Overview:
Health Insurance Portability and Accountability Act (HIPAA) and Research

CADC Scientists Monthly Meeting

Steve Gregorich
August 8, 2017

Health Insurance Portability and Accountability Act (HIPAA) and Research

Common confusion about how HIPAA impacts research requirements

Potentially, differing interpretations across institutions and IRBs

Within institutions, details/definitions are not always well-articulated;
Researchers, IRB members, attorneys often lack a ‘shared’ language

This presentation will summarize

. Some HIPAA definitions and concepts

. Key University of California (UC) positions on HIPAA & research

Like all institutions, the UC position on HIPAA & research is evolving

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA *Privacy Rule*

Protect confidentiality & security of PHI arising from health care provision

. 18 HIPAA Identifiers

Names	Account numbers
Geographic subdivisions smaller than a state, Geocodes	Certificate/license numbers
Dates. All elements of dates except year, unless individual is > 89 yrs.	Vehicle identifiers/serial numbers
Telephone numbers	Device identifiers/serial numbers
Fax numbers	Web URLs
Electronic mail addresses	IP addresses
Social security numbers	Biometric identifiers
Medical record numbers	Full face photographic images
Health plan beneficiary numbers	Any other unique identifying number, characteristic, or code

Entities Subject to HIPAA: Covered & Hybrid Entities

Covered Entity

. An organization that has to comply with HIPAA

. *Health care provider* that conducts certain transactions in electronic form

(furnish, bill, or receive payment for health care in the normal course of business *and* transmit any covered transactions electronically)

. *Health care clearinghouse*, or

. *Health plan*

Hybrid Covered Entity: UCSF is a Hybrid Covered Entity

. A single entity that performs both covered and non-covered functions

. Split operations: health care versus non-health care components

. Most Privacy Rule requirements apply only to health care components

. E.g., research labs excluded from the hybrid entity's health care components are not subject to the Privacy Rule

Use and Disclosure of PHI

. When PHI is shared w/in a covered entity, that is a use of the PHI

. When PHI is shared outside a covered entity, that is a disclosure

. HIPAA allows use and disclosure of PHI for research purposes

Such uses and disclosures must follow HIPAA guidance and must be part of a research plan that is IRB-approved

Use and Disclosure of PHI

. E.g., Participants sign a HIPAA Authorization to have PHI from their medical record disclosed to an investigator for research purposes (or a waiver allowing disclosure of PHI is issued by the IRB)

. Once the information is transcribed into the research record

- . It is no longer PHI subject to the HIPAA Privacy Rule
- . It is governed by the HIPAA Authorization terms & informed consent
- . These research data derive from voluntary participation in a study, not as a result of a healthcare provision event
- . Best practices for research involving human subjects must be held

Creation of PHI by a Research Project

Research studies conducted by non-covered entities can create PHI

. If a research study

(1) Provides health care, *and*

(2) Personally-identifiable information from the research study is entered into the existing medical record of a covered entity,

. Then the research data entered into the medical record becomes PHI

This is the only way that a research project conducted by a non-covered entity can create PHI

. However, the corresponding research data held in the research database is <u>not</u> PHI and is <u>not</u> governed by the Privacy Rule

Best Practices for Research that is not Subject to HIPAA…

…require

. Maintenance of confidentiality

. Security of information

. 'Need to know'

. Minimum necessary information collected

. Separation of person-identifiable data from scientific data

. Role-based access control for individually-identifiable data elements

…but, typically do not require

. HIPAA administrative requirements for business associate agreements

. Logging of disclosures

. Audit trails

Summary

The label ‘PHI’ should be used sparingly to refer to the 18 types of identifiers that are created, received, or maintained *by a covered entity* under HIPAA (or a health care component of a hybrid covered entity)

With appropriate authorization, research conducted by non-covered entities may access PHI from patient medical records of a covered entity, but once received, those data no longer constitute PHI

Research data created, received, or maintained by non-covered entities does not include PHI and is not governed by HIPAA

According to UC, PHI-like information in a research data record constitutes *Research Health Information* (RHI).

RHI is not subject to the HIPAA Privacy Rule, but is subject to standard 'best practice' guidelines for research

Q&A

Q: Is the research team/center/unit/lab conducting the research considered a *covered entity* (or a health care component of a *hybrid covered entity*) that is subject to HIPAA?
For the types of research that we conduct, the answer is 'No'

Q: Are data elements that a research project collects directly from voluntary study participants, under informed consent, considered by UC as PHI that is subject to HIPAA? No

Q. If a research project obtains HIPAA Authorizations (or a waiver) to abstract/extract PHI from the medical records of a covered entity and subsequently enter the abstracted data elements into the research data base, does UC consider the abstracted data elements in the research data to be PHI subject to HIPAA? No

Q. UC does require the research data systems and processes used by non-covered entities to be fully compliant with HIPAA standards? No

Is a person, business, or agency a covered health care provider?