Research HIPAA Training

45 CFR 160, 45 CFR 164 Subpart E &
Health Information Privacy – Research (Guidances)

v2.0 effective 30 April 2020

Jeannie Perkins, MS, CCRP, CRCP

Chief Research Compliance Officer

(Data Protection Officer; Director of the HRPP)

The HIPAA Privacy Rule

- Addresses the use and disclosure of Protected Health Information (PHI) by organizations subject to the Privacy Rule (Health Insurance Portability & Accountability Act, HIPAA), called covered entities
- Requires safeguards to protect PHI and sets limits and conditions on uses/disclosures but still allows researchers to access the medical information needed to conduct research
- Gives individuals rights over their health information; they must be informed of:
  - The uses/disclosures of their PHI for research purposes
  - Their right to access their information held by covered entities
  - Their right to complain to covered entities/HHS
- The Health Information Technology for Economic and Clinical Health Act (HITECH Act) further supports HIPAA requirements by establishing the Breach Notification Rule (see Slide 13 herein) and the enforcement of HIPAA

Key Definitions

- **Covered Entities (CE) –** health care providers (among others) who transmit health information (e.g. doctors, clinics, hospitals) and must comply with HIPAA = ***Our clinical sites***
- **Business Associates (BA)** – entities that perform functions involving the use/disclosure of PHI on behalf of, or provides services to, a CE
  - Sending data to JCHR for data analysis = JCHR is a BA
  - NOTE: JCHR is not necessarily a BA (as it's usually our research), but we have to comply because we rely on CEs to provide PHI to us
- **PHI** – individually identifiable health information, held or maintained by a CE or its BAs, that is transmitted or maintained in any form

CE & BA Requirements
(45 CFR 164.308, .310, .312, .314, .316)

- We must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use/disclosure/request (i.e., research)
- Ensure confidentiality, integrity, and availability of PHI created, received, maintained, or transmitted (i.e., secure database)
- Protect against reasonably anticipated threats to security/integrity of PHI by putting security measures in place (e.g., limit access to workstations/ programs, use malware, have logins/passwords, automatic logoff, encryption, transmission security, address incidents)
- Protect against reasonably anticipated uses/disclosures of PHI that are not permitted (e.g., train sites to only send redacted material to JCHR)
- Implement policies & procedures (review & update periodically); ensure employees are compliant (e.g., auditing and audit trails)

What is PHI?
The 18 HIPAA Identifiers

https://privacyruleandresearch.nih.gov/pr_08.asp

- Names (including initials)
- Geography smaller than state
- Dates (except year) directly related to individuals (discharge, DOB)
- Phone number
- Fax number
- Email address
- SSN
- MRN
- Health plan numbers
- Account numbers
- Certificate/license #
- VIN, serial number, license plate #
- Device identifiers, serial numbers
- URLs
- IP addresses
- Biometrics (retina, fingerprint, voice)
- Full-face photos or other comparable images
- Any other unique identifying #, characteristic, or code

NOTE: Retinal images are PHI too!

What About De-Identified Data?
(45 CFR 134.514 (a-b) & Guidance 1.3)

- If there is no reasonable basis to believe that information can be used to identify someone, it is not individually identifiable health information and is considered **de-identified**
- Required de-identification methods of PHI:
  - Expert Determination
    - Applied statistical methods → There is a very small risk that individuals could be identified
  - Safe Harbor
    - Remove all 18 identifiers → No actual information present to identify an individual

What if You Can't Fully De-Identify?
(45 CFR 164.514 (e) & Guidance 2.10)

- An entity may use/disclose under a **Limited Data Set**
  - Can only contain de-identified information, *and/or*
  - Only dates, or other potentially unique identifying numbers, characteristics or codes – not otherwise specified in the other 16 HIPAA identifiers
  - Limited Data Sets may contain identifiable information and are still PHI, so entity and recipient must enter into a Data Use Agreement
- **Data Use Agreement (DUA)**
  - Establishes how data may be used, by whom, and how it will be protected
  - Recipient must use appropriate safeguards & cannot use data in a way not accounted for in DUA; must report to entity any use/disclosure not provided for

PHI in Email

- **Internal JCHR staff** – PHI may be included in email between authorized internal staff; limit to minimum necessary
- **External individuals** – Include only the PHI essential for the task (e.g., sending an email to a participant – email is obviously included, but exclude any other PHI); use JCHR webmail and a secure device (e.g. encrypted laptop)
  - Don't auto-forward from a JCHR account that may receive PHI
  - Don't send PHI via an instant messaging application (unless confirmed to be secure by contacting RCC@jaeb.org)
- **Encryption** – email attachments are acceptable if:
  - Encryption password meets minimum requirements (at least 10 characters with letters and numbers)
  - Communicate password through a method other than email
  - Options: encrypt a PDF or zip file; encrypt in Microsoft Office

Precautions You Can Take to Protect PHI

- Avoid conversations involving PHI in common areas
- Do not leave PHI in a voicemail
- Confirm that anything mailed or emailed to a participant corresponds to that participant
- Never leave PHI unattended whether in your office, in conference rooms or at printers, fax machines, or copiers
- Deposit PHI in a Shred-it® box when no longer needed
- Access PHI from a secure off-site location via JCHR's VPN instead of carrying it
- Encrypt devices that can access PHI (laptop computer, cell phone)

- **If you accidentally disclose PHI or come across unattended PHI (e.g. fax left in CCA), inform the Data Protection Officer immediately (DPO@jaeb.org)**

HIPAA Breaches

- A breach is the acquisition, access, use, or disclosure of PHI in a manner that compromises its security or privacy
- A breach does not include:
  - Unintentional acquisition, access, or use of PHI by someone acting under the authority of a CE/BA if it occurred in good faith within the scope of authority and does not result in further use/disclosure (e.g., a JCHR employee not on that specific study)
  - An inadvertent disclosure by someone authorized to access PHI at a CE/BA to another authorized person at the same CE/BA (e.g., Bob sent to Susan, both are JCHR employees, but Susan not on specific study)
  - A disclosure of PHI where a CE/BA has good faith that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information (e.g., accidentally overheard a name spoken in the hallway)

Reporting HIPAA Breaches

- A breach is reportable if the entity cannot ***demonstrate*** that there is a low probability that the PHI has been compromised based on a ***risk assessment*** of at least the following factors (consult the Data Protection Officer (DPO) at DPO@jaeb.org):
  1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  2. The unauthorized person who used the PHI or to whom the disclosure was made;
  3. Whether the PHI was actually acquired or viewed; and
  4. The extent to which the risk to the PHI has been mitigated

Reporting HIPAA Breaches

- The Research Compliance Committee (RCC) must be notified within twenty-four (24) hours of identification of a breach at RCC@jaeb.org
  - The RCC will advise regarding corrective and preventive actions
- The Institutional Review Board (IRB) must be notified of any qualifying breaches within seven (7) calendar days on an Significant Deviation/Noncompliance xForm via IRBManager
  - The Director of the HRPP will determine if any other institutions/sites need to be notified, and then will notify accordingly
- NOTE: Per regulation, the BA (JCHR) must notify covered entities if a breach occurs at or by the BA. The CEs (sites) must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, the media. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

When Can We Use/Share PHI for Research Conduct?

- When there is a Business Associate Contract/Agreement (45 CFR 164.502(a)(3)), and/or
- When use is approved for research whereas (45 CFR 46.512(i)):
  - Subject/legally authorized representative (LAR) has provided permission (HIPAA language/authorization), or
  - Without individual authorization if:
    - CE (IRB) says that subject/LAR does not have to provide authorization, in whole or in part (e.g., teen gender identity study, because obtaining authorization from a parent could violate the rights of the teen)
    - CE (IRB or Privacy Board) approves Preparatory to Research Activities, known as a Partial HIPAA Waiver (e.g., site wants to pre-screen from their hospital medical records)
    - CE (IRB) confirms that the research is of decedents only

Creating HIPAA Authorizations

- Focus on the privacy risks; state how, why, and to whom PHI will be used/disclosed
- Signed copy must be provided to participant/LAR
- Must be retained by the CE for no less than 6 years
- Can be combined with study consent or remain separate; written in plain language (NOTE: Some states have other requirements)

- **Core elements**:
  - Description of PHI to be used/disclosed
  - Identification of the person(s)/class of persons authorized to use/disclose and those to whom the CE may disclose
  - Purpose of each requested use/disclosure
  - Authorization expiration date or expiration event, e.g. “end of study” or “none”
  - Participant/LAR signature and date

HIPAA Authorizations

- **Required statements**:
  - Participants have the right to revoke authorization and explain how; exceptions to this right if applicable
  - Whether treatment, payment, enrollment, or eligibility of benefits is conditional on authorization, including research-related treatment and consequences of refusing to provide authorization (e.g., you can't be in the study if you don't want to provide PHI as it is necessary for the study)
  - Potential risk that PHI will be re-disclosed by the recipient; may include a statement that HIPAA may no longer protect health information disclosed to the recipient

General Waiver/Alteration Criteria
(45 CFR 164.512(i)(2)(ii))

Can waive/alter if all of the following are true:

1. Use/disclosure involves no more than minimal risk (Using the gender identity example, what if study involves investigational hormonal replacement therapy? It would no longer be minimal risk, so waiver would not be OK)
2. Have adequate plan to protect PHI from improper use/disclosure
3. Have adequate plan to destroy PHI at earliest opportunity unless otherwise justified or required by law
4. Confirm PHI will not be reused/disclosed to others except as required by law
5. Confirm research couldn't be practicably carried out without waiver/alteration
6. Confirm research couldn't be conducted without access to/use of PHI

Preparatory to Research: Partial HIPAA Waiver Criteria
(45 CFR 164.512(i)(2)(a-c))

- PHI use/disclosure is solely to prepare for research (e.g., prescreening)
- PHI cannot be removed from the covered entity (i.e., cannot leave the site)
- PHI access/use is necessary for the research purposes (e.g., can't enroll if I cant identify potential participants)
- **What could be covered:**
  - Reviewing ER admissions to see if the population I want to study is abundant enough to meet the sample size
  - Prescreening medical records to see who might qualify for study
- **What is <u>not</u> covered:**
  - Sending PHI to a Reading Center to get certified to work on a study

Questions, Comments, Concerns?

DPO@jaeb.org