Got Data?

Data Protections Guidance for IRB Members

IRB Member Training – May, 2018

Definitions

Anonymous data: Data that at no time has a code assigned that would permit the data to be traced back to an individual. This includes any information that was recorded or collected without any of the 18 identifiers as defined by HIPAA. Note that IP addresses are considered to be identifiable even though the address is linked to the computer and not specifically to the individual

De-Identified: Investigator cannot readily ascertain the identity of the individual

Coded: Identifying information (such as name) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a code (number, letter, symbol, or any combination) and a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens

Definitions

Protected Health Information (PHI): All individually identifiable health information transmitted or maintained by a covered entity, regardless of form or media

- Excludes education records
- Excludes employment records

PII: Personally Identifiable Information: "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[1]

Sensitive Research Data: Data is considered sensitive when disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation.

Definitions (HIPAA)

Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard (e.g. billing to insurance)

Use: the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component

Disclosure: The release, transfer, access to, or divulging of information outside the entity holding the information.

Minimum Necessary: The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request.

Sensitive Data

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Family Educational Rights and Privacy Act (FERPA)

Children's Online Privacy Protection Act (COPPA)

Pennsylvania Confidentiality of HIV-Related Information Act

Pennsylvania Drug and Alcohol Abuse Control Act

Pennsylvania Mental Health Procedures Act

Other sensitive issues:

- Credit card data
- Social Security Numbers
- Mobile/social media applications

HIPAA

HIPAA Privacy Rule

Protects privacy of patient records provided to health plans, doctors, hospitals and other health care providers

Provides patients with access to their records and more control over how their Protected Health Information (PHI) is used and disclosed

Regulates the collection and use of PHI for research purposes

Equal standards of privacy protection for all research using PHI

**Applies to Covered Entities

HIPAA Security Rule

Establishes national standards to protect electronic protected health information (PHI)

Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI

HIPAA at Penn

Covered Entities:

Penn School of Medicine/ University of Pennsylvania Health System (UPHS)

Penn School of Dental Medicine

Living Independently for Elders (LIFE) Program

Student Health Services

HR Benefits Program

**Workforce members from offices at Penn that support any of the covered entities names above must also comply with HIPAA requirements (the IRB is included in this)

Who enforces HIPAA?

HIPAA is enforced nationally by the Office of Civil Rights

HIPAA Privacy Officers (Each covered entity at Penn has at least one. At Penn, these individuals are responsible for ensuring compliance with the HIPAA privacy rule, including the review of potential breaches for potential reporting)

Lauren Steinfeld – Penn Medicine Chief Privacy Officer

HIPAA Security Officers (These individuals handle information security to ensure plans for data protection and storage meet HIPAA requirements)

The Privacy Board (the IRB)

The Privacy Rule requires that waivers/alterations be reviewed by either a privacy board or an IRB

Some institutions have separate review entities

Composition requirements are similar but not equivalent

HIPAA and Research

Protections increase as the level of PHI increases

Research with De-Identified Data

Research using some (Indirect) identifiers

Research using major (Direct) identifiers

Authorization or Waiver Required

Research using Direct Identifiers

The use of direct identifiers requires either a HIPAA waiver or authorization

Waiver/Authorization must be reviewed by the privacy board

The waiver or authorization is generally for a single use

Alterations of HIPAA [e.g. altering the signature requirement] may be permissible as it is for consent

Protected Health Information: Major (Direct) Identifiers

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

Research using Some (Indirect) Identifiers

Can qualify as a limited data set provided:

All16 major identifiers are excluded

A limited data set may include:

city, state, zip code

elements of dates related to subject

other numbers, characteristics or codes not listed as direct identifiers

Protections:

No authorization/waiver is required for use/disclosure

In order to disclose a limited data set, a data use agreement is required

Data Use Agreement Defined: An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

Research with De-Identified Data

Definition of De-Identified Data:

Must exclude all 16 major identifiers

In addition must exclude

all geographic identifiers smaller than State (may include first three digits of zip code, depending on whether the population in that zip code > 20,000 people)

-all elements of dates (except year) directly related to the individual (for individuals over 90, all individuals over 90 can be reported in aggregate)

any other unique identifying number, characteristic or code.

The covered entity disclosing the information may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual.

Requirements: NONE

Caveat: For research purposes, must comply with all other IRB requirements for approval

Other Activities with PHI

Preparatory to Research

No Authorizations/Waivers required

May use PHI to prepare a research protocol or for similar purposes preparatory to research provided:

- The PHI is not disclosed outside of the covered entity
- The PHI is necessary for the research
- The use clearly meets the definition of "preparatory to research"
  - *Examples:*
    - Searching charts to identify the number of incidents of a certain condition for preparation of a protocol
    - Reviewing charts to obtain contact information for recruitment purposes for an IRB-approved study

Common Questions

Where are the materials coming from?

How many subject records/specimens are involved?

Where will the data be stored once you obtain it?

How long will you retain identifiable information? Will there be a separate linking set?

Who will you share materials with?

What is HIPAA Authorization?

Definition: An individual's express permission to allow a covered entity to use or disclose specified PHI for a particular purpose.

Must contain the following key elements:

- The PHI collected as part of the study
- The purpose of the use/disclosure
- Who may use or disclose PHI
- Who may receive PHI
- The duration of the authorization (if it does not expire, this should be indicated)
- The right to revoke the authorization
- A statement that once information is shared outside of the covered entity it may no longer be protected by HIPAA

When do I not have to obtain consent and HIPAA authorization?

When you meet the following criteria for a consent waiver:

Study poses no greater than minimal risk

Waiving consent does not impact subjects rights or welfare

You have a mechanism for returning pertinent information to subjects

The study cannot be practicably conducted without the waiver

Waiver of HIPAA Authorization

Use or disclosure involves no more than minimal risk to the individuals

IRB Application should include:

- *adequate plan to protect PHI from improper use/disclosure*
- *adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research*
- *adequate written assurances that PHI will not be reused/disclosed*
- *Justification for why the research could not be practicably conducted without the waiver*
- *Justification for why the research could not be practicably conducted without access to the PHI*

ePHI Requirements

https://irb.upenn.edu/mission-institutional-review-board-irb/guidance/other-elements-research

Data Storage

ePHI requirements

- Institutionally secured & managed network drive
- Institutionally secured & managed device
- Institutionally- approved third-party computing environment

Encryption of data on device to protect against loss/theft of device

Use of secure data transmission channels to protect against data interception

Strong passwords to protect against unauthorized access

Store data behind a secure Penn or UPHS firewall whenever possible

Ensure strong data security controls on all storage sites

Transmission

Recommend using a secure transmission process even if the data is anonymous, coded, or non-sensitive information

Encrypt, encrypt, encrypt

Use of a Penn- approved encrypted portable drive

Utilize Penn-approved secure encrypted file transfer solution

For assistance in selecting a Penn-approved portable drive or secure file transfer solution, please contact your Local Support Provider/Security Liaison.

Email/Texts

Email notifications are generally not secure, except in very limited circumstances, and should not be used to share or transmit research data.

Text messages are stored by the telecommunications provider and therefore are not secure. Data should be encrypted when "in-transit," and the University provides extensive guidance, software, and resources to assist researchers in this.