsel if there’s no local partner

INTERNATIONAL IMPLICATIONS

Resources

- HIPAA Privacy Policy 0P25 Use or Disclosure of PHI for Research Activities
- HIPAA Policy 0P9 Accounting of Disclosures
- OHSP Policy 702 HIPAA Privacy Rule
- OHSP Explains…Navigating HIPAA Compliance in Human Subject Research: The Privacy Rule; The Security Rule
- GDPR Q & A for Researchers
- URMC HIPAA Website - includes links to research forms and monthly HIPAA Highlights

Refer to the URMC HIPAA website for full policies/ procedures, training modules and other important information



Check Out the URMC HIPAA Website

QUESTIONS?

Kathleen_Tranelli@urmc.rochester.edu
784-6154