Evaluating Reports of Data Incidents

Purpose

This document provides guidance for the notification, reporting, and documentation of data incidents involving unexpected or incidental access to information. It is intended to assist researchers in responding appropriately when data is accessed or shared without prior intent or authorization and must be disclosed in accordance with organizational or regulatory requirements. This guidance helps ensure consistent handling, promotes transparency, and supports compliance efforts during such events.

Note: When data events occur, it is essential to determine 1) where the data originated and 2) which IRB oversees human subject protections oversight for the research study. These factors impact who must be notified, what information needs to be reported, and which IRB the event needs to be submitted to.

Regulations

This guidance supports compliance with federal regulations (45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)), which require that research involving human participants include adequate provisions to protect participant privacy and maintain data confidentiality. It also aligns with the ethical principles of *respect for persons* and *beneficence* from the Belmont Report, which require Institutional Review Boards (IRBs) to ensure the protection of participants' privacy and confidentiality throughout the course of a study.

Additionally, this guidance adheres to:

- HIPAA Privacy Rule (45 CFR Part 164, Subpart A and E), which establishes a category of health information, defined as protected health information (PHI), which a covered entity may only use or disclose to others in certain circumstances and under certain conditions.
- HIPAA Security Rule (45 CFR Part 164, Subpart C), which sets standards to protect the confidentiality, integrity, and availability of electronic protected health information.

Key Definitions

Data Incident: An event that results in unauthorized access, use, or disclosure in violation of applicable data protection policies. This includes incidents that compromise the confidentiality, integrity, or privacy of sensitive information such as Protected Health Information (PHI) or Personally Identifiable Information (PII).

Protected Health Information (PHI): Any health information that includes any of the 18 elements identified by HIPAA and maintained by a covered entity or any information that can be reasonably used to identify a person.

Personally Identifiable Information (PII): Data that, alone or when combined with other relevant information, could potentially identify a particular person. In research, this may include data obtained directly from participants through methods such as surveys or interviews. While it is not considered PHI and is therefore not subject to the HIPAA Privacy and Security Rules, PII is covered by other state and federal laws for the privacy and confidentiality of research health information.

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

For further details, visit the IRB Office webpage HIPAA, PHI, & PII.

Examples of Data Incidents

Data incidents may include, but are not limited to, the following examples:

- Sending communications to incorrect individuals *(e.g., recruitment letters addressed to the wrong patient)*
- Misplaced/lost fully executed consent forms containing a participant's name
- Sharing identifiable information with a study sponsor or non-IRB-authorized personnel
- Sending identifiable participant data to the wrong recipient via email
  Viewing or accessing identifiable data without authorization (e.g., not IRB-approved study team member, HIPAA waiver not granted, participant has not signed HIPAA authorization, etc.)

- Discussing identifiable participant information in a public/shared space.

Process for Notifying, Reporting and Documenting Data Incident Events

Step 1: Notification of the Event to the Northwestern Institutional contact and/or other affiliates as appropriate (complete all that apply)

a) If the event includes Northwestern data (i.e., Northwestern and/or Northwestern-affiliated): Notify the appropriate parties listed in Table 1 by email, describing at a minimum the incident and outlining the Principal Investigator's (PI) planned corrective and preventive actions. Consult with these contacts to obtain any additional guidance or required actions.

b) If the event did not include Northwestern data (i.e., Northwestern and/or Northwestern-affiliated): Notify only the privacy officer of the covered entity whose data was affected. For example, if the incident involved data from the external site, the Northwestern team should inform that site's study team, who will notify their own privacy office.

In the email notification to the appropriate parties, include all applicable items listed in **Table 2.** Please ensure the appropriate parties are notified prior to or at the same time as reporting the data event as a reportable new information to the IRB of Record in Step 2.

Step 2: Report the Event to the IRB of Record (complete all that apply)

Determine if the event meets IRB reportability requirements as soon as possible, even when a solution is pending.
Note: A data incident is considered an unexpected event if the risk of loss of confidentiality is described in the Informed Consent Form. Unintended disclosures of private/personal information are considered events that may cause harm, increase the risk of harm, adversely affect the rights or welfare of participants, or undermine the scientific integrity of the data.

a) If the event includes Northwestern data (i.e., Northwestern and/or Northwestern-affiliated) and Northwestern is the IRB of Record:

- Use the Incident Assessment Tool HRP-1207 (IAT) to determine reportability to the Northwestern IRB Office, document the event, conduct a root cause analysis, and form Corrective and Preventive Action (CAPA) Plans.
- Follow the appropriate timeline to submit a reportable new information (RNI) in eIRB+.
- In the RNI submission, select "Confidentiality" as one of the RNI categories.
- In the RNI summary, provide the communication with the institutional contacts as supporting documentation within the RNI. If this communication is not available, provide the plan to notify the appropriate institutional contact(s) to consult on the required next steps and the PI's planned corrective and preventive actions.

- Once the RNI is submitted and the required institutional contacts complete their reviews, including any directions for the PI to take follow-up actions, which may include updates to the proposed Corrective and Preventive Action (CAPA) Plan, provide the email correspondence with the required institutional contacts within the supporting information section of the RNI application, or by adding a comment to the RNI submission in eIRB+.
- If a modification is required to resolve the event, reference the modification number within the documentation of the event.

b) If the event does not include Northwestern data (i.e., Northwestern and/or Northwestern-affiliated) and Northwestern is the IRB of Record:

- Use the Incident Assessment Tool HRP-1207 (IAT) to determine reportability to the Northwestern IRB Office, document the event, conduct a root cause analysis, and form Corrective and Preventive Action (CAPA) Plans.
- If the event meets the Northwestern reporting criteria, the Northwestern study team should submit an RNI in eIRB+ and follow all guidelines mentioned directly above.
- Reminder: For any RNIs submitted to the Northwestern IRB involving a relying site, local reporting requirements may apply at the relying site. The NU PI and study team must pass any determinations to relying sites.

c) If the event includes Northwestern data (i.e., Northwestern and/or Northwestern-affiliated) and Northwestern is not the IRB of Record:

- Review the external IRB's reporting criteria and if criteria are met, submit an RNI to the external IRB. Note: sometimes this is facilitated by an external study team.
- If the event is reported to the external IRB, a parallel RNI submission is required in eIRB+ per HRP-092 SOP.

d) If the event does not include Northwestern data (i.e., Northwestern and/or Northwestern-affiliated) and Northwestern is not the IRB of Record:

- Review the external IRB's reporting criteria and if appropriate, submit an RNI to the external IRB (sometimes facilitated by an external study team).
- If the event is reported to the external IRB, follow guidance in HRP-092 SOP External IRBs regarding whether or not a parallel RNI in eIRB+ is required.

Step 3: Documentation of the Event in the research record

For any data incident, the PI or study team must document all relevant information in real time. The following should be saved in the study's research record:

- All correspondence with participants regarding the data event
- Copies of documentation submitted to, received from, or created for the IRB of record regarding the incident
- Any correspondence with external entities related to the event

Appendix

Table 1: Address these contacts in the email as applicable to the event

Required Northwestern Institutional Contact:	**Abby Cosentino-Boehm, DrPH** Director of Clinical Research Operations Feinberg School of Medicine a-cosentino-boehm@northwestern.edu **Copy the IRB Compliance Team** (irbcompliance@northwestern.edu) on all communications.
If the event involves **Shirley Ryan AbilityLab (SRALAB)**, include the following contact in addition to the **Required Northwestern Institutional Contact**:	**Sadie Sial** **Research & Compliance Analyst** Shirley Ryan AbilityLab ssial@sralab.org compliance@sralab.org **Copy the IRB Compliance Team** (irbcompliance@northwestern.edu) on all communications.

Table 2: In the email notification to the appropriate parties, include all applicable items

A summary of the event, including relevant dates, the roles of involved individuals, and other contributing factors;
A completed Incident Assessment Tool or a PDF copy of the draft or submitted RNI to document the event and corrective action plan;
The current status of impacted participants/potential participants (note: each data record is equivalent to a human participant);
Whether the event occurred before or after obtaining informed consent (and HIPAA Authorization), or if the IRB approved the study with a waiver of the requirement to obtain participants' HIPAA Authorization;
Any relevant reliance agreements; and
Describe the data. ▪ Explain where the data originated (e.g., Northwestern Medicine patients, Shirley Ryan Ability Lab patients, the Family Institute patients, etc.) ▪ Distinguish between research and clinical data. For example, determine whether the data includes PHI or PII.

Additional Resources

- Research Data: Ownership, Retention, and Access Policy
  - Northwestern University IT Policies, Standards, and Guidelines
  - Data Access Policy: Information Technology - Northwestern University
  - HIPAA/ISO Information Security Guidance
  - Protect Your Research
- Feinberg Information Security & Access Policy
- IRB Office HIPAA Requirements Webpage