University Health Network
Policy & Procedure Manual
Administrative: Privacy & Access

1. Policy

University Health Network (UHN) is committed to prioritizing the needs of patients. UHN recognizes the right to privacy as a principle of respect for patient autonomy, based on the individual's right to control information related to their healthcare.

Patient privacy and a patient's right to access their health records are protected by law under the Personal Health Information Protection Act (PHIPA).

The privacy of visitors to UHN, including patient family members and caregivers, is protected by the Freedom of Information and Protection of Privacy Act (FIPPA). FIPPA also provides members of the general public with the right to request access to copies of UHN's corporate records. For UHN revenue-generating initiatives, customer privacy is protected by the Personal Information Protection and Electronic Documents Act (PIPEDA) and Canada's Anti-Spam Legislation (CASL).

UHN's commitment to privacy and access to information, as set out in these statutes, requires all of its agents to comply with this policy and related policies concerning information.

This policy applies to UHN as a health information custodian, its agents (including employees, physicians, contractors, consultants, volunteers, learners, and other workers at UHN, including all personnel affiliated with third parties), and to all programs, procedures, and technologies at UHN that involve personal health information (PHI) and personal information (PI).

1.1 Patient Privacy Rights

UHN makes specific information about its policies and practices relating to the management of patient privacy readily available to individuals. (See Privacy at University Health Network patient education brochure (form D-5053) for more information.)

UHN will provide patients with information about:

- why PHI is collected
- how it is used
- with whom it may be shared and why
- patient rights with respect to the PHI

1.2 Rules for the Use and Disclosure of PHI for the Purpose of Providing Patient Care

1.2.1 Patient Requests for Access to Records

Patients may access some of their PHI collected for clinical care electronically using the UHN patient portal, myUHN. Through myUHN, patients can access upcoming and past appointments, as well as completed results, notes, reports, and other records.

Patients may also contact UHN Health Record Services (HRS) from myUHN or via email at HealthRecordServices@uhn.ca to request access to, or copies of, their clinical records of PHI.

Patients requesting copies of their records for themselves or for third parties (such as lawyers or insurance companies) should complete the Authorization for Disclosure of Personal Health Information form (form 2323) or other equivalent written request which may include documentation by a care provider in the health record. (Form 2323 is available on the myUHN portal and the UHN website.)

Refer to Patient Access to the Medical Record policy 1.40.003 for more information about patients' rights to access their records of PHI, including the right to access their original records and/or their chart during an inpatient admission.

1.2.2 Accuracy of Records

Patients may contact HRS to challenge the accuracy and completeness of their information as contained within their medical record, and to request a correction. If a challenge/correction request is not resolved to the satisfaction of the patient, they have the right to appeal UHN's decision to the Information and Privacy Commissioner of Ontario (IPC), and/or to submit a statement of disagreement, which UHN will store in the patient's medical record.

HRS may send corrected information or the statement of disagreement, at the request of the individual, to the persons to whom UHN has disclosed the information with respect to which the individual requested the correction of the record, except if the correction cannot reasonably be expected to have an effect on the ongoing provision of healthcare or other benefits to the individual.

Refer to Patient Requests for Correction to Medical Record policy 1.40.010 for more information.

1.2.3 Patient-Requested Audits

Patients may contact UHN Privacy to request an audit log of accesses to their electronic medical record. (Refer to the Audit Request Form.)

1.2.4 Consent Directive/Lockbox

Patients may withdraw their consent to the collection, use, and disclosure of their PHI for the purpose of providing healthcare to them. This is commonly referred to as a "lockbox".

Clinicians must request consent to override a lockbox for the purpose of providing care, either from the patient or the substitute decision maker (SDM) for the patient. The clinical user may override the lockbox citing an emergency only when:

- it is not reasonably possible to obtain this consent, **and**
- the risk of not accessing the locked information may lead to serious harm.

Other staff who require access for purposes such as billing, coding, scheduling, etc. do not require express consent and may override the lock in the health information system (HIS) by selecting the reason "Support Functions."

Lockbox requests from patients are generally submitted using a Lockbox (Consent Directive) Request Form and by contacting the Privacy Office at 416-340-4800 ext. 6937 or by email at privacy@uhn.ca.

1.2.5 Information and Privacy Commissioner

Patient privacy concerns should be escalated to UHN's Privacy Office. In situations where UHN Privacy is unable to resolve a concern, patients will be advised that they may contact the IPC by email at info@ipc.on.ca or by phone at 416-326-3333.

1.2.6 Freedom of Information

As part of the broader public sector, all Ontario hospitals are subject to FIPPA. FIPPA provides a public right of access (with limited exceptions) to records in the custody or control of UHN. FIPPA applies to PI, but does not apply to records of PHI.

All FIPPA requests must be submitted in writing to the UHN FIPPA Coordinator's Office. Requestors may be referred to UHN's Freedom of Information website or to email at FOI@uhn.ca to obtain further information.

1.2.7 Cooperation with the UHN Privacy Office

All UHN agents are required to cooperate with Privacy Office staff during a complaint, breach investigation, containment or remediation of a privacy issue, a privacy impact assessment, or an audit. Failure to cooperate with Privacy Office staff in their attempts to ensure or support compliance with UHN policy or provincial privacy laws may result in disciplinary measures.

1.2.8 Consent

UHN collects, uses, and discloses PHI with the consent of the patient or their SDM, or as is otherwise permitted or required by PHIPA and the Public Hospitals Act (PHA).

Where consent of an individual is required, the consent must:

- be of the individual
- be related to the information
- not be obtained through deception or coercion

The individual must be informed:

- of the purpose of the collection, use or disclosure of the information, **and**
- that consent may be provided or withheld.

1.2.9 Express and Implied Consent

UHN may rely on express or implied consent when collecting, using, or disclosing PHI for the purpose of providing patient care. PHI may be used and disclosed with assumed implied consent to healthcare professionals within a patient's **circle of care**, which includes, but is not limited to, doctors, nurses, pharmacists, allied health professionals, administrative staff supporting the provision of care, other employees assigned to care for a patient, and learners.

A patient's **express consent** is required for a patient's PHI to be disclosed:

- to a person that is not a health information custodian (HIC); **or**,
- for a purpose other than providing healthcare or assisting in healthcare.

Refer to Release of Patient Information policy1.40.002 for further information on:

- how to obtain a patient's express consent for the disclosure of their PHI for a non-healthcare purpose
- circumstances where disclosure for non-healthcare purpose may occur without consent

Refer to Consent for the Collection, Use & Disclosure of Personal Health Information for more information about when a patient's express consent is required, when implied consent may be sufficient, and when PHI may be used or disclosed without patient consent.

1.2.10 Obtain Consent from the Capable Patient

When consent is required for the collection, use, or disclosure of an individual's PHI, the consent must be obtained from the patient when the patient is capable of consenting to the collection, use, or disclosure.

An individual is capable of consenting to the collection, use, or disclosure of PHI if the individual is able to:

- understand the information relevant to deciding whether to consent to the collection, use, or disclosure of PHI, **and**
- appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent.

Where the individual is not capable of consenting to the collection, use, or disclosure of PHI, consent must be obtained from the patient's SDM.

1.2.11 Privacy Reviews, Privacy Impact Assessments & Threat-Risk Assessments

All new programs and projects at UHN that impact how PHI/PI/corporate confidential information (CCI)/anonymized information is handled or stored require review by the UHN Privacy Office. UHN Privacy and Digital Security will assess projects to ensure that appropriate physical, administrative, and technical safeguards are in place. This requirement does not apply to research projects. For research, refer to section 1.3.4 Research.

The project owner must submit a Privacy Intake Form for Projects to UHN Privacy.

UHN Privacy may conduct a privacy impact assessment (PIA) to assess the impact that the new system, technology, or program may have on an individual's privacy and the confidentiality of their PHI/PI, and to ensure that proper information governance is in place. (Refer to Privacy Support for Projects for more information.)

Where projects involve a new technology or change in technology, a threat-risk assessment by UHN Digital Security is also required.

1.2.12 Security of Systems and PHI/PI

UHN protects PHI/PI through appropriate physical, administrative, and technical safeguards. The safeguards are consistent with industry best practices to protect PHI/PI while being transferred, processed, or stored. These safeguards include security software and encryption protocols, firewalls, locks and other access controls, privacy impact assessments, threat-risk assessments, staff training, and confidentiality agreements.

The Privacy Office and Digital Security monitor the security of PHI/PI by conducting audits of clinical systems and business units.

1.2.13 Appropriate Use of Information Technology at UHN

All UHN agents must be aware of their obligations under, and abide by, Appropriate Use of Information & Information Technology policy 1.40.012, which requires UHN agents to

use only UHN-approved information technology (IT) resources to conduct UHN business.

All forms of technology involving PHI/PI at UHN must be used in a manner consistent with this policy and Appropriate Use of Information & Information Technology policy 1.40.012, including technologies not explicitly mentioned in these policies.

For more information about the appropriate use of IT at UHN, staff can contact UHN Digital at ext. 4357.

1.2.14 Vendor and External Party Access to UHN PHI/PI

All vendors, contractors, consultants, or other external parties who require access to UHN IT and/or UHN PHI/PI must enter into a signed written agreement with UHN, reviewed by Corporate Legal Affairs, that includes:

- UHN Confidentiality Agreement
- UHN Information Practices Agreement, available from the Privacy Office
- requirement for vendors, contractors, or consultants to complete UHN Privacy and Cyber Security eLearning or equivalent training approved by the UHN Privacy Office

(For further information, refer to Vendor & Related Party Access policy 1.40.018, Procurement policy 1.90.012, and Appropriate Use of Information & Information Technology policy 1.40.012.)

1.2.15 Retention, Archiving and Destruction of PHI/PI

UHN has established information retention guidelines that define consistent minimum standards and requirements for the length of time records of PHI/PI are to be maintained. (Refer to Management, Retention & Destruction of UHN Records policy 1.30.007.)

UHN has established appropriate practices and timelines for the secure disposal of PHI/PI, consistent with confidentiality, legal, and regulatory requirements. (Refer to Management, Retention & Destruction of UHN Records policy 1.30.007.)

Researchers are responsible for the storage/retention of research data, as defined in their approved research protocol. (Refer to Data Ownership, Stewardship & Security of Health Information policy 40.50.004 and Management, Retention & Destruction of UHN Records policy 1.30.007.)

1.3 Rules for the Use and Disclosure of Patient Data for Purposes Other Than for Care (Research, Quality Improvement, Education)

PHI or anonymized data that is sent from or received by UHN for research, quality improvement, or educational purposes must be handled in compliance with UHN policies. Any necessary consents and/or internal approvals must be obtained prior to use or transfer. Also refer to Data Access, Sharing, and Use policy 1.130.002 for guidance on the principles and rules that ensure data is available to support organizational strategy and operations.

1.3.1 Limiting PHI and the UHN De-identification and Anonymized Data Standard

UHN and its agents must only collect, use, disclose, and retain the minimum amount of PHI required to achieve the research, quality improvement, or education purpose.

De-identified information should be used instead of PHI whenever it is feasible to do so.

The **UHN De-identification and Anonymized Data Standard** ("Standard") provides guidance to UHN agents using personal health information for a purpose other than to provide care (i.e. research, quality improvement) with respect to how to modify patient data, images, or recordings in order for the data to be sufficiently de-identified and no longer considered PHI.

Data, images, or recordings that do not conform to this Standard may be considered PHI.

When UHN agents are not able to anonymize information to meet the Standard, the Privacy Office must be consulted for advice and recommendations on risk mitigation.

1.3.2 Use of Anonymized Information

Anonymized information (including data, images, and recordings) is considered a UHN corporate resource. Any use or transfer outside of UHN of anonymized information must comply with UHN policies. Any necessary approvals must be obtained prior to use or transfer.

Anonymized patient/participant information may be used for UHN-supported purposes (including patient care, research, quality improvement, or education) provided it is used in a manner that:

- does not jeopardize the safety or well-being of patients/participants and the UHN community
- does not reflect poorly on UHN
- is consistent with UHN's stated values
- does not expose UHN to unacceptable ethical, reputational, legal, regulatory or technical risks

When publishing, sharing, or presenting anonymized information:

- Do not add information that would cause the data or images to become identifiable, or unnecessarily increase the risk of re-identification.
- Ensure that descriptions and commentary related to anonymized information are professional in both tone and content.
- Follow UHN's Data Ownership, Stewardship & Security of Health Information policy 40.50.004 and Social Media Guidelines.

1.3.3 External Data Sharing of PHI and/or Anonymized Information for Research, Quality Improvement and/or Education

When sharing data outside of UHN for research, quality improvement, or education:

- Always consult with UHN Legal to determine whether a data sharing agreement is required for the data sharing initiative.
- Always consult with Privacy where rare images or data are at play.
- When sharing PHI, consult with UHN Privacy and Digital Security to determine whether a privacy impact assessment and/or threat risk assessment is required.

  Note: Where sharing PHI further to a Research Ethics Board (REB)-approved study, consultation with Privacy and Digital Security is not required.

- When the project involves technology, consult with Privacy and Digital Security.

  Note: For research projects, consultation with Privacy and Digital Security is required only for UHN-investigator initiated studies. Consultation is not required for industry sponsored studies.

Exceptions: Regulatory reporting, OHIP billing, case conferences.

1.3.4 Research

Research project proposals involving the collection, use, or disclosure of PHI, anonymized or any other UHN data must be reviewed and approved by the UHN REB or an authorized external Board of Record (BOR). The REB or BOR will address consent requirements for the use of PHI. (Refer to Requirements for Informed Consent Process policy 40.20.011.)

All data arising from research projects must conform to Data Ownership, Stewardship & Security of Health Information policy 40.50.004 and section 1.3.12 Information Governance for Storage of PHI at UHN Outside of the Health Information System of this policy, including the requirements for access controls, auditing, and secure storage.

1.3.5 Quality Improvement Project Proposals

Quality improvement (QI) projects must:

- be submitted to the UHN Quality Improvement Review Committee (QI@uhn.ca) for review and institutional approval prior to proceeding, **and**
- have approval by the appropriate manager/director/executive sponsor, depending on the scope of the project.

For more information on which projects must be submitted, refer to the Privacy and Security Intake Form.

1.3.6 Consent and QI Projects with External Data Sharing

Except where the patient's express consent has been obtained for such disclosure, PHIPA does not permit the disclosure of PHI to external parties (nor in publications) in relation to QI projects. (For example, the transfer of UHN PHI to a multi-site QI project without patient consent is not permitted.)

1.3.7 Education

PHI may be used without consent for the purposes of educating UHN agents. For internal UHN use, a supervising clinician, department head, or manager must approve the use of PHI for educational purposes where the trainee/agent is not in the patient's circle of care. Where training agents outside of the circle of care, PHI should be anonymized to the greatest extent possible to achieve the purpose.

If collecting and storing patient data outside of the HIS for educational purposes (i.e. in a registry), refer to the Data Access, Sharing, and Use policy 1.130.002.

The sharing of anonymized information for external educational purposes requires approval by an executive sponsor (defined as a vice-president (VP) or executive vice-president (EVP) or appropriate delegate/signatory authorizing the educational initiative).

Exceptions: Where UHN staff share case studies at a conference or share anonymized medical images through social media for educational purposes in accordance with Use of Medical Images in Education, VP/EVP approval is not required as long as the data is fully anonymized and/or patient consent has been obtained and documented.

(Also refer to External Observers and Authorized Guests in Clinical Areas policy 1.40.019 and Remote Observation of Surgical Procedures policy 37.30.001.)

1.3.8 Consent and External PHI Sharing for Educational Purposes

Except where the patient's express consent has been obtained, PHIPA does not permit the disclosure of PHI to external parties for educational purposes. See section 1.3.3 External Data Sharing of PHI and/or Anonymized Information for Research, Quality Improvement and/or Education.

(Also refer to External Observers and Authorized Guests in Clinical Areas policy 1.40.019 and Remote Observation of Surgical Procedures policy 37.30.001.)

1.3.9 External Observers in Clinical Areas

To foster excellence in patient care and academics, select individuals who are not part of a patient's internal care team may observe examinations, procedures, and other activities for educational purposes. Such observerships must comply with the requirements set out in External Observers and Authorized Guests in Clinical Areas policy 1.40.019.

Vendors who require access to clinical areas for patient care or training duties must comply with Vendors in Clinical Areas policy 1.40.025.

1.3.10 Registries

When collecting and storing patient data in internal registries or sharing patient data with registries external to UHN, refer to Data Access, Sharing, and Use policy 1.130.002.

1.3.11 Exceptions

Exceptions to the rules governing the use and sharing of anonymized data set out in this policy must be approved by the Chief Legal Officer.

1.3.12 Information Governance for Storage of PHI at UHN Outside of the Health Information System

The project owner must submit any project involving the storage of PHI outside of the health information system for research, quality improvement, education, or care purposes to UHN Privacy and UHN Digital Security for review and to ensure that the following standards are met:

- access to records is given only to those with a professional need to know
- the records are protected from corruption or loss
- an audit trail is created when records are accessed or released, and audit logs are retained
- records are available in a timely and efficient manner
- records are stored, retained and disposed of in accordance with Management, Retention & Destruction of UHN Records policy 1.30.007 and Appropriate Use of Information & Information Technology policy 1.40.012
- agents are properly trained, including UHN's mandatory annual Privacy and Cybersecurity eLearning, and adhere to the policies and procedures developed for the management of records that they handle in the course of their duties

1.4 Privacy Operations Services

1.4.1 Privacy Incidents

UHN agents must report privacy incidents, including instances when an agent knows, or has reason to believe, that PHI was collected, used, or disclosed without proper authorization and when PHI is lost or stolen. A UHN agent must also report situations that present a risk to patient privacy.

UHN agents must report incidents involving the unauthorized collection, use, or disclosure of PI and notify affected individuals where it is reasonable in the circumstances to believe that there is a real risk of significant harm (RROSH).

Both the report form and instructions for completing the form can be found on the UHN Safety Event Reporting & Review web portal. Privacy incidents are investigated and managed in accordance with Patient Safety Event Reporting & Review policy 3.20.005.

UHN relies on agents to participate in the review of privacy incidents in order to determine the extent of a breach, to mitigate its impact, and to prevent or reduce the recurrence of similar incidents. Early reporting of privacy incidents can result in mitigation strategies that reduce the extent of the breach and its consequences. (Refer to the Incident Management section of the Privacy Office website for more information.)

When privacy incidents occur, UHN Privacy will assist agents to:

- identify the scope of the breach and take steps for containment;
- notify the individuals affected by the breach, as soon as reasonably possible, and include certain required information in the notice, including a statement that the individual is entitled to make a complaint to the IPC; **and**
- notify any staff (and other custodians, as appropriate) who need to be advised of the breach.

Where required by PHIPA, UHN Privacy will notify the IPC and/or the regulatory colleges as appropriate.

1.4.2 Department and System Audits

The Privacy Office conducts audits of information systems used to collect, use, document, and disclose PHI for the purpose of detecting and deterring unauthorized activity. Site visits are also conducted on request or as part of a review or investigation.

1.4.3 Accessing Records of PHI

UHN agents may only access records of PHI as needed for the purposes of their UHN-authorized role. Any other access is considered a privacy breach and may be reportable to the Information and Privacy Commissioner of Ontario and incur discipline as described in Sanctions for Breaches of Personal Health Information policy 2.50.008.

UHN agents must not directly view their own health records in UHN's electronic systems. These systems are only to be used for work-related purposes. As is the case with any other patient, UHN agents may access their PHI using the myUHN Patient Portal or by contacting Health Records.

UHN agents may not access the records of family members, neighbours, or friends, even with their consent, except for work-related purposes.

1.4.4 Email

Refer to Consent for Use of Email policy 1.40.014, Appropriate Use of Information & Information Technology policy 1.40.012, and Information Security policy 1.40.028 for complete details on the acceptable usage of email and best practices.

1.4.5 Use of Shared Systems for Patient Care Only

Shared systems enable healthcare providers to centrally access PHI from healthcare facilities across Ontario. Examples of shared systems are:

- ConnectingOntario
- OLIS (laboratory test orders and results)
- DHDR (dispensed drug history)
- Care Everywhere

Shared systems may **only** be used for patient care. This is a standard provision in the terms of use for each system. Shared systems **may not** be used for research, training, quality improvement, or educational purposes. These systems are audited and subsequently investigated. Confirmed misuse can result in user access suspension/ termination.

1.4.6 Training and Awareness

UHN makes its agents aware of the importance of maintaining the confidentiality of personal health information.

All UHN agents must sign a Confidentiality Agreement (form D-3236) or online through UHN's mandatory privacy and security training module, and complete UHN privacy training at the onset of their association with UHN and annually thereafter.

Ongoing educational efforts will be delivered by UHN Privacy to ensure all UHN agents are provided with tools, training, and support, as appropriate, to assist them in fulfilling their duties as it relates to the privacy of PHI.

1.4.7 Ministry of Health, Government Agencies & Government-Funded Agencies

The law permits UHN to disclose PHI to organizations such as the Ministry of Health, Ontario Health, Public Health Ontario, Canadian Institute for Health Information, Institute

for Clinical Evaluative Sciences (ICES), and other similar organizations for the planning and management of the health system.

An agreement must be in place between UHN and the organization before any PHI is disclosed to the organization. If an agreement is not in place, UHN Legal must be contacted and will assist in developing an agreement.

1.4.8 PHI from Outside Organizations

Whenever an agent of UHN is provided with records of PHI from an outside organization for the purpose of the provision of care (such as a hospital, researcher, or government agency), UHN policies and procedures governing the handling and retention of PHI must be followed with respect to the external records. These records become part of the patient chart.

1.4.9 Enforcement and Sanctions

UHN applies progressive discipline in dealing with privacy breaches; however, any breaches of this policy, including, but not limited to, repeated or intentional breaches and breaches of related privacy policies may result in suspension or termination, and reporting to the relevant regulatory college and the Information and Privacy Commissioner of Ontario as outlined in Sanctions for Breaches of Personal Health Information policy 2.50.008 and the UHN Confidentiality Agreement (form D-3236).

Collection, use, or disclosure of PHI in contravention of PHIPA may result in fines of up to $200,000 for individuals and up to $1,000,000 for UHN upon conviction. UHN will not normally cover or insure individuals for fines resulting from the collection, use or disclosure of PHI in contravention of PHIPA and this policy.

1.4.10 Employee Privacy

UHN is committed to protecting the privacy of its employees. Employee personal information will only be collected, used, and disclosed as per Personal Information Protection policy 2.10.013. Employees who have requests or concerns regarding their UHN employee records should contact People & Culture. UHN may electronically monitor employees' online activities as described in Electronic Monitoring policy 1.40.004.

1.4.11 Policy Review

This policy will be reviewed at least once every two years and as issues arise, including amendments to legislation or new guidance from the IPC. The Privacy Office will be responsible for ensuring that any relevant changes to this policy are communicated to UHN agents, patients, and visitors.

1.5 Related Documents

- Code of Workplace Ethics
- Confidentiality Agreement (form D-3236)
- Consent for the Collection, Use & Disclosure of Personal Health Information
- Data Ownership, Stewardship & Security of Health Information policy 40.50.004
- Data Quality policy 1.40.016
- Patient Safety Event Reporting & Review policy 3.20.005
- Appropriate Use of Information & Information Technology policy 1.40.012
- Patient Access to the Medical Record policy 1.40.003
- Patient Requests for Correction to Medical Record policy 1.40.010
- Personal Information Protection policy 2.10.013
- Release of Patient Information policy 1.40.002
- Sanctions for Breaches of Personal Health Information policy 2.50.008
- Management, Retention & Destruction of UHN Records policy 1.30.007
- Vendors in Clinical Areas policy 1.40.025
- Vendor & Related Party Access policy 1.40.018.
- Electronic Monitoring policy 1.40.004

2. Definitions

Note: All defined terms appear in this policy. The first instance of each term in each section of this policy is hyperlinked to its definition; however, every instance of a defined term has the same definition.

Agent: A person that, with the authorization of UHN, acts for or on behalf of the organization in respect of PHI for the purposes of UHN, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by UHN, and whether or not the agent is being remunerated. Examples of agents of UHN include, but are not limited to: employees, volunteers, learners, physicians, residents, fellows, consultants, researchers, vendors.

Anonymized information: Information for which it is not reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual and is anonymized in accordance with UHN De-identification and Anonymized Data Standard. Includes data, images, and recordings. Anonymized data is different from coded data.

Coded data: Data that has certain direct identifiers removed but which does not meet the standard of anonymized; it is still considered personal health information.

Collect personal health information: To gather, acquire, receive, or obtain the information by any means from any source.

Confidential information: Confidential information maintained at UHN falls under the following three categories:

- **Corporate confidential information (CCI):** Information maintained by UHN that is not routinely made publicly available, including financial, administrative, commercial, and technical information, and may also include records containing legal advice and employee-related information. These records may be subject to FIPPA.

- **Personal health information (PHI):** Any identifying information about an individual relating to the individual's health or to the provision of healthcare to the individual. For example, an individual's health insurance number and/or medical record number would be considered personal health information, subject to PHIPA.

- **Personal information (PI):** Information about an identifiable individual not related to the individual's health or to the provision of healthcare to the individual. Examples include an individual's age, religion, address, and telephone number. Records that contain PI are subject to FIPPA.

Disclose personal health information: To make PHI available or to release it to another health information custodian or to another person outside of UHN.

Health information custodian (HIC): Persons or organizations under PHIPA, such as hospitals, who have custody or control of PHI as a result of the work they do. As a public hospital, UHN is a health information custodian (as per Personal Health Information Protection Act, 2004, Schedule A, Explanatory Note).

Information and Privacy Commissioner of Ontario (IPC): The IPC oversees compliance by public institutions and healthcare providers with provincial access and privacy laws. In performing this role, the IPC will resolve appeals when access to information is refused, investigate privacy complaints related to PI/PHI, review privacy policies and information management practices, conduct research on access and privacy issues, and educate the public.

Personal health information: See confidential information.

Project owner: The UHN manager, director, principal investigator, project manager, or staff member who has been delegated the authority from a department to initiate or oversee a project or research study.

Record of personal health information: PHIPA defines a record as PHI in any form or in any medium, whether it be in written, oral, printed, photographic or electronic form, or otherwise. This includes emails and video recordings.

Substitute decision maker (SDM): If an individual is determined to be incapable of consenting to the collection, use, or disclosure of PHI by a health information custodian,

a person described in one of the following paragraphs may, on the individual's behalf and in the place of the individual, give, withhold, or withdraw the consent:

- The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual.
- The individual's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual.
- The individual's representative appointed by the Consent and Capacity Board if the representative has authority to give the consent.
- The individual's spouse or partner.
- A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent. This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent.
- A parent of the individual with only a right of access to the individual.
- A brother or sister of the individual.
- Any other relative of the individual.

Use personal health information: To view, handle, or otherwise deal with the information within UHN or among UHN agents only. Use does not include disclosure of the information outside of UHN.