Protecting Participants

25 April 2025

Personal Health Information

Personal Health Information is any information about an individual, whether living or deceased, in oral or recorded form. In practice that means any information that can be used to identify a patient.

This information might relate to:

- The individual's physical or mental health (including information about the health history of the individual's family)
- The provision of health care to the individual (including identification of a person as a provider of health care to the individual)
- Payments or eligibility for health care
- The donation by the individual of a body part or bodily substance
- The individual's substitute decision-maker.

- Medical Record Number
- Patient's Last Name
- Patient's First Name
- Full Address
- Employer
- Social Insurance Number
- Ontario Health Insurance Number
- Mother's Medical Record Number
- Visit Number
- Telephone Number

UHN corporate intranet: https://intranet.uhn.ca/departments/privacy/phi.asp

Privacy Considerations

- In accordance with Canadian Federal PIPEDA + Ontario PHIPA regulations (*and HIPPA in the United States*), we have a duty in healthcare to protect the health information of our patients
  - It is the responsibility of all hospital staff/team members to maintain and protect patient rights and privacy
- In research, we have additional responsibilities to protect patient information and be cautious in what we share as per TCPS-2 and GCP
  - Extra caution needs to be made in our role, as we are in a unique position where we do share a lot of information with external stakeholders (i.e. sponsors, monitors, REBs, etc.)
- In the chat, what are the potential risks and consequences of privacy breaches?

What is a Safety Event (formerly known as "incident")?

- Any unexpected, unusual or unplanned event and/or near miss affecting or potentially affecting a patient, visitor, staff, or UHN operations.
- Classifications (per UHN Policy 3.20.005)

  - **Near miss:** Incident identified, patient(s) not impacted.
  - **Minor:** Involves identifiable PHI and/or corporate confidential information (CCI), and at least one of the following:

    a. 1 to 10 individuals have been impacted
    b. no risk of intentional harm to individual(s)

  - **Moderate:** Involves identifiable PHI and/or CCI, and at least one of the following:

    a. 11 to 50 individuals have been impacted
    b. minimal risk of intentional harm to individual(s)

  - **Severe:** Involves identifiable PHI and/or CCI, and at least one of the following:

    a. 51 to 100 individuals have been impacted
    b. suspected risk of intentional harm to individual(s)

  - **Critical:** Involves identifiable PHI and/or CCI, and at least one of the following:

    a. more than 100 individuals have been impacted
    b. proven risk and/or confirmed case of intentional harm to individual(s)

What is a Privacy Breach?

- A type of safety event
- Any action that results in the inappropriate collection, use or disclosure of personal health information (PHI), including when PHI is lost or stolen.
- Examples:
  - A source document was not properly de-identified prior to being provided to the sponsor (e.g. In cases where these are routinely submitted as supporting documentation)
    - Fax/Scanned documents
  - A sponsor was copied on an email containing PHI
    - Best practice is to start a new email chain if PHI is involved.
  - Full DOB provided to sponsor when only partial DOB was REB approved
  - A lost/misplaced medical chart or research chart
  - Queries in EDC

How to check what PHI is approved for external rel

Review the current RE

OCREB

7.1 *What (if any) Personal Information or Personal Health Information will be sent to or colle
group for the purposes of this study (this includes specimens, questionnaires, diaries, re
etc.) (select all that apply)?

- ☐ None, study participant ID only
- ☐ Full name
- ☐ Full initials
- ☐ Partial initials
- ☐ Full date of birth
- ☑ Partial date of birth
- ☑ Full date of death
- ☐ Partial date of death
- ☐ Age
- ☑ Sex and/or gender
- ☐ Full postal code
- ☐ First 3 digits of postal code
- ☑ Pathology specimen number
- ☐ Medical device identifier
- ☑ Admission date
- ☑ Discharge date
- ☐ Medical record number
- ☐ Ontario health card number
- ☐ Driver's licence number
- ☐ Address
- ☐ Telephone number
- ☐ Fax number
- ☐ E-mail address
- ☐ Full face photograph
- ☐ Voice/audio recording
- ☑ Other information

7.1.1 *Specify other information:

-Study participant ID
-Race & ethnicity

7.1 *What (if any) Personal Information or Personal Health Information will be sent to or collected by the lead researcher/research group for the purposes of this study (this includes specimens, questionnaires, diaries, registration forms, case report forms, etc.) (select all that apply)?

- ☐ None, study participant ID only
- ☐ Full name
- ☐ Full initials
- ☐ Partial initials
- ☐ Full date of birth
- ☑ Partial date of birth
- ☑ Full date of death
- ☐ Partial date of death
- ☐ Age
- ☑ Sex and/or gender
- ☐ Full postal code
- ☐ First 3 digits of postal code
- ☑ Pathology specimen number
- ☐ Medical device identifier
- ☑ Admission date
- ☑ Discharge date
- ☐ Medical record number
- ☐ Ontario health card number
- ☐ Driver's licence number
- ☐ Address
- ☐ Telephone number
- ☐ Fax number
- ☐ E-mail address
- ☐ Full face photograph
- ☐ Voice/audio recording
- ☑ Other information

What do I do when I identify a Privacy Breach?

Note: The person who first identifies the breach is the one who reports it internally. As the coordinator, we need to complete the additional steps for documenting and reporting externally regardless.

Investigate Root-Cause

a) What happened (i.e. date, time, location, etc.)?
b) Cause and extent of the Safety Event or Privacy Breach
c) Did the Safety Event or Privacy Breach put anyone's safety at risk?

**If applicable, reach out to those involved for further clarification of the Safety Event.

What do I do when I identify a Safety Event or Privacy Breach?

Inform your manager & supervisor

- For moderate, severe, or critical privacy incidents, also notify the Privacy Office **at your Institution** (always CC your manager + supervisor when corresponding with Privacy Office).

Once all the information has been gathered, then we can proceed with reporting.

4.1. Identification of a Privacy Incident

The conduct of clinical research and the collection of data for these purposes include the use of PHI. All PHI collected for research purposes must be approved by the Research Ethics Board (REB). On the rare occasion that PHI is inappropriately collected, used or disclosed, it is considered to be a privacy incident. All privacy incidents must be reported to the Privacy Office (PO) via the UHN Incident Reporting & Review eForm. Privacy training is mandatory for all clinical research personnel.

Upon learning of a privacy incident, immediate action must be taken. Many of the following steps need to be carried out simultaneously, or in quick succession. At minimum, the following parties need to be informed:

- Department Manager(s)
- PO
- REB
  Note: when reporting to UHN REB within CAPCR, the question “Are you required by the study sponsor, lead site, or REB to report this event?” should be answered ‘Yes’.

Depending on the nature or seriousness of the privacy incident, additional parties may require notification (e.g. the patient). The PO determines which additional parties require notification. The PO also provides guidance around determining the severity of the incident as well as how to address the containment, remediation, notification, and escalation.

What do I do when I identify a Safety Event or Privacy Breach?

- Escalate as appropriate and in accordance with SOPs
- Develop a plan with management/ PI
- Start basic corrective actions within 24 hours
- Document all actions and keep records

What do I do when I identify a Safety Event or Privacy Breach?

Notify the team members involved (including participant-facing coordinator, department manager, nursing manager, MRP and the PI).

If applicable: Follow up with the investigator and/or participant-facing coordinator to ensure patient was notified of the safety event.

Only send participant notifications in an event of a privacy breach if:

1) Privacy Office has recommended notification
2) Content and method of notification has been vetted by the Privacy Office

What do I do when I identify a Safety Event or Privacy Breach?

Submit the incident report using the UHN Incident Reporting & Review eForm

- NOTE: Per SOP SC325 The staff member who is most involved with, discovers, or is informed of the safety event completes the Incident Report eForm.
- Be as detailed as possible with the description of the safety event. Please make sure to include the following:
  - How/when it was identified
  - How/when it was resolved
  - Dates/method of PHI destruction
  - Include a CAPA (be detailed with steps)
  - Follow up with study staff as necessary to ensure all necessary documentation is in place
  - Retraining (document date and who)
- **Have the Clinical Research manager review the description prior to submission.**
- **Online UHN Safety Event reporting is not the same or equivalent to REB reporting.**

Tips for Mitigating Privacy Breaches

- Knowing what PHI is approved by the REB
- Reviewing CRFs and source documents for PHI content prior to submitting to external parties (e.g. Sponsor)
- Refraining from forwarding internal email communications about study participants to the sponsor
  - If communication is needed, best practice is to start a new email chain with the sponsor instead of looping them into an existing communication chain
  - PHI should not be included in the subject line of emails, but can be included within the body of the email when communication is internal
- Verifying that the recipient's contact information is correct prior to sending documentation to external parties
- Keeping all PHI on UHN premises and ensuring that confidential waste bins are used when disposing of documents containing PHI
- Always taking a moment to double check your work

Other Resources

- CCRU SOP SC325 Identification and Reporting of Incidents Related to Research
- CCRU SOP SC321 Protocol Amendments and Deviations
- UHN Policy 3.20.005 Clinical: Patient Safety Event Reporting & Review
- UHN Policy 1.40.007 Administrative: Privacy & Access
- Privacy Office
  - Privacy Breach Patient Notification Guidelines
- UHN REB Guidelines
- OCREB Guidelines

Thank you

Jasmine Grant

CCRU Education

ccrueducation@uhn.ca

CAN TAP TALENT