Northwestern University IRB Guidance on Evaluating Reports of Data Incidents

The federal regulations (45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)) require that research involving human participants have adequate provisions in place to protect the privacy of participants and maintain data in a confidential manner in order for the research to receive IRB approval. Additionally, the respect for persons and beneficence principles of the Belmont Report require the IRB to ensure the participants' privacy and confidentiality are protected throughout the course of the study.

The purpose of this guidance is to distinguish between different types of data, establish the difference between privacy and confidentiality, and assist in the preparation of Reportable New Information (RNI) submissions involving data incidents.

Key Definitions

Health Insurance Portability and Accountability Act (HIPAA):

An act passed by Congress in 1996, HIPAA does the following:

- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
- Reduces health care fraud and abuse;
- Mandates industry-wide standards for health care information on electronic billing and other processes; and
- Requires the protection and confidential handling of protected health information

Protected Health Information (PHI):

Individually identifiable information relating to an individual's past, present, or future health status created, collected, transmitted, or maintained by a HIPAA-covered entity for the provision of healthcare, payment for healthcare services, or use in healthcare operations. Under HIPAA, there are 18 unique identifiers of the individual or of relatives, employers, or household members of the individuals that, when combined with health information, constitute PHI. The 18 identifiers are as follows:

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers

9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

Personally Identifiable Information (PII):

Data that could potentially be used to identify a particular person. Examples of PII include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

What is the difference between PHI and PII?

Information or data from the medical records can be used to identify an individual are considered to be PHI before the individual signs an authorization to access or use the data, or the IRB, acting as the privacy board, grants a waiver of the requirement to obtain documented HIPAA authorization. At Northwestern, the authorization is included at the end of an informed consent form. Data are considered to be PII after a consent form has been signed.

See additional information here.

Anonymous:

Data are anonymous if no one, including the researcher, can connect the data to the individual who provided it. No identifying information is collected from the individual, including direct identifiers such as name, address, etc.

De-Identified:

Data are de-identified when any direct or indirect identifiers or codes linking the data to the individual subject's identity are stripped and destroyed. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

Coded:

Identifying data (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. The code cannot include information about the individual, such as initials, numerical representations of birth date, etc.

Confidential:

Confidential data includes a link between the data and the individual who provided it. The research team is obligated to protect the data from disclosure outside the research according to the terms of the research protocol and the informed consent document.

Identifiable:

> ***Direct Identifiers:*** information that can be directly linked to an individual or of relatives, employers, or household members of the individual, such as name, address, etc**.**
>
> ***Indirect Identifiers:*** information regarding other unique individual characteristics of an individual or of relatives, employers, or household members of the individual

Sensitive information:

PHI that includes psychotherapy notes or information relating to relating to HIV/AIDS; behavioral or mental health; developmental disabilities; treatment for substance (alcohol or drugs) use disorder; genetic testing and counseling; artificial insemination; sexual assault/abuse; domestic abuse of an adult with a disability; child abuse and neglect; and, if the individual is a minor, sexually transmitted illnesses, pregnancy and birth control.

Privacy:

A person's desire to control the access of others to themselves. For example, persons may not want to be seen entering a place that might stigmatize them, such as a pregnancy counseling center that is clearly identified as such by signs on the front of the building. Privacy concerns people, whereas confidentiality concerns data.

Confidentiality:

An extension of privacy that refers to the researcher's agreement with the participant about how the participant's identifiable private information will be handled, managed, and disseminated.

What is the difference between privacy and confidentiality?

Privacy ***"People"***	**Confidentiality** ***"Data"***
• The way potential participants are identified and contacted • The setting where potential participants will interact with the researcher team and who is present during research procedures • The methods used to collect information about participants • The type of information being collected • Access to the minimum amount of information necessary to conduct the research	• An extension of privacy • Pertains to identifiable data • An agreement about maintenance and who has access to identifiable data • What procedures will be put in place to ensure that only authorized individuals will have access to the information, and • Limitations (if any) to these confidentiality procedures • In regards to HIPAA, protection of patients from inappropriate disclosures of Protected Health Information (PHI)

Data Incident:

An event that leads to a violation of data policies and puts data at risk of exposure. This is a broad term that includes many different kinds of events.

Data Breach:

Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. Any actual or suspected data breach (including unauthorized access to or compromise of data, theft or removal of equipment, papers, storage media, etc.) must be reported immediately to: FSMIT-Policy@northwestern.edu. Those university staff who receive these reports will contact NMHC or SRAlab, as appropriate, regarding violations involving their respective PHI.

Preparing RNI Submissions that Involve Data Incidents

When reporting an event that involves data privacy, confidentiality, or a data incident, it is important to distinguish between research data and clinical data, and whether HIPAA is involved. Prepare and submit the event to the IRB in a Reportable New Information submission, following the appropriate timeline. In the RNI submission, select "**Confidentiality**" as one of the RNI categories. In the RNI summary, detail your plan to notify the appropriate contact(s) identified below to consult on the required next steps and the PI's planned corrective and preventive actions. Then, save a copy of your submitted RNI to your records and to include in your email to the contact(s) below..

In your email notification, include the following:

- A copy of the RNI;
- A summary of the event, including relevant dates, the roles of involved individuals, and other contributing factors;
- The current status of impacted participants/potential participants;
- Whether the event occurred before or after obtaining informed consent;
- The origin of potential participant data used for recruitment (e.g., Northwestern Medicine patients, Shirley Ryan Ability Lab patients, the Family Institute patients);
- The PI or designee's immediate actions taken to address the event; and
- Proposed preventive actions.

Please include the IRB Compliance Unit (irbcompliance@northwestern.edu) on all communications.

Contact:

- **Abby Cosentino-Boehm, DrPH**
  Director of Clinical Research Operations
  Feinberg School of Medicine
  a-cosentino-boehm@northwestern.edu

If the event involves Shirley Ryan AbilityLab (SRALAB), include the following contact **in addition** to the one above:

- **Pattie Gregory MS, CHC, CHRC, CHPC**
  Compliance Revenue Integrity Officer
  Shirley Ryan AbilityLab

  pgregory@sralab.org

When the above contacts have concluded their ancillary reviews, including directing the PI to take follow-up actions, which may include updates to the proposed corrective and preventive action plan, include the email correspondence with the individuals listed above within the supporting information section of the RNI application. Be sure to incorporate their required corrective and preventive actions into the final RNI submission. If a modification is required to resolve the event, please reference the modification number within the RNI submission.

Events should be reported in real-time, as soon as possible, even if a solution is pending.

Review the IRB Office's guidance on how to write an effective corrective and preventive action plan (CAPA).

Additional guidance on data retention and storage from the Office of Research and NUIT can be found at:

- Research Data Ownership, Retention, and Access Policy
- Guidelines for Security and Confidentiality of Data Files
- Data Access Policy
- HIPAA/ISO Information Security Guidance
- Protect Your Research Environment Guidance

Resources:

https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

https://www.hhs.gov/hipaa/for-professionals/index.html

https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

https://www.it.northwestern.edu/index.html

https://www.research.northwestern.edu/policies/