Status **Active** PolicyStat ID **14573766**

Origination	07/2021
Last Approved	06/2024
Effective	06/2024
Last Revised	06/2024
Next Review	06/2025
Owner	Nyranne Martin: Chief Legal Officer/General Counsel
Area	Legal, Privacy & Risk Management
References	Corporate Policy

Privacy, ADM II 260b

Corporate Policy

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:

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' in the Epic Health Information System).

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): Has the meaning defined in PHIPA. For clarity, PHI includes any information about a Patient's physical or mental health and the provision of healthcare to that Patient, 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, 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: Permanent or temporary, full-time, part-time, casual or contract employees, trainees, and volunteers, including but not limited to physicians, residents, interns, researchers, students, and any other individuals who perform work or supply services at TOH.

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 communications.
- We routinely monitor TOH's information systems for cyber security reasons, which may reveal Staff PI. See Corporate Policy – Acceptable Use and Corporate SOP – Search of a Patient, Visitor or Staff Belongings or Activities.

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).
- We will get consent from Staff to view their PI when we intentionally monitor their information systems, except where permitted or required by law and authorized by a department head, Human Resources, or Employee Relations. See Corporate Policy – Acceptable Use and Corporate SOP – Search of a Patient, Visitor or Staff Belongings or Activities.
- 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. Where an Individual does not have the capacity to provide valid and knowledgeable consent, we will get consent from the Individual’s authorized SDM.
- We will generally rely on implied consent when collecting non-sensitive PI or PHI that a

reasonable person would consider appropriate in the circumstances.

- Staff and external stakeholders will not take photographs, videos, or audio recordings of any Individual without consent. External stakeholders may be asked to delete unauthorized photos, videos, or audio recordings. See Corporate Policy - Communications and Corporate Policy - Social Media.

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.
- 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.
- We will maintain confidentiality of the Staff and others reporting the breach to the greatest extent as possible.

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 Risk Hub 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 ADM VII 230 – Acceptable Use

Corporate Policy ADM III 400 – Communications

Corporate Policy ADM III 500 - Social Media

Corporate Policy ADM III 310 – Retention and Destruction of Corporate Records

Corporate Policy ADM VII 340 – TOH Information Security Awareness & Training

Corporate Policy ADM IV 330 - Payment Card Industry Data Security Standard (PCI DSS) Compliance

Corporate SOP II 263 – Auditing End-Users

Corporate SOP III 340 – Consent to Collection, Use and Disclosure of Personal Information or Personal Health Information

Corporate SOP III 330 – Consent Directives ("Lock-Box")

Corporate SOP II 264 – Privacy Breach Management

Corporate SOP II 266 – Privacy Obligations in Agreements

Corporate SOP II 267 – Privacy and Security Training

Corporate SOP III 381 – Request for Access or Correction to Personal Information and Personal Health Information

Corporate SOP II 265 – Responding to Privacy-Related Inquiries and Complaints

Corporate SOP III 311 – Retention and Destruction of Corporate Records by Record Type

Corporate SOP II 350 – Secure Transfer of Sensitive Information

Related Legislation or Regulatory Requirements:

Canada's Anti-Spam Legislation (CASL)

Freedom of Information and Protection of Privacy Act (FIPPA)

Personal Health Information Protection Act, 2004 (PHIPA)

Personal Information Protection and Electronic Documents Act (PIPEDA)

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

Summary of Changes:

June 2024

- Added policy statement in the Consent section- "*Staff and external stakeholders will not take photographs, videos, or audio recordings of any Individual without consent. External stakeholders may be asked to delete unauthorized photos, videos, or audio recordings. See Corporate Policy - Communications and Corporate Policy - Social Media*"

Protection des renseignements personnels

Politique de L'Hôpital d'Ottawa

Objectif

L'Hôpital d'Ottawa (l'Hôpital) protège la vie privée de chaque personne qui lui confie ses renseignements personnels ou ses renseignements personnels sur la santé. La présente politique énonce les règles de l'Hôpital en matière de protection de la vie privée qui s'appliquent à la collecte, à l'utilisation, à la divulgation et à la conservation de renseignements personnels ou de renseignements personnels sur la santé.

Portée

La présente politique s'applique à toutes les personnes qui traitent des renseignements personnels ou des renseignements personnels sur la santé au sujet d'une personne, que ce soit au nom de l'Hôpital ou dans tout emplacement où l'Hôpital offre des soins ou des services. Elle ne concerne pas les renseignements au sujet d'une personne qui sont liés à son statut professionnel (p. ex., les coordonnées professionnelles d'un membre du personnel).

Définitions

Collecte : Action (effectuée par l'Hôpital ou toute personne qui travaille en son nom) de recueillir directement des renseignements personnels ou des renseignements personnels sur la santé, de la part d'une personne ou d'un tiers.

Consentement : Permission accordée par une personne de recueillir, d'utiliser ou de divulguer ses renseignements personnels ou renseignements personnels sur la santé.

Directive sur le consentement : Limite imposée par une personne sur les manières dont l'Hôpital peut recueillir, utiliser ou divulguer ses renseignements personnels ou renseignements personnels sur la santé (mention « Break-the-Glass » dans le système Epic).

Dépositaire : Organisme autorisé par la loi à prendre des décisions au sujet de renseignements personnels ou de renseignements personnels sur la santé et qui est tenu de protéger ces renseignements. Cette définition comprend celle d'un « dépositaire de renseignements sur la santé » au sens de la *Loi sur la protection des renseignements personnels sur la santé* (**LPRPS**) et celle d'une « institution » au sens de la *Loi sur l'accès à l'information et la protection de la vie privée* (**LAIPVP**). Aux fins de la présente politique, l'Hôpital est le dépositaire.

Divulgation : Action (effectuée par l'Hôpital ou toute personne qui travaille en son nom) de communiquer des renseignements personnels ou des renseignements personnels sur la santé (y compris verbalement) à une personne extérieure à l'Hôpital.

Soins de santé : Observation, examen, évaluation, soins, service ou intervention réalisés à des fins de santé.

Dépositaire de renseignements sur la santé : Organisme, au sens de la LPRPS, qui est autorisé par la loi à prendre des décisions au sujet de renseignements personnels sur la santé et qui est tenu de protéger ces renseignements.

Personne : Individu sur lequel portent les renseignements personnels ou renseignements personnels sur la santé (le mandataire spécial de la personne est compris dans cette définition, le cas échéant).

Institution : Organisme, au sens de la LAIPVP, qui est autorisé par la loi à prendre des décisions au sujet de renseignements personnels et qui est tenu de protéger ces renseignements.

Culture juste : Philosophie assurant la gestion juste, éthique et cohérente de tout manquement à une obligation. Elle favorise le signalement honnête de tout manquement pour favoriser l'amélioration continue dans tout l'Hôpital.

Patient : Personne, au sens de la définition de la présente politique, qui reçoit des soins de l'Hôpital (le mandataire spécial du patient est compris dans cette définition, le cas échéant).

Images du patient : Toute image fixe ou en mouvement d'un patient (même si le patient ne peut pas y être identifié). Sont comprises dans cette définition les photographies, vidéos et images numériques. Sont exclues de cette définition les images diagnostiques comme les radiographies, l'imagerie par résonance magnétique, les échographies ou les photographies d'échantillons de pathologie.

Renseignements personnels sur la santé : Selon le sens défini dans la LPRPS. Par souci de clarté, les renseignements personnels sur la santé englobent tout renseignement sur la santé physique ou mentale d'un patient et la prestation de soins de santé à ce patient, dont l'identité de son fournisseur de soins et son numéro de facturation, les notes cliniques et ses résultats d'examens liés à ses soins en cours, déjà reçus ou à recevoir. Ils comprennent le dossier médical conventionnel, ainsi que des extraits vidéo, des

images et d'autres renseignements qui n'en font pas habituellement partie.

Renseignements personnels : Tout renseignement sur une personne pouvant permettre de l'identifier, dont les données démographiques, les emplois préalables, etc. Ils peuvent porter sur les membres du personnel de l'Hôpital, ses bénévoles, ses donateurs et toute autre personne qui confie à l'Hôpital des renseignements sur elle-même. Ils peuvent prendre diverses formes, comme des fichiers physiques ou électroniques, des enregistrements sonores, des images ou des extraits vidéo.

Évaluation de l'impact sur la protection de la vie privée : Évaluation cernant les risques à la vie privée associés à un programme ou à une initiative et comportant des recommandations pour atténuer ces risques.

Atteinte à la vie privée : Collecte, utilisation, divulgation, copie, modification, destruction, vol ou perte de renseignements personnels ou de renseignements personnels sur la santé à des fins non autorisées, que ce soit de manière intentionnelle ou accidentelle.

Document : Tout support contenant des renseignements, sous quelque forme que ce soit. Comprend fichiers électroniques et physiques, courriels, messagerie et autres formes de correspondance, enregistrements sonores, sur film et microfilm, illustrations, photographies et graphiques, documents lisibles par machine et tout autre matériel documentaire.

Propriétaire de répertoire : Membre du personnel de L'Hôpital d'Ottawa responsable d'administrer les renseignements personnels ou renseignements personnels sur la santé stockés dans un répertoire.

Répertoire : Système électronique ou papier servant à classer les renseignements personnels ou renseignements personnels sur la santé.

Demande d'accès : Action d'une personne qui demande à consulter ses propres renseignements personnels ou renseignements personnels sur la santé, ou à en obtenir une copie.

Demande de rectification : Action d'une personne qui demande la rectification de ses renseignements personnels ou renseignements personnels sur la santé si elle estime que ceux-ci sont inexacts ou ne sont plus à jour.

Membre du personnel: Tout employé permanent ou temporaire, à temps plein, à temps partiel, occasionnel ou contractuel, tout stagiaire et tout bénévole, y compris tout médecin, résident, stagiaire, chercheur et étudiant à l'Hôpital et toute personne qui réalise un travail ou fournit des services à l'Hôpital.

Mention de désaccord : Note qu'une personne peut faire joindre à ses renseignements personnels ou renseignements personnels sur la santé si elle estime que ceux-ci sont inexacts (c.-à-d. qu'elle n'est pas d'accord avec l'information).

Mandataire spécial : Personne autorisée à prendre des décisions au nom de la personne concernée sur la collecte, l'utilisation et la divulgation de ses renseignements personnels ou renseignements personnels sur la santé.

Ressources de l'Hôpital : Outils et matériel qui appartiennent à L'Hôpital d'Ottawa (courriel de l'Hôpital, système de dossier de santé électronique, téléphones, système de stationnement, etc.). Le temps de

travail rémunéré du personnel fait également partie des ressources de l'Hôpital.

Utilisation : Tout traitement de renseignements personnels ou de renseignements personnels sur la santé, y compris leur consultation et leur traitement électronique par le personnel de l'Hôpital.

Énoncés de politique

Responsabilité

- Nous sommes responsables des renseignements personnels et des renseignements personnels sur la santé qui sont en notre possession, y compris ceux que nous pouvons transmettre à des tiers aux fins de traitement. Nous protégeons ces renseignements personnels ou renseignements personnels sur la santé, de même que la vie privée des personnes sur lesquelles ils portent.
- À L'Hôpital d'Ottawa, la structure de gouvernance en place prévoit la délégation par le Conseil des gouverneurs de la responsabilité en matière de vie privée. Ainsi, le chef de la protection des renseignements personnels est responsable de maintenir et de superviser le programme de protection de la vie privée de l'Hôpital.
- Nous avons en place un programme de protection de la vie privée, comprenant des politiques et des procédures écrites.
- Nous donnons à tous les membres du personnel une formation sur la protection de la vie privée avant de leur donner accès à des renseignements personnels ou renseignements personnels sur la santé, et chaque année par la suite.
- Nous exigeons que toute personne qui travaille en notre nom s'engage envers la protection de la vie privée en signant un accord de confidentialité ou une entente qui comprend des obligations concernant la protection de la vie privée.
- Nous faisons la promotion du respect de la vie privée dans les courriels, les bulletins d'information, les publications et d'autres formes de communications.
- Nous surveillons régulièrement les systèmes d'information de l'Hôpital à des fins de cybersécurité, ce qui pourrait révéler des renseignements personnels de membres du personnel. Consulter la politique *Acceptable Use* et la procédure opérationnelle normalisée *Search of a Patient, Visitor or Staff Belongings or Activities*.

Collecte, utilisation et divulgation de renseignements personnels ou de renseignements personnels sur la santé

- Nous recueillons, utilisons et divulguons des renseignements personnels ou des renseignements personnels sur la santé uniquement dans la mesure permise ou requise par la loi. Consulter la procédure opérationnelle normalisée *Obtaining Consent for Collection, Use, or*

Disclosure of Personal Information or Personal Health Information (Obtenir un consentement pour la collecte, l'utilisation ou la divulgation de renseignements personnels ou de renseignements personnels sur la santé).

- Une personne peut imposer une limite quant à la collecte, à l'utilisation et à la divulgation de ses renseignements personnels ou renseignements personnels sur la santé (des exceptions s'appliquent).
- Avant ou au moment de collecter, d'utiliser ou de divulguer des renseignements personnels ou des renseignements personnels sur la santé d'une personne, nous indiquons et sommes en mesure d'expliquer l'objectif de la collecte, de l'utilisation ou de la divulgation.
- Nous recueillons les renseignements personnels ou les renseignements personnels sur la santé directement auprès de la personne concernée, sauf s'il existe un motif légitime et légal de le faire indirectement.
- Seuls les membres du personnel qui doivent recueillir, utiliser ou divulguer des renseignements personnels ou des renseignements personnels sur la santé pour exercer leurs responsabilités professionnelles seront autorisés à le faire.
- Nous recueillons, utilisons et divulguons seulement les renseignements personnels ou renseignements personnels sur la santé qui sont nécessaires pour les motifs précisés à la personne concernée.
- Nous consignons les motifs pour lesquels nous recueillons des renseignements personnels ou des renseignements personnels sur la santé.
- En cas d'utilisation ou de divulgation de renseignements personnels ou de renseignements personnels sur la santé ne correspondant pas aux objectifs de la collecte, nous consignons l'activité dans le document pertinent.
- Nous nous efforçons de nous assurer que les renseignements personnels ou renseignements personnels sur la santé sont exacts, complets et à jour, de sorte qu'ils répondent aux objectifs de leur collecte.
- Nous ne faisons pas de mise à jour régulière des renseignements personnels ou de renseignements personnels sur la santé d'une personne, sauf si c'est nécessaire pour répondre aux besoins de leur collecte.
- Nous consignons la divulgation de renseignements personnels ou de renseignements personnels sur la santé dans la mesure du possible.

Consentement

- Nous comptons habituellement sur le consentement implicite d'une personne pour la collecte, l'utilisation et la divulgation de ses renseignements personnels ou renseignements personnels sur la santé si cela est requis pour lui fournir des soins de santé, sauf si la personne a retiré son consentement (mention « Break-the-Glass »).
- Nous obtenons un consentement pour la collecte, l'utilisation et la divulgation de renseignements personnels ou de renseignements personnels sur la santé, sauf si la loi nous en exempte.
- Nous ne demandons pas le consentement d'une personne pour la collecte, l'utilisation et la

divulgation de ses renseignements personnels ou renseignements personnels sur la santé autrement qu'aux fins principales et légitimes explicitement décrites.

- Nous obtenons le consentement du personnel pour l'utilisation de leur image à des fins publiques (brochure, article, etc.).
- Nous obtenons le consentement du personnel pour voir leurs renseignements personnels lorsque nous surveillons leurs systèmes d'information, sauf lorsqu'une loi, un chef de service autorisé, les Ressources humaines ou les Relations avec les employés nous permettent ou exigent de procéder autrement. Consulter la politique *Acceptable Use* et la procédure opérationnelle normalisée *Search of a Patient, Visitor or Staff Belongings or Activities*.
- Le consentement est valide et éclairé seulement s'il est raisonnable de s'attendre à ce qu'une personne visée par nos activités comprenne la nature, l'objectif et les conséquences de la collecte, de l'utilisation ou de la divulgation des renseignements personnels ou des renseignements personnels sur la santé faisant l'objet de son consentement. Dans le cas où un particulier n'a pas la capacité de donner un consentement valide et éclairé, nous obtenons ce consentement de son mandataire spécial autorisé.
- Nous comptons habituellement sur le consentement implicite d'une personne pour la collecte de renseignements personnels ou de renseignements personnels sur la santé qui ne sont pas de nature délicate, dans les situations où une personne raisonnable trouverait approprié de le faire.
- Le personnel et les intervenants externes ne peuvent pas prendre de photos ou faire un enregistrement vidéo ou audio d'un particulier sans son consentement. Nous pouvons demander aux intervenants externes de supprimer toute photo ou tout enregistrement vidéo ou audio non autorisé. Veuillez consulter à ce sujet la Politique générale – Communications et la Politique générale – Médias sociaux.

Transparence

- Nous publions de l'information au sujet de notre programme de protection de la vie privée sur notre site Web et dans nos installations.
- Nous informerons chaque personne sur :
    - le type de renseignements personnels ou de renseignements personnels sur la santé que nous recueillons à son sujet;
    - l'objectif de la collecte de renseignements personnels ou de renseignements personnels sur la santé;
    - l'utilisation que nous faisons de ses renseignements personnels ou renseignements personnels sur la santé.
- Lorsque nous informons une personne du type de renseignements personnels ou de renseignements personnels sur la santé que nous recueillons et de l'objectif de la collecte, nous le faisons avant la collecte, sauf dans les situations où il est évident que la personne connaît l'objectif.
- Nous publions des renseignements sur les droits en matière de protection de la vie privée et les moyens de communiquer avec notre Bureau de la protection de la vie privée et de

l'information pour faire valoir ces droits.

Droits à l'accès et à la rectification

- Nous permettons à toute personne d'accéder à ses renseignements personnels ou renseignements personnels sur la santé, sauf dans certaines situations particulières. Consulter la procédure opérationnelle normalisée *Request for Access or Correction to Personal Information and Personal Health Information* (Demande de consultation et de correction de renseignements personnels ou renseignements personnels sur la santé).
- Nous rectifions les renseignements personnels ou renseignements personnels sur la santé qui sont incomplets ou inexacts, ou qui ne sont plus à jour, sauf dans certaines situations particulières.
- Si nous refusons de modifier des renseignements personnels ou renseignements personnels sur la santé et que la personne à qui ils appartiennent est en désaccord, elle peut joindre une « Mention de désaccord » aux renseignements qui sont en notre possession.
- Nous avisons les organismes auxquels nous avons déjà divulgué des renseignements si une rectification ou une Mention de désaccord peut avoir des répercussions qui concernent la personne ou le service qu'elle reçoit.

Gestion des atteintes à la vie privée

- Le personnel doit signaler toute atteinte possible à la vie privée dès que possible au Bureau de la protection de la vie privée et de l'information.
- Nous prenons les mesures pour contenir toute atteinte à la vie privée, en avisons les personnes concernées, menons des enquêtes et réglons la situation le plus rapidement possible. Consulter la procédure opérationnelle normalisée *Privacy Breach Management*.
- Un membre du personnel responsable d'une atteinte à la vie privée peut faire l'objet d'une enquête conforme à la culture juste, comme le stipule la politique générale *Employee Accountability*.
- Dans la mesure du possible, nous maintenons la confidentialité du membre du personnel ou de toute autre personne qui signale une atteinte à la vie privée.

Gestion du risque et assurance

- Nous consignons en format électronique ou autre la collecte, l'utilisation ou la divulgation de renseignements personnels ou de renseignements personnels sur la santé, dans la mesure du possible.
- Nous réalisons des vérifications, s'il y a lieu, pour évaluer la pertinence de la collecte, de l'utilisation et de la divulgation de renseignements personnels ou de renseignements personnels sur la santé.

- Nous passons en revue les pratiques de notre personnel et de nos fournisseurs pour nous assurer qu'ils protègent adéquatement la vie privée et les renseignements personnels ou renseignements personnels sur la santé (p. ex. vérification des accès informatiques du personnel).
- Nous menons des évaluations des risques et de l'impact sur la protection de la vie privée, ainsi que des examens opérationnels, pour trouver des façons de mieux protéger la vie privée.

Durée de conservation

- Nous avons un programme de sécurité de l'information visant à protéger les renseignements personnels et renseignements personnels sur la santé contre la perte et le vol, ainsi que l'accès à ces renseignements, leur divulgation, leur copie, leur utilisation ou leur modification sans autorisation. Consulter la politique « Sécurité de l'information ».
- Nous conservons les renseignements personnels ou renseignements personnels sur la santé aussi longtemps que nécessaire pour répondre à l'objectif pour lequel les renseignements ont été recueillis et pour remplir nos obligations juridiques. Consulter la politique *Retention and Destruction of Corporate Records by Record Type* (Conservation et destruction des dossiers de l'Hôpital).
- Dans la mesure du possible, nous conservons les renseignements personnels et les renseignements personnels sur la santé dans des répertoires de données structurés pour faciliter le repérage.
- Nous conservons les renseignements personnels et les renseignements personnels sur la santé au Canada dans la mesure du possible. Dans les cas où cela est impossible, nous en avisons la personne à qui ils appartiennent dans la mesure du possible.
- Si nous n'avons plus besoin de certains renseignements personnels ou renseignements personnels sur la santé pour répondre à un objectif, nous les détruisons conformément à la procédure opérationnelle normalisée *Retention and Destruction of Corporate Records by Record Type* (Conservation et destruction des dossiers de l'Hôpital par type de document).

Systèmes partagés

- L'Hôpital d'Ottawa utilise des systèmes informatiques partagés qui servent à la collecte, à l'utilisation et à la divulgation de renseignements personnels sur la santé pour fournir des soins aux patients.
- Nous suivons les politiques mises en place par les responsables des systèmes partagés.

Exceptions

Tout membre du personnel qui n'est pas en mesure de respecter la présente politique doit faire approuver une exception par le chef de la protection des renseignements personnels, le Bureau de la protection de la vie privée et de l'information ou le responsable de la gestion des risques.

Questions ou préoccupations

Pour toute question ou plainte au sujet de notre programme de protection de la vie privée, des méthodes de protection des renseignements personnels ou des renseignements personnels sur la santé, ou encore de la présente politique, communiquer avec le Bureau de la protection de la vie privée et de l'information à infoprivee@lho.ca ou au 613-739-6668.

Documents connexes

- Politique générale ADM VII 230 – Acceptable Use
- Politique générale ADM III 400 – Communications
- Politique générale ADM III 500 – Médias sociaux
- Politique générale ADM VII 310 – Retention and destruction of Corporate Records
- Politique générale ADM VII 340 – TOH Information Security Awareness and Training
- Politique générale ADM IV 330 – Conformité aux normes de sécurité des données industrielles concernant les cartes de paiement (PCI DSS)
- Procédure opérationnelle normalisée II 263 – Auditing End-Users
- Procédure opérationnelle normalisée III 340 – Consent for Collection, Use, or Disclosure of Personal Information or Personal Health Information
- Procédure opérationnelle normalisée III 330 – Consent Directives ("Lock-Box")
- Procédure opérationnelle normalisée II 266 – Privacy Obligations in Agreements
- Procédure opérationnelle normalisée II 267 – Privacy and Security Training
- Procédure opérationnelle normalisée III 381 – Request for Access or Correction to Personal Information & Personal Health Information
- Procédure opérationnelle normalisée II 265 – Responding to Privacy-Related Inquiries and Complaints
- Procédure opérationnelle normalisée III 311 – Retention and Destruction of Corporate Records by Record Type
- Procédure opérationnelle normalisée II 264 – Privacy Breach Management
- Procédure opérationnelle normalisée II 350 – Secure Transfer of Sensitive Information

Lois et règlements connexes

- Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
- *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)
- *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP)

- *Loi canadienne antipourriel* (LCAP)

Références

- Commissariat à la protection de la vie privée du Canada. Aide sur la façon de se conformer à la LPRPDE.
- Commissariat à la protection de la vie privée du Canada. Bulletins sur l'interprétation de la LPRPDE.
- Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* (Toronto ON, 2015)
- Commissaire à l'information et à la protection de la vie privée de l'Ontario : Ordonnance HO-14
- Commissaire à l'information et à la protection de la vie privée de l'Ontario : Ordonnance HO-010
- Commissaire à l'information et à la protection de la vie privée de l'Ontario : Ordonnance HO-002

Résumé des changements

Juin 2024

- Ajout de l'énoncé de politique à la section Consentement – « *Le personnel et les intervenants externes ne peuvent pas prendre de photos ou faire un enregistrement vidéo ou audio d'un particulier sans son consentement. Nous pouvons demander aux intervenants externes de supprimer toute photo ou tout enregistrement vidéo ou audio non autorisé. Veuillez consulter à ce sujet la Politique générale – Communications et la Politique générale – Médias sociaux* »

Approval Signatures

Step Description	Approver	Date
Final QA & Publish	Serena Clarke: Coordinator, Policy and Procedure Management	06/2024
CEO Final Approval	Cameron Love: President and CEO, TOH	06/2024

Invite SMT Members to Review the Policy & Approve After the SMT Meeting. Type the person's name and your message and they will receive it by email. Add the "how to provide feedback" instruction in your message to them.	Sylvie Lortie: Other Title (Not on List)	06/2024
QA Check-Opportunity for Union Review. Feedback can be provided in the comments section. Type the person's name and your message and they will receive it by email.	Serena Clarke: Coordinator, Policy and Procedure Management	06/2024
Please Review and Approve. Feedback can be provided in the comments section. Type the person's name and your message and they will receive it by email.	Nyranne Martin: Chief Legal Officer/General Counsel	06/2024
Initial Authoring Phase- Edit Document	Elisabeth Oliviero: Other Title (Not on List)	06/2024