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

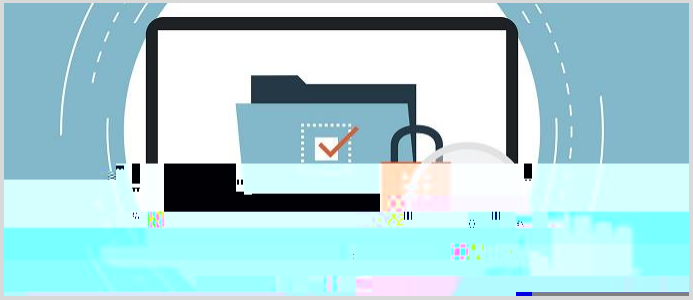
Overview of HIPAA
Bases for Use and Disclosure of PHI in Research
External uses and disclosures
Security Considerations
Common mistakes/ Cautions for Research Coordinators
Breach response
International Considerations

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

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-

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:

Limited Data Sets

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

Ensure agents/contractors agree to same restrictions

Preparatory to Research

Examples: Cohort identification, feasibility reviews

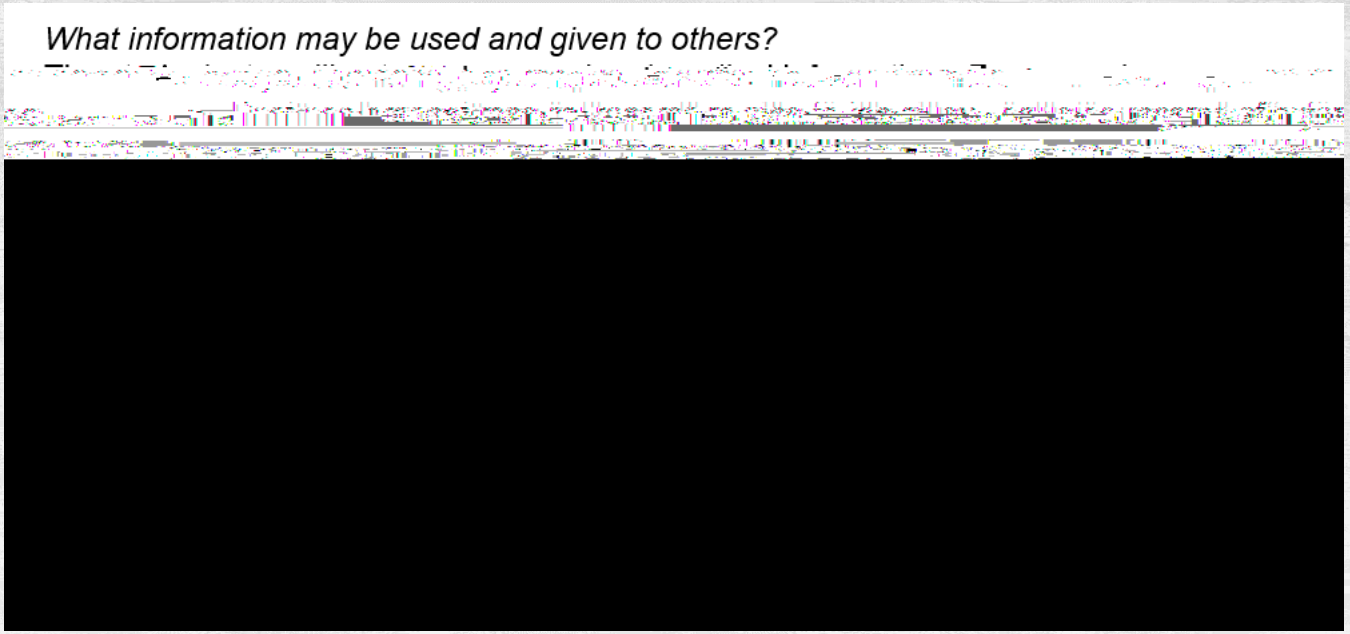
Researcher attestation (Form 25.3) required (except if PI/researcher is accessing only records of own patients)

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.)

AUTHORIZATION:

Excerpts from Bio-Medical Study Informed Consent Template



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

HIPAA-permitted research

or

HIPAA BASES for USING or DISCLOSING PHI

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

EXTERNAL DATA SHARING

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

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?

Security Rule

Requires covered entities to

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

- ü Cloud storage (Box.com)
- ü REDCap database

Follow Research Data Security Classification guidance

SECURITY CONSIDERATIONS

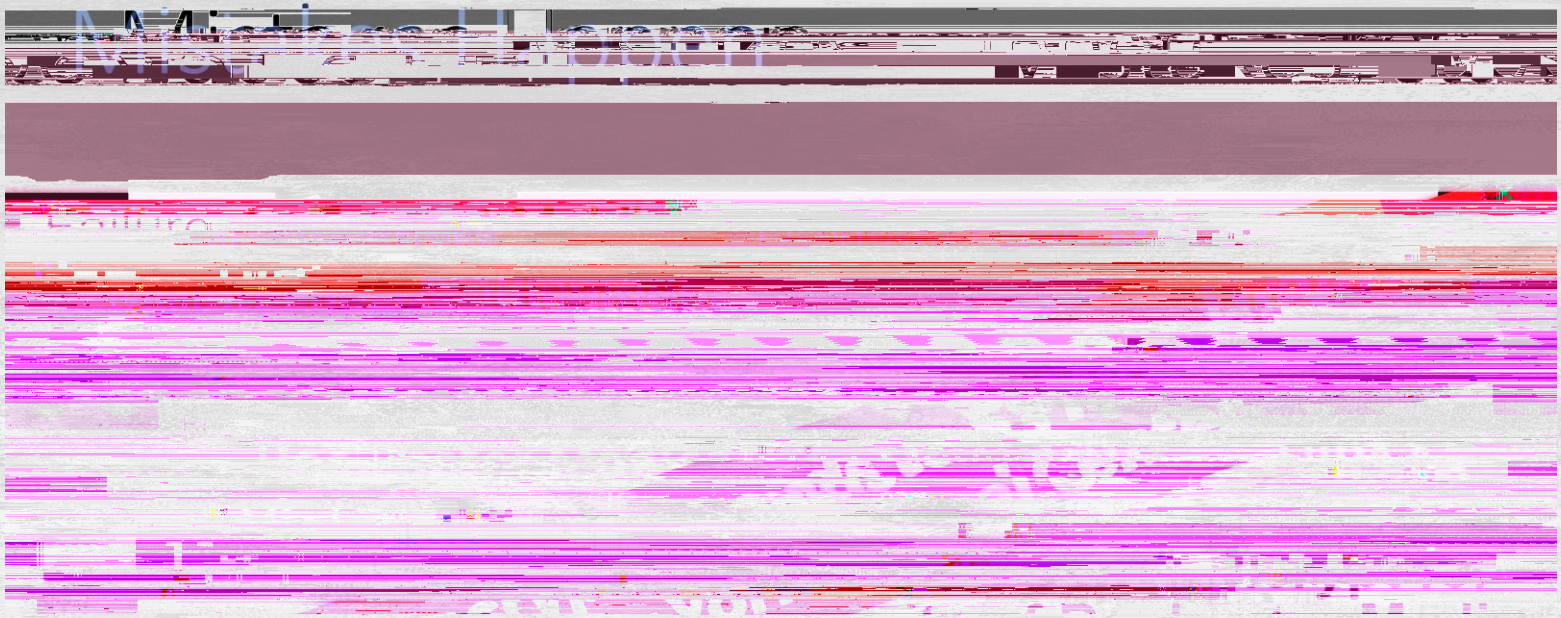
Day-to-day use of electronic media:

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 _____
Beware of phishing
Encrypt email with PHI via
Email and texting to subjects requires risk disclosure

See also: _____

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



Let’s Stay Out of the News :-)

CAUTIONS FOR RESEARCH COORDINATORS

Inadvertent Disclosures

Misdirected documents e.g. lab requisition to the wrong patient

Misdirected email

Watch out!

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

Emailing PHI: Important Tips

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.

Attachments: Removing PHI

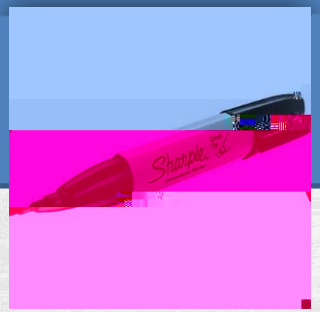
Printed Materials:

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.

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

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

Look up your colleague record because she has been out ill and you are concerned

Review a

Check on someone who failed to qualify for your study several months later, because he seemed like a nice guy

Your accesses are audited

Snooping : No job-related reason

Minimum Necessary Rule

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

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

GDPR Compliance

Requires implementation of technical and operational measures

Must give EU subjects notice of their rights (usually paired with Informed Consent)

Caveat: GDPR applies even to coded data (called

More: China has a similar law. PI is responsible to comply with local

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

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

QUESTIONS?