UNITY HEALTH TORONTO

Caring hearts. Leading minds.

Title:	**Privacy of Personal Health Information**		
Document Type:	Policy	Document #:	UHT0001531
Program:	Information Access and Privacy	Effective Date:	May 26, 2021
Executive Sponsor:	Vice President, Quality, Performance, Info Management & CIO	Last Reviewed:	March 2021
Owner/Lead:	Senior Director Enterprise Risk, Emergency Preparedness & Chief Privacy Officer	Last Revised:	March 2021
Approval Body:	Executive Committee	Review Cycle:	3 year
Applicable Sites:	☒ **Unity Health** ☐ **Providence** ☐ **St. Joseph's** ☐ **St. Michael's**		

1.0 PURPOSE

Unity Health Toronto ("**Unity Health**") is committed to protecting the privacy of the **personal health information ("PHI")** that we collect or create about patients, clients and residents (referred to as "**patients**" below) when providing care, conducting research, or performing other hospital operations.

Unity Health is a **health information custodian ("HIC")**, as defined under the ***Personal Health Information Protection Act, 2004*** **("PHIPA")**. This policy describes how PHI collected or created by Unity Health is handled in accordance with PHIPA and the 10 core principles of privacy set by the Canadian Standards Association. Related policies and procedures are listed in **Appendix A**; compliance with this policy requires compliance with the policies and procedures listed.

Unity Health is also responsible for PHI entrusted to us by other HICs in the course of providing service to them, to support care provision to their patients. This policy describes how Unity Health will maintain the privacy of that PHI.

Information related to the handling of **personal information ("PI")** is described in the *Privacy of Personal Information policy.* PI includes, but is not limited to:

- identifiable information about people who are users or consumers of a service, but are not identified as Unity Health patients (e.g. people who visit our public website, people who pay for parking, people who shop in our gift shops); and
- identifiable information about staff, medical staff and affiliates (e.g. employee or volunteer information, credentialing information, or information about contractors).

This policy applies to all medical staff, staff, students, volunteers, patient partners, researchers, vendors, and third party service providers, and any other individual or entity who handles PHI on behalf of Unity Health, or who comes into contact with PHI in the course of their duties (referred to as "**Agents**" below).

2.0 POLICY FOR UNITY HEALTH PHI

Unity Health handles all PHI that we collect or create about the patients we serve in accordance with PHIPA, direction from our privacy commissioner, and emerging best practice.

A. Consent for the Collection, Use and Disclosure of Personal Health Information

- **Consent Required:** Unity Health requires the consent of the patient to collect, use, or disclose PHI, unless otherwise permitted by law.

- **Capacity to Consent:** Consent must be voluntary, knowledgeable, and relate to the information in question. For consent to be valid, the patient must have capacity to consent. If a patient does not have capacity, consent must be obtained from the patient's substitute decision-maker, as defined under PHIPA.

- **Authority to Rely on Implied Consent:** PHI may be used within Unity Health, or disclosed (released) to the patient's other health care providers, for health care (within the "circle of care"), without express written or verbal consent, as long as Unity Health has reason to believe that the patient wants the PHI to be seen and shared with their health care providers. A patient's request for treatment constitutes implied consent to use and disclose their PHI for care.

- **Authority to Use or Disclose without Consent:** In certain circumstances, Unity Health may collect, use or disclose PHI without express or implied consent). These activities are permitted or required by law and include:

    - Planning and managing our programs and services
    - Getting paid or providing payment
    - Conducting activities that increase the quality of care we provide or reduce errors or risks
    - Supporting the planning and management of the health care system
    - Conducting research (with approval from a Research Ethics Board)
    - Educating our Agents
    - Compiling statistics
    - Responding to legal proceedings

- **Requirement to Obtain Express Consent:** Express written or verbal consent must be obtained from a patient where:

    a) a patient wishes to release any of their PHI to a third party that is not a health care provider,
    b) Essential Care Partner or caregiver requests PHI about a patient,
    c) Unity Health wishes to disclose PHI to a party not authorized under PHIPA to receive it without consent, or
    d) Unity Health wishes to collect new PHI for a purpose other than provision of health care or other than where PHIPA permits.

Examples include:

- ✓ third parties that are not health care providers such as lawyers, insurance companies, employers, and landlords
- ✓ collecting or disclosing PHI to patients' family members or chosen caregivers (unless the patient does not have capacity and the individual is the substitute decision-maker), or
- ✓ collecting new PHI for a purpose other than care, such as quality improvement (e.g. a survey collecting patients' experiences with a treatment, where the data will be analyzed but not used to provide immediate care to the survey respondents) or research (where the REB has not waived the requirement for consent).

- **Consent for Fundraising or Marketing**: Before using or disclosing PHI for fundraising, Unity Health will obtain express consent from patients, or will rely on implied consent, as long as patients have had a sufficient amount of time to withdraw their consent (60 days since their date of discharge) and the only information used or disclosed is the patient's name and mailing address. PHI will not be used for marketing without express consent from the patient.

- **Withholding or Withdrawal of Consent ("Lockbox"):** If express consent is sought, a patient may choose not to give consent. Similarly, a patient may choose to withdraw their implied consent for their PHI to be used or disclosed for care. Lastly, a patient may choose to withdraw their consent specifically for the use of their PHI for fundraising or to connect them with a spiritual advisor. PHIPA limits how much the use or disclosure of PHI can be restricted and these limits will be described to patients when they request a lockbox.

- **Documentation of Consent:** Where express consent is sought, Agents must document this in the patient's record. Where express or implied consent is withheld or withdrawn, this must also be documented in the patient's record.

B. Limiting Collection, Use and Disclosure of Personal Health Information

- **Limited Collection:** Unity Health must limit the amount and type of PHI collected to what is necessary to fulfill the intended purpose.

- **Sources of Collection:** PHI will be collected directly from the patient, unless the law permits or requires Unity Health to collect PHI from other sources (such as from Essential Care Partners or other family, friends, bystanders or others).

- **Prioritizing De-Identified Information**: Unity Health will not collect, use or disclose PHI if de-identified information will serve the purpose.

- **Limits on Agents:** Agents may not view, share, receive or otherwise handle PHI unless they have a legitimate "need to know" it, as part of their duties. If an Agent is in doubt whether they are allowed to handle PHI, the Agent should ask their supervisor.

- **Authority to Disclosure**: PHI must not be disclosed outside of Unity Health for reasons other than care, except with the consent of the patient, or as permitted or required by law.

C. Retention, Storage & Disposal of Personal Health Information

- **Retention:** Unity Health has established retention guidelines that define consistent minimum standards for the length of time PHI and records of PHI are to be maintained. PHI will be retained according to the network "Record Management & Retention" policy.

- **Storage:** PHI, and records of PHI in all forms, must be securely stored. Storage standards are dictated in the "Secure Handling of Confidential Information in Digital Format" policy.

- **Disposal:** PHI that is no longer required must be securely destroyed, erased, or de-identified safely and securely.

- **Research:** Researchers are responsible for the secure storage and destruction of research data, as defined in their approved research protocol.

D. Ensuring Accuracy of Personal Health Information

- **Requirement to Maintain Accuracy:** Unity Health will take reasonable steps to ensure that the PHI in our custody is as accurate, complete, and up-to-date as is necessary to minimize the possibility that inappropriate information may be used to make a care-related decision about a patient.

E. Safeguards for Personal Health Information

- **Safeguards:** Unity Health takes steps to ensure that PHI is protected against theft, loss and unauthorized use or disclosure. Unity Health also takes steps to ensure that the confidentiality, integrity, and availability of records of PHI is maintained. The nature of the safeguards will vary depending on the sensitivity and nature of the information, and include:
    - physical safeguards (such as locked filing cabinets and rooms),
    - administrative/organizational safeguards (such as permitting access to PHI only to Agents who "need-to-know"), and
    - technical safeguards (such as requiring passwords, encryption, and audits).

F. Patient Rights

- **Right to Access:** Patients may request to see and/or receive a copy of their PHI, regardless of the form in which the PHI is stored. Unity Health will respond to each request, within reasonable timelines and costs to the requestor, in accordance with PHIPA. Unity Health will take reasonable steps to ensure that the requested PHI is made available in a format that is understandable.

- **Unity Health Agents:** Agents of Unity Health may not access their own paper and/or electronic records outside of the standard release of information processes available to all patients and, by extension, may not directly view their own records in electronic systems using their user credentials.

- **Right to Correct:** Patients may request corrections to PHI that they feel is inaccurate or incomplete for the purpose it was collected or created. Unity Health will respond to each request, within reasonable timelines and to the extent required, as dictated by PHIPA. In some cases, instead of making a correction, patients may tell Unity Health to attach a statement of disagreement to their file.

- **Right to Challenge:** A patient or any other person may ask questions or challenge the compliance of Unity Health with PHIPA and/or Unity Health privacy policies. Unity Health will investigate all inquiries, complaints and challenges of compliance, and will respond to the patient, as appropriate.

G. Patient Notice

- **Content of Notice:** Unity Health will publicly make available the following information about our policies and practices about how PHI is handled, including:
    - the ways and reasons PHI is collected, used and disclosed,
    - the process for patients to view or request copies of their PHI,
    - the process for patients to request corrections to their PHI,
    - the process for patients to request lockboxes,
    - the process for patients to withdraw their consent for their PHI to be disclosed for fundraising or spiritual care,
    - descriptions of shared electronic systems through which PHI may be disclosed,
    - contact information for our Privacy Office, to whom complaints or inquiries can be made, and
    - a description of how a patient can make a complaint to the privacy commissioner.

- **Format of Notice:** Unity Health will determine the methods for providing the information listed above, while ensuring that the notices are as accessible as possible, given varying literacy, language, and/or formatting needs of patients and Essential Care Partners.

H. Privacy Breaches

- **Breach**: All confirmed or suspected **privacy breaches** must be reported immediately to the Privacy Office, which will execute the *Privacy Breach Management* policy.

- **Disciplinary Action**: Failure to comply with PHIPA, this policy, related policies and procedures of Unity Health, or privacy-related contractual obligations may result in disciplinary action, up to and including termination of employment, privilege, services and/or access to PHI. Discipline will depend on the nature and severity of the breach, as previously applied by Unity Health or expected by a privacy commissioner, and intentional actions or repeated negligence will result in stronger

discipline. Unity Health and its Agents may also be subject to the fines and penalties set out in PHIPA.

3.0 POLICY FOR PHI OF OTHER HICs

Unity Health is responsible for providing and maintaining certain shared electronic systems that allow two or more health information custodians to collect, disclose and use PHI to provide and support the provision of care. Unity Health is also responsible for providing various services to other HICs to support the management of the PHI that they collect or create about the patients that they serve.

The obligations of Unity Health as a service provider and as a **health information network provider (HINP)**, along with our procedures for handling PHI in the course of these activities, are defined under PHIPA and in agreements with participating HICs.

In particular, Unity Health will:

- Only use, disclose or otherwise handle the PHI as directed by the HIC
- Ensure that Agents handling the HIC's PHI are aware of, and agree to, their obligations with respect to handling it
- Notify the HIC if the PHI was handled in contravention of PHIPA or the HIC's direction

In addition to the above, when Unity Health is a HINP, we will:

- Provide the HIC with a plain language description of services, which will also be posted publicly
- Provide an audit of accesses or disclosures to the PHI in the shared system (upon request)
- Provide a summary of the privacy assessment (upon request)
- Provide a summary of the security assessment (upon request)
- Enter into a written agreement with the HICs

4.0 ENFORCEMENT

The Chief Privacy Officer, with the aid of the Privacy Office staff, will monitor adherence to this policy using a risk-based model, and report to the appropriate governance bodies. Any exceptions to this policy must be approved in advance by the Chief Privacy Officer and may require involvement of other groups.

5.0 ACCOUNTABILITY

To maintain compliance with PHIPA and all privacy-related policies:

- In addition to supporting all activities described above, the Privacy Office will:
    - implement and maintain an appropriate privacy strategy,
    - develop policies, procedures, controls and standards,
    - report and escalate risks to senior management / the board,
    - conduct audits,
    - monitor PHI-handling practices,
    - conduct routine assessments of new and modified work processes or systems,

- conduct assessments of operational compliance,
- log and support the creation of inventories that track systems which process PHI,
- provide education and awareness around the appropriate handling of PHI,
- work with IT Security to ensure that PHI is collected, viewed, disclosed, transmitted, stored, and disposed of securely, and
- assess, limit and monitor the activities of vendors and third parties who assist Unity Health in providing service.

- Agents will:
  - only collect, use, disclose, retain, dispose, or otherwise handle PHI as permitted or required by law, and only as directed by Unity Health,
  - report breaches to the Privacy Office,
  - identify and raise risks, and/or opportunities, to enhance, privacy compliance to the Privacy Office (e.g. enhancements to electronic patient records)
  - request a review of changes to existing systems/processes, and/or new plans to change the way PHI is handled, and
  - sign confidentiality agreements, including but not limited to the Unity Health Privacy and Confidentiality Agreement, end user agreements, and complete privacy education annually and/or as otherwise required by these.

- Vendors, Service Providers & Third Parties will:
  - adhere to this and all related policies, and
  - adhere to provisions in signed agreements, including but not limited to completing education as requested and reporting privacy breaches to Unity Health immediately.

6.0 DEFINITIONS

Term/Acronym	Definition
Health Information Custodian (HIC)	Refers to an entity, defined under the Personal Health Information Protection Act, 2004 (PHIPA), that is permitted or required under PHIPA to collect, use or disclose PHI related to the patients, clients or residents served by that HIC that is in the custody or control of the HIC. As a single legal entity, Unity Health Toronto is a single HIC for the purposes of PHIPA, though the activities of Unity Health Toronto are governed by multiple laws (e.g., Public Hospitals Act, Long-Term Care Homes Act, Home Care and Community Services Act).
Health Information Network Provider (HINP)	Refers to an entity, defined under the *Personal Health Information Protection Act*, 2004 (PHIPA), that provides and maintains an electronic system for two or more HICs to collect and disclose PHI in the other HIC's custody for the purpose of care (otherwise known as a '**shared system'**).
Personal health information (PHI)	Personal health information (PHI) is defined in the Personal Health Information Protection Act, 2004 and may be amended from time to time. PHI is any information that identifies a person and relates to their health or to the provision of care, treatment or assessment for that individual. PHI can exist in any form (oral, written, or electronic). Any information that is not explicitly

	related to health is also PHI, if it is contained in a record of PHI. Examples of PHI and records of PHI include: a paper record of treatment in a physician's office, an electronic record of all diagnostic tests performed on a patient, a faxed referral for a patient, an email discussing the Power of Attorney for a named client. PHI includes, but is not limited to: • Information relating to the physical or mental health of the individual, including the individual's medical history and the individual's family medical history; • Information relating to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual; • Information relating to the payment or eligibility for health care; • Information relating to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance; • The individual's health care number; or • Information that identifies an individual's substitute decision-maker.
Personal information (PI)	Information about an identifiable individual as it is defined in the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Personal Information Protection & Electronic Documents Act (PIPEDA),* or other applicable laws, which may be amended from time to time. PI is identifying information about an individual who is not a patient, client or resident, that is personal in nature (i.e. does not relate to an individual's business identity or work activities). PI relates to staff, third parties, or other affiliates, can exist in oral or recorded form, and includes, but is not limited to: • Information that relates to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or martial or family status of the individual; • Information that relates to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • Any identifying number, symbol or other particular assigned to the individual; • The address, telephone number, fingerprints or blood type of the individual; • The personal opinions or views of the individual except where they relate to another individual; • Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; • The views or opinions of another individual about the individual; and/or • The individual's name where it appears with other personal

	information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.
***Personal Health Information Protection Act*, 2004 (PHIPA)**	Ontario's privacy legislation that governs the manner in which PHI may be collected, used and disclosed within the health care system. It also regulates some individuals and organizations that receive PHI from health care providers.
Privacy breach	Any contravention of a rule under PHIPA, PIPEDA, FIPPA or other applicable privacy law. This includes a loss, theft or inappropriate access to PHI/PI that occurred through inappropriate collection, use, disclosure, retention, modification or destruction, whether or not the activity was intentional or inadvertent. This also includes any contravention of a Unity Health privacy-related policy or procedure, or an expectation set out by a privacy commissioner. Breaches also include a failure to protect PI or PHI with which an employee or agent is entrusted (e.g. leaving health records unattended, sharing passwords or discussing personal health information via social media). • A **confirmed breach** is an incident where a contravention has been established. • A **suspected breach** is an incident where a contravention has yet to be established. • A **near miss/good catch** is an incident that poses a risk to compliance and was caught before a breach (contravention) occurred.

7.0 REFERENCES

Personal Health Information Protection Act, 2004

Related Policies

- Health records
- Information Access and Privacy
- Information Technology
- Communications and Public Affairs

8.0 ATTACHMENTS/APPENDIX

Appendix A – Unity Health Privacy & Confidentiality Agreement

Version	Approval/Sub-approval body	Approval date
01	Executive Committee	May 5, 2021