Corporate Policy

Privacy

Policy Purpose:

The Ottawa Hospital ("TOH") protects the privacy of Individuals who entrust us with their personal information ("PI") or personal health information ("PHI"). This policy sets out our privacy-related rules for collecting, using, disclosing, and retaining PI or PHI.

Scope:

This policy applies to all people handling PI or PHI about Individuals on TOH's behalf and at any TOH site. It does not relate to information about a person in their professional capacity (e.g., business contact information for one of our staff members).

Definitions:

Agent: Any person working on behalf of TOH regardless of whether they are paid by TOH (e.g., staff, physicians, volunteers).

Collect: When TOH or anyone working on TOH's behalf receives PI or PHI directly from an Individual or third-party.

Consent: An Individual giving permission to collect, use, or disclose their PI or PHI.

Consent Directive: An Individual limiting how TOH collects, uses, or discloses their PI or PHI (also known as a 'break-the-glass').

Custodian: An organization that has the legal right to make decisions about PI or PHI and who is required to protect it. This includes the definition of a Health Information Custodian (HIC) under PHIPA and Institution under FIPPA. For the purposes of this policy TOH is the Custodian.

Disclose: When TOH or anyone working on TOH's behalf gives PI or PHI (including verbally) to someone outside TOH.

Health care: Any observation, examination, assessment, care, service, or procedure that is health-related.

Health Information Custodian (HIC): An organization defined in PHIPA that has the legal right to make decisions about PHI and who is required to protect it.

Individual: The person to whom the PI or PHI relates and includes their substitute decision maker (SDM) where relevant.

Institution: An organization defined in FIPPA that has the legal right to make decisions about PI and who is required to protect it.

Just Culture: A framework used to ensure consistency in how breaches of duty are addressed in a supportive, just and ethical environment. The Just Culture supports honest reporting of breaches of duty with the goal of continuous improvement in the organization.

Patient: A person who receives care at TOH (and includes his or her SDM where relevant) and is a type of Individual as defined in this policy.

Patient Images: Any still or moving image of a patient (even if the patient cannot be identified). This includes photographs, videos, and digital images. Patient images do not include diagnostic images like x-rays, MRIs, ultrasounds, or photography of pathological specimens.

Personal Health Information (PHI): Any information about a patient's health care, such as their provider, billing number, clinical notes and test results. It can include current, previous, or future health care. PHI can include the traditional health record as well as video footage, images, etc. that do not form part of the traditional health record.

Personal Information (PI): Any information about an identifiable Individual such as demographics, credit card information, employment history, etc. PI may be about TOH staff, volunteers, donors, or any other Individual that entrusts information about themselves to TOH. PI can include information in many forms such as physical or electronic files, as well as audio, images, video footage, etc.

Privacy Impact Assessment: An assessment that identifies the privacy risks associated with a program or initiative and that makes recommendations to address them.

Privacy Breach: Collecting, using, disclosing, copying, modifying, or destroying PI or PHI for an unauthorized purpose regardless of whether it is intentional or accidental, or instances where PI or PHI is lost or stolen.

Record: Any record of information in any form. This includes: electronic and physical files; email, messaging, and other correspondence; audio, film, and microfilm; pictures, photographs, and graphics; and machine-readable records and other documentary material.

Repository Owner: The staff member at TOH responsible for managing PI or PHI in a repository.

Repository: An electronic or paper-based filing system of PI or PHI.

Request for Access: An Individual asking to see or get a copy of their PI or PHI.

Request for Correction: An Individual asking to correct their PI or PHI if they think it is out of date or inaccurate.

Staff: Anyone who works on behalf of TOH. This includes permanent or temporary, full-time, part-time, casual or contract employees, trainees and volunteers, and vendors. This also includes administrative and clinical personnel like administrative assistants, physicians, residents, interns, researchers and students.

Statement of Disagreement: A note that an Individual may attach to their PI or PHI if they feel that it is incorrect (i.e., if they disagree with the information).

Substitute Decision-Maker (SDM): A person who is authorized to make decisions on behalf of the Individual about how their PI or PHI is collected, used, or disclosed.

TOH Resources: Specific tools and equipment belonging to TOH (e.g., TOH email, electronic health record system, telephones, parking system), as well as paid Staff time.

Use: Any handling of PI or PHI including viewing or electronic processing of PI or PHI by TOH Staff.

Policy Statement(s):

Accountability:

- We are responsible for PI or PHI in our control, including PI or PHI that we may send to third parties for processing. We will protect this PI or PHI and the privacy of the Individuals to whom it relates.

- TOH has a governance structure in place with delegated responsibility from the Board for privacy matters. This includes a Chief Privacy Officer who is responsible for maintaining and overseeing TOH's privacy program.

- We will have a privacy program in place including documented policies and procedures.

- We will provide privacy training to Staff before giving them access to PI or PHI and every year after.

- We will impose relevant privacy obligations on everyone working on our behalf by requiring them to sign confidentiality agreements or embedding privacy obligations in their agreements with TOH.

- We will promote privacy with email, newsletters, brochures, and other communication.

Collecting, Using, and Disclosing PI or PHI:

- We will only collect, use, and disclose PI or PHI as permitted or required by law. See Corporate SOP – Obtaining Consent for Collection, Use, or Disclosure of Personal Information or Personal Health Information.

- An Individual can limit how we collect, use, and disclose their PI or PHI with some exceptions.

- At the time of or before we collect, use, or disclose an Individual's PI or PHI, we will identify and be able to explain the purpose of the collection, use, or disclosure.

- We will only collect PI or PHI from the Individual directly unless there is a legitimate and lawful reason to collect it indirectly.

- We will only allow Staff who need to collect, use, or disclose PI or PHI as part of their job responsibilities to do so.

- We will only collect, use, or disclose as much PI or PHI as needed for the purpose we identify to the Individual.

- We will document the purposes for which we collect PI or PHI.

- If we use or disclose PI or PHI in a manner that is not consistent with the purpose of collection, we will document it in the relevant record.

- We will try to make sure PI or PHI is accurate, complete, and up-to-date as necessary to fulfill the purposes of collection.

- We will not routinely update an Individual's PI or PHI unless this is necessary to fulfill the purposes for which the PI or PHI was collected.

- We will record disclosures of PI or PHI where possible.

Consent

- We generally rely on an Individual's implied consent for the collection, use, and disclosure of PI or PHI if the information is required for the purposes, including providing health care, unless the Individual has withdrawn their consent (i.e. break-the-glass).

- We will get consent to collect, use, and disclose PI or PHI unless exempted by law.

- We will not require an Individual to consent to the collection, use, or disclosure of PI or PHI beyond that which is needed to fulfil the explicitly specified, primary, and legitimate purpose.

- We will get consent from Staff to use their image for public purposes (e.g., brochure, news).

- Consent is only valid and knowledgeable if it is reasonable to expect that an Individual to whom our activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the PI or PHI to which they are consenting.

- We will generally rely on implied consent when collecting non-sensitive PI or PHI that a reasonable person would consider appropriate in the circumstances (e.g., collecting information at a card payment machine).

Transparency

- We will publish information about our privacy program on our website and in our buildings.

- We will inform Individuals about:
    - The type of PI or PHI that we collect about them;
    - The purpose for which we collect their PI or PHI; and
    - What we do with their PI or PHI.

- When informing Individuals about the type of PI or PHI we collect and the purposes, we will do that before collection unless it is clear in the circumstances that the Individual would be aware of the purpose (e.g., collection of credit card number when paying in the cafeteria).

- We will publish information about an Individual's privacy rights and how to contact our Information and Privacy Office to exercise them.

Access and Correction Rights

- We will provide an Individual with access to their own PI or PHI except in limited circumstances. See Corporate SOP – Request for Access or Correction to Personal Information and Personal Health Information.

- We will correct PI or PHI that is incomplete, out-of-date, or inaccurate except in limited circumstances.

- If we refuse to change the PI or PHI and the Individual it belongs to disagrees, they may attach a "Statement of Disagreement" to their PI or PHI in our control.

- We will inform organizations to which we have previously disclosed information if a correction or Statement of Disagreement may impact the Individual or service that they receive.

Privacy Breach Management:

- Staff must report any possible privacy breach to the IPO through the Safety Learning System as soon as possible.

- We will contain, inform, investigate, and resolve breaches as soon as possible. See Corporate SOP – Privacy Breach Management.

- Staff responsible for privacy breaches may be subject to a Just Culture investigation as outlined in Corporate Policy – Employee Accountability.

Risk Management and Assurance:

- We will record electronically or otherwise when we collect, use, or disclose PI or PHI where practical.

- We will undertake audits to evaluate the appropriateness of the collection, use, and disclosure of PI or PHI, as appropriate.

- We will review our Staff and vendor practices to ensure they appropriately protect privacy and PI or PHI (e.g., audit Staff computer access).

- We will conduct privacy impact and risk assessments and operational reviews to identify ways to be more privacy protective.

Retention

- We will have an information security program in place to protect PI or PHI against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. See Corporate Policy – TOH Information Security.

- We will retain PI or PHI only as long as necessary to fulfil the purpose for which it was collected and to meet legal requirements. See Corporate SOP – Retention and Destruction of Corporate Records by Record Type.

- Where possible, we will retain PI or PHI in structured data repositories to enable easy retrieval.

- We will retain PI or PHI in Canada where possible. Where it is not possible to retain PI or PHI in Canada, we will inform the Individual to whom the PI or PHI relates where possible.

- If we no longer need PI or PHI to fulfil a purpose, we will destroy it according to Corporate SOP – Retention and Destruction of Corporate Records by Record Type.

Shared Systems:

- TOH has shared computer systems in which we collect, use, and disclose PHI to provide care to Patients.

- TOH will follow the policies established by those overseeing the shared system.

Exceptions:

- Staff unable to follow this policy must get approval from the Chief Privacy Officer, the IPO, or the Privacy and Information Security Steering Committee for an exception.

Questions or Concerns:

Questions or complaints about our privacy program, how we protect PI or PHI, or this policy should be directed to the IPO at infoprivacyoffice@toh.ca or (613) 739-6668.

Related Documents:

Corporate Policy – TOH Information Security

Corporate Policy - Communications

Corporate Policy - Retention and Destruction of Corporate Records

Corporate SOP – Request for Access or Correction to Personal Information and Personal Health Information

Corporate SOP – Retention and Destruction of Corporate Records by Record Type

Corporate SOP – Auditing End-Users

Corporate SOP - Responding to Privacy-Related Inquiries and Complaints

Corporate SOP - Privacy and Security Training

Corporate SOP - Privacy Breach Management

Corporate SOP – Privacy Obligations in Agreements

Corporate SOP – Obtaining Consent for Collection, Use, or Disclosure of Personal Information or Personal Health Information

Corporate SOP - Consent Directives

Corporate SOP - Secure Transfer of Sensitive Information

Related Legislation or Regulatory Requirements:
Personal Health Information Protection Act, 2004 (PHIPA)
Personal Information Protection and Electronic Documents Act (PIPEDA)
Freedom of Information and Protection of Privacy Act (FIPPA)
Canada's Anti-Spam Legislation (CASL)

References:
Office of the Privacy Commissioner of Canada. PIPEDA Compliance Help.
Office of the Privacy Commissioner of Canada. Interpretation Bulletins.
Information and Privacy Commissioner of Ontario, "Detecting and Deterring Unauthorized Access to Personal Health Information" (Toronto: ON, 2015)
Information and Privacy Commissioner of Ontario, Order HO-14
Information and Privacy Commissioner of Ontario, PIPA Order HO-010
Information and Privacy Commissioner of Ontario, PIPA Order HO-002