Kensington Health	CORPORATE PRIVACY POLICY	CORP-CPS-03.001

Manual:	Corporate Policy Statements	**Reviewed Date:**	May 2021
Original Date:	October 2018	**Revised Date:**	May 2021
Approved By:	Chief Privacy Officer	**Signature:**	

SCOPE

- ☑ Kensington Gardens
- ☑ Kensington Hospice
- ☑ Second Mile Club
- ☑ Eye Bank of Canada Ontario Division
- ☑ Kensington Diagnostic Imaging Clinic
- ☑ Kensington Eye Institute
- ☑ Kensington Screening Clinic
- ☑ Kensington Vision and Research Centre

CONTENTS

PURPOSE

Kensington Health's Corporate Privacy Policy is adopted in accordance with the Ontario Personal Health Information Protection Act (PHIPA), 2004. The purpose of this Policy is to balance an individual's fundamental right to privacy and right of access to their Personal Health Information (PHI), with Kensington Health's need to collect, use and disclose PHI in connection with its operations as service providers and Health Information Custodians (HIC) in Ontario.

OVERVIEW

There are seven (7) Health Information Custodians (HIC) at Kensington Health:

1. **Kensington Gardens:**[1] a 350-bed, long-term care facility offering 24-hour nursing and life enhancement services.
2. **Kensington Hospice:**[2] a 19-bed hospice providing palliative and end-of-life care.
3. **Second Mile Club:**[3] provides community programs for seniors and adults with disabilities.
4. **Kensington Diagnostic Imaging Centre (KDIC)**:[4] provides patients with access to ultrasound, x-ray, bone mineral density, breast imaging and biopsy services.
5. **Kensington Cancer Screening Clinic (KCSC)**:[4] provides patients with access to colonoscopy and gastroscopy screening procedures as well as gastrointestinal treatment.
6. **Kensington Eye Institute (KEI)**:[4] provides ambulatory surgical and medical vision care.
7. **Kensington Vision & Research Centre (KVRC) - Physician HIC:** [4] provides clinical, diagnostic and ancillary vision care. The physicians have custody of patients PHI and therefore act as the HIC. KVRC is their service provider.

Trillium Gift of Life Network (TGLN) : Under the Gift of Life Act, TGLN is permitted to collect, use and disclose personal health information as required and in accordance with other applicable laws. The Eye Bank of Canada's Ontario Division (EBCOD) is designated as a Class D facility (Tissue Bank) under the Gift of Life Act. While the EBCOD can upload its own data, all Donor data is under the custody of the TGLN.

The Kensington Health programs set out above have jointly decided to follow a single set of policies and procedures with respect to privacy laws.

POLICY

1. PRINCIPLE 1: Accountability for PHI

1.1. Delegation of Responsibilities

1.1.1. Kensington Health is responsible for PHI in its custody or control and each HIC has delegated operational day-to-day responsibility for privacy compliance to Kensington Health's Chief Privacy Officer (CPO).

1.1.2. Each HIC is ultimately accountable for its own compliance with PHIPA and thus each HIC has its own Privacy Officer.

1.1.3. Kensington Health demonstrates its commitment to privacy and the confidentiality of PHI by:

- Implementing policies and procedures to protect PHI;
- Educating anyone who collects, uses or discloses PHI on Kensington Health's behalf about their responsibilities
- Authorizing the CPO to: receive and respond to complaints, field inquiries, make privacy policies and procedures publicly available and review the Corporate Privacy Policy.

1.2. Discrepancies

1.2.1. If there is a discrepancy between this Policy and PHIPA, PHIPA takes precedence.

1.2.2. The Corporate Privacy Policy is reviewed annually to ensure that it reflects current legislation and practices at Kensington Health.

1.2.3. Kensington Health's Privacy Committee will review and approve proposals to update or amend privacy policies or procedures.

1.2.4. Kensington Health's Senior Leadership Team will approve any changes to the Corporate Privacy Policy.

1.3. Implementation

1.3.1. The Corporate Privacy Policy is implemented throughout the organization, by the CPO, using appropriate means to ensure that Kensington Health staff understand and apply the privacy principles in their daily work.

1.4. Third Parties

1.4.1. Kensington Health is responsible for vendors and third-party care and service providers acting on behalf of Kensington Health and accessing PHI.

1.4.2. Kensington Health uses contractual means and educational training sessions to ensure that a comparable level of protection is applied when PHI is handled by third party service providers.

2. PRINCIPLE 2: Identifying Purposes for the Collection of PHI

2.1. Whenever Kensington Health collects PHI from an individual, it will explain the purpose for the collection at the time of the collection, or as soon as is reasonably possible.

2.2. Kensington Health collects PHI for purposes related to:

- an individual's physical or mental health, including the family health history;
- the provision of health care, including the identification of a person as a provider of health care to the individual;
- payments or eligibility for health care, or eligibility for coverage of health care;

- the donation of any bodily substance or derived from the testing or examination of any bodily substance (i.e. blood tests);
- the individual's health insurance number; and
- contacting a person who is acting on an individual's behalf for treatment purposes, or your next-of-kin, if appropriate.

2.3. When PHI that has been collected is to be used for a purpose not previously identified, the new purpose will be identified. Unless the new purpose is permitted or required by law, consent is required before the information can be used for that purpose.

3. PRINCIPLE 3: Consent for the Collection, Use and Disclosure of PHI

3.1. Kensington Health operates within the Circle of Care model. The Circle of Care model means that implied consent is assumed when providing health care or assisting in providing health care.

3.2. Consent is valid under PHIPA if: it is the consent of the individual (or the appropriate SDM); it is knowledgeable; it relates to the information; and it is not obtained through deception or coercion.

3.2.1. Written Consent is required in the following circumstances:

- Where PHI is disclosed to an individual or organization that is outside the Circle of Care;
- Where PHI is disclosed to another healthcare provider or custodian, but the purpose is unrelated to the individual's direct care; and
- Where there are additional uses or disclosures that are not consistent with the purposes for which the information was originally obtained.

3.2.2. Form of Consent

Consent must be obtained in writing and should include the date and time of consent. In exceptional circumstances where verbal consent must be obtained, it must be adequately documented by Kensington Health staff in the individual's electronic medical record (EMR) and/or in the individual's physical file as appropriate.

When seeking an individual's consent, the individual should be informed of the following elements:

- The purpose of the consent and specific PHI data elements involved;
- Any uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought (if the PHI was already collected by Kensington Health);
- Any consequences that may result from withholding consent;
- Any alternatives to providing consent; and
- The source(s) that will be asked to provide the PHI.

3.3. Permissible Forms of Indirect Collection without Consent

3.3.1. The requirement to obtain consent does not apply to collection of PHI in the following exceptional circumstances:

- ***Existing Consent:*** the PHI is to be used or disclosed in accordance with a consent already obtained from the individual
- **Consistent Purpose:** the PHI is to be used or disclosed for a purpose that is consistent with the purpose for which that information was obtained
- **Circle of Care**: the PHI is to be used for purposes as set out in this policy

3.4. Permissible Forms of Use without Consent

3.4.1. Kensington Health may use PHI about an individual without consent for the following purposes:

- For the purpose for which the information was collected and for all the functions reasonably necessary for carrying out that purpose;
- For planning or delivering programs and services;
- Risk management, error management or activities to improve or maintain the quality of care or any related programs or services of Kensington Health;
- Educating agents to provide healthcare;
- Destroying PHI or modifying PHI in order to conceal the identity of the individual;
- A proceeding or contemplated proceeding in which Kensington Health is expected to be party or witness;
- Obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;
- Research, provided all PHIPA requirements are met; or
- If permitted or required by law.

3.5. Permissible Forms of Disclosure without Consent

3.5.1. Kensington Health may disclose PHI without consent if the recipient of the information is within the Circle of Care

3.5.2. Kensington Health may also disclose PHI without consent as set out in PHIPA in exceptional circumstances related to:

- Public interest and grave hazards;
- Health and safety of an individual/risk of serious harm to person or group;
- Legal proceedings;
- Public health authorities;
- Under various legislative instruments; or
- For research purposes, but only if all PHIPA requirements are met.

3.6. Substitute Decision Maker

3.6.1. If Kensington Health believes that an individual is incapable of providing consent, an authorized person, substitute decision maker (SDM), is able to make-a-decision on the individual's behalf, provided that they are legally entitled to do so.

3.7. Consent Directive ("Lock-Box")

3.7.1. An individual has the right to restrict Kensington Health from accessing, using or sharing his or her PHI for the purpose of providing or assisting in the provision of health care.

3.7.2. Kensington Health staff will have the individual of their SDM to fill out a *Lockbox Request Form*, clearly documenting their request and instructions. The completed form will be scanned into the individual's EMR or placed in their physical file.

3.7.3. The CPO will be notified and will ensure that the appropriate safeguards are in place to control the lock-box from being accessed inappropriately. Inappropriate access to the lock-box constitutes a breach of individual privacy.

3.7.4. Any Kensington Health employee receiving such a request from an individual must notify the CPO of that request.

4. PRINCIPLE 4: Limiting Collection of PHI

4.1. Kensington Health limits the collection of PHI to that which is necessary to fulfill the purposes identified and in accordance with the requirements set out in PHIPA.

4.2. PHI is collected directly from the individual, unless the law permits or requires collection from third parties or custodians.

4.3. In connection with any PHI to which Kensington Health has access, Kensington Health shall:

4.3.1. Collect PHI:

- For the purposes of providing or supporting health care to the individual;
- Within the limits of each staff member's employment; and
- As stated in Kensington Health's policies.

4.3.2. Avoid Over-Collection

Where PHI is disclosed to Kensington Health by a third party, such as another healthcare provider and it falls outside the purposes identified for the collection, the Kensington Health CPO will work with the relevant Kensington Health staff to return or destroy the unnecessary PHI, as necessary, so as to avoid over-collecting of PHI.

If Kensington Health receives PHI that does not fall within the intended purpose for collection, the inadvertent disclosure may constitute an incident or breach. This will be investigated on a case-by-case basis led by Kensington Health's CPO with the assistance of the clinical professional involved and legal counsel, where applicable.

5. PRINCIPLE 5: Limiting Use, Disclosure and Retention of PHI

5.1. Use and Disclosure of PHI

5.1.1. Kensington Health uses and discloses PHI for purposes related to:

- An individual's physical or mental health, including the family health history ;
- The provision of health care, including the identification of a person as a provider of health care to the individual;
- Payments or eligibility for health care, or eligibility for coverage of health care;
- The donation of any bodily substance or derived from the testing or examination of any bodily substance (for example, blood tests);
- Relating to the individual's health insurance number; and
- Relating to contacting a person who is acting on your behalf for treatment purposes (or your next-of-kin, if appropriate).

5.1.2. Kensington Health only uses and discloses PHI for the purposes for which it was collected, or as permitted or required by law.

5.1.3. Kensington Health will not use and disclose PHI if other information, namely de-identified or aggregate information, will serve the purpose.

5.1.4. PHI will be retained in the EMR or physical file as required by law. Otherwise it will be securely destroyed, erased, or made anonymous.

5.2. Use of PHI by Kensington Health Staff, Volunteers and Third-Parties

5.2.1. Kensington Health employees, third-parties and volunteers are authorized to access PHI on a need-to-know basis only where required to perform official Kensington Health duties and as per the ***Access Management Policy***.

5.2.2. The CPO will maintain a log of agents who are granted access to PHI.

5.2.3. Kensington Health has appropriate processes and procedures to be followed upon termination or cessation of the employment, contractual, or other relationships to ensure access privileges are terminated and/or Kensington Health property is returned.

5.3. Disclosure of PHI

5.3.1. All disclosures of PHI, including the disclosure of identifiable information, de-identified data or aggregate data, to persons external and internal to Kensington Health must comply with the Corporate Privacy Policy and as required by law.

5.3.2. In the case of any proposed transfer or disclosure of PHI outside of Canada, or access to PHI from a location outside of Canada, all such proposed transfers, disclosures or access must be reviewed by Kensington Health's legal counsel.

5.4. Retention, Destruction and Transfer of PHI

5.4.1. Retention of PHI

Kensington Health retains PHI on both local servers and cloud-based EMR systems. Kensington Health prohibits PHI to be retained on a desktop computer or on any other servers.

If Kensington Health has custody or control of PHI that is the subject of a request for access, Kensington Health shall retain the information for as long as necessary to allow the requestor to exhaust any recourse available. Kensington Health will contact legal counsel to confirm that the right position has been taken.

5.4.2. Destruction of PHI

Kensington Health will ensure that any records (electronic and paper-based) of PHI in their custody or control are disposed of in a secure manner:

- Where further retention of PHI might unfairly prejudice the interests of the individual to whom the information pertains; or
- Where PHI is no longer required for the purpose for which it was obtained or compiled by Kensington Health.

A contract is in place between Kensington Health and the company conducting the destruction of any physical files or documents containing PHI.

Contracts are in place between Kensington Health and the EMR companies to ensure that PHI is destroyed electronically in keeping with this Corporate Privacy Policy and PHIPA.

A PHI destruction log must be maintained by the CPO. The PHI destruction log will be maintained indefinitely.

5.4.3. Transfer of PHI

Kensington Health must ensure that records of PHI in their custody or control are transferred in a secure manner.

Kensington Health remains responsible for any record of PHI, even where the records are being retained by an agent.

6. PRINCIPLE 6: Accuracy of PHI

6.1. Kensington Health must take all reasonable steps to ensure that PHI is as accurate, complete, and up to date as is necessary for the purposes for which it is to be used, including:

- Direct collection or validation with the individual;
- In the case of indirect collection;
- Taking reasonable measures to ensure that the PHI is obtained from a reliable source;
- Before using the PHI, taking measures to verify or validate the accuracy of the PHI against a reliable source where authorized or where consent was obtained; and
- Where Kensington Health validates PHI, documenting the source and/or technique used to validate the PHI.

6.2. Kensington Health will ensure that individuals are given the opportunity to access their own PHI before correcting any inaccurate PHI prior to any decision-making.

6.3. If the individual can demonstrate that the PHI is incorrect or incomplete and provides Kensington Health with the information necessary to correct the record, Kensington Health is obligated to correct the record of PHI.

6.4. Kensington Health does not routinely update PHI, unless this is necessary to fulfill the purposes for which the information was collected.

6.5. Once an individual has terminated its relationship with Kensington Health, Kensington Health will no longer be responsible for keeping the individual's record updated.

7. PRINCIPLE 7: Safeguards for PHI

7.1. General

7.1.1. Kensington Health has physical, administrative and technical systems in place to safeguard PHI in its custody against loss, theft, unauthorized access, disclosure, copying, use, or modification.

7.1.2. The nature of the safeguards corresponds to the sensitivity of the information collected; the amount, distribution and format of the information; and the method of storage.

7.1.3. Kensington Health has implemented security safeguards, which includes but is not limited to:

- Physical measures (i.e. locked filing cabinets, controlled access to offices);
- Administrative measures (i.e. confidentiality agreements, permitting access on a need-to-know basis, privacy training sessions, email confidentiality notice);
- Technological measures (i.e. the use of passwords, encryption, audits and other industry standards).

7.1.4. Kensington Health reviews the practices associated with the secure disposal and destruction of PHI and ensures that unauthorized parties do not access PHI.

7.2. Safeguards for Use and Disclosure

7.2.1. In considering the appropriate safeguards for the retention, use and disclosure of PHI, Kensington Health shall:

- Limit access and use of PHI by administrative, electronic or physical means (as applicable) in order to protect the PHI;
- Employ appropriate measures to ensure that access, use and disclosure of PHI is monitored and documented, which measures must allow for the timely identification of inappropriate or unauthorized access or handling of PHI related to the particular program or activity; and
- Ensure personnel only use PHI for permitted purposes and within the scope of their role at Kensington Health and in accordance with the limits on use and disclosure set out in this Policy.

7.3. Safeguards Regarding Third Parties

7.3.1. When PHI is disclosed to a third-party, Kensington Health shall ensure that:

- For a public sector institution, an agreement or arrangement with appropriate safeguards has been established between Kensington Health and that public sector institution;
- For a private sector organization or third-party service provider, a contract is established with that private sector entity or third-party service provider/contractor outlining measures and provisions to address the following:
  - Control over the PHI;
  - Limitations on collection and handling as well as any prohibitions regarding the PHI for the purposes of the contract;
  - Administrative, technical and physical safeguards; and
  - Obligations of other parties acting on behalf of the third-party service provider.

7.4. Privacy Education and Training

7.4.1. Kensington Health shall ensure that it provides annual training to its staff.

7.4.2. Kensington Health's Chief Privacy Officer is also responsible for ongoing privacy awareness, reminders and updates to all Kensington Health staff members, agents, volunteers and third-party service providers.

7.4.3. The CPO is responsible for reviewing privacy training materials and updating such materials on a regular basis; at least annually.

7.4.4. The CPO shall ensure that employees of Kensington Health receive privacy training in the following areas:

- Application of PHIPA, including:
  - The purpose of PHIPA,
  - The applicable definitions (collection, use, disclosure, retention, and destruction),
  - Their responsibilities, including the principles for assisting requesters of records,
  - Delegation, exemption decisions and the exercise of discretion,
  - The requirement to provide complete, accurate and timely responses, and
- Sound privacy practices for the creation, collection, retention, validation, use, disclosure and disposition of PHIPA;
- Specific policies, processes and protocols related to the administration of PHIPA, including policies on management of information and violation of PHIPA.

7.5. Sanctions for Inappropriate Use of PHI

7.5.1. Employees who use PHI inappropriately are subject to disciplinary action on a case by case basis as determined by Kensington Health.

7.6. Information Security

7.6.1. Kensington Health has practices in place for information security (which includes but is not limited to, network resources, desktop computers, mobile computing devices and wireless data transmission) including the requirement for all information security related devices to be encrypted, as needed.

7.6.2. Practices include, but are not limited to:

- Ensuring that no PHI is stored on the desktop;
- Ensuring that only the minimum amount of PHI required is stored;
- Using appropriate secure passwords at all times for mobile computing devices, desktop computers and any other device that may store PHI and other sensitive information;
- Incorporating time-out applicability for screens and adding lock functions for all required devices;
- Ensuring that devices containing PHI are always stored in a secure location only accessible to the user; and
- Having sufficient physical controls as required (i.e. keys to areas where PHI is stored and locked cabinets).

7.7. Mobile Computing

7.7.1. Employees or agents of Kensington Health are not allowed to store any data on their own personal mobile device.

7.7.2. It is the duty of each employee and agent of Kensington Health to follow this rule.

7.8. Emails

7.8.1. Kensington Health has a secure messaging platform (end-to-end encryption) for all email messaging, including between Kensington Health and other HICs and between Kensington Health and its individuals.

7.8.2. Employees and agents of Kensington Health must not send PHI on their own personal email.

7.8.3. This rule applies to the use of all email services at Kensington Health, including those accessed remotely or through webmail.

7.9. Privacy Incidents and Breaches

7.9.1. Privacy breaches include any inadvertent or intentional theft or loss of PHI; unauthorized collection, use or disclosure of PHI; unauthorized modification or destruction of PHI; or any non-compliance with this Policy or other privacy-related policies, procedures and protocols.

7.9.2. In the event of an actual or suspected privacy incident or breach, Kensington Health staff must comply with all applicable policies and laws.

7.9.3. If a privacy incident or breach occurs, staff are obligated to notify the Chief Privacy Officer immediately.

7.9.4. The Privacy Officer of each HIC is responsible for leading and adhering to any applicable law, which can include, but is not limited to:

- Containment - to ensure that steps are taken to protect PHI from further theft, loss or unauthorized use or disclosure and to protect records of PHI from further unauthorized copying or disposal;
- Notification - to notify affected individual(s) at the first reasonable opportunity and include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under PHIPA;
- Investigation - conduct an investigation of the breach including a review of all relevant information systems and policies, practices and procedures (setting out the scope of the investigation and the process to be followed in the investigation); and
- Remediation: discipline and notifying/reporting to the IPC; communicate and implement findings of the investigation, including any recommendations.

7.9.5. Any third-party service provider who may have access to PHI must sign a service agreement with Kensington Health to make them aware of their privacy responsibilities, including with respect to breaches.

Notification Requirements to the IPC

7.9.6. Kensington Health will report the following categories of breaches to the Commissioner:

(1) Use or disclosure without authority (but not if the breach is accidental)
(2) Stolen information (but not if the stolen information was de-identified or properly encrypted)
(3) Breach results in further use or disclosure without authority
(4) Patterns of similar breaches
(5) Disciplinary action against a college member
(6) Disciplinary action against a non-college member
(7) Significant breach

Notification Requirements to the Governing Regulatory College

7.9.7. Kensington Health must give written notice of any of the following events to the governing Regulatory College within 30 days of the event occurring:

- The regulated health professional is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of PHI.
- The regulated health professional resigns and Kensington Health has reasonable grounds to believe that the resignation is related to an investigation or other action with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of PHI.

Follow-up Recommendations:

7.9.8. Upon the completion of the investigation of the privacy incident or breach, the CPO will make recommendations to prevent recurrence in conjunction with Privacy Officers and the Privacy Committee.

7.9.9. The HIC Privacy Officer shall maintain a log of all incidents or breaches.

7.10. Privacy Logging, Monitoring and Auditing

7.10.1. Kensington Health has implemented measures necessary to ensure that it is able to audit all instances in which individuals access PHI found in paper records.

7.10.2. Kensington Health's EMR systems also provides logging, monitoring and auditing capabilities. Kensington Health periodically monitors and audits instances where individuals access PHI on its electronic information systems.

7.10.3. Kensington Health's EMR systems also logs all instances where all or part of the PHI is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag.

7.10.4. The CPO will maintain a log of when he or she audits the EMR system to review how individuals access PHI on its electronic information systems.

7.11. Privacy Impact Assessment (PIA)

7.11.1. A PIA is Kensington Health's organizational risk management tool and process used to identify the effects of a given process or activity on an individual's privacy. PIAs also serve to identify any risks to Kensington Health.

7.11.2. Currently Kensington Health conducts PIA's as per its ***Privacy Risk Management Policy***. All risks identified in PIAs will be recorded in a privacy risk register.

8. PRINCIPLE 8: Openness about PHI Policies and Practices

8.1. Information about Kensington Health's policies and practices relating to the management of PHI are publicly available, including:

- contact information for the Kensington Health Chief Privacy Officer, to whom complaints or inquiries can be made;
- how to access PHI held by Kensington Health, and making requests for correction;
- a description of the type of PHI held by Kensington Health, including a general account of its use and disclosures; and
- posters that explain Kensington Health's privacy practices.

9. PRINCIPLE 9: Individual access to PHI

9.1. Kensington Health will respond to an individual's request within reasonable timelines and costs to the individual, as governed by PHIPA. Kensington Health will take reasonable steps to ensure that the requested information is made available in a form that is understandable.

9.2. An individual who successfully demonstrates the inaccuracy or incompleteness of his or her PHI may request that Kensington Health amend his or her information.

9.3. Access to PHI

9.3.1. Any individual has the right to access their PHI under the control of Kensington Health. This is subject to certain limited and specific exemptions as set out in this Policy.

9.3.2. Access requests can be formal or informal. If the requestor provides a formal written request for access, it will fall under PHIPA and all requirements and timelines set out in the legislation and the ***Personal Health Information Policy*** must be met.

9.4. Correction

9.4.1. Requestors are entitled to seek to correct any PHI which they believe to be inaccurate or incomplete. Requestors have the right to:

- request the correction of the PHI where he or she believes there is an error or omission therein;
- require that a notation be attached to the information reflecting any correction requested but not made;
- in the case of the previous disclosure of the information for an administrative purpose, require that any recipient within 2 years prior to the time of the correction or notation be notified of the correction or notation.

9.5. Processing Requests for Correction

9.5.1. Kensington Health must, within the days set out in PHIPA (a maximum of 30 days), process the written request and give a written notice to the requestor. The time allowed for processing a request for correction is counted from the receipt of a complete request, with the day after receipt being counted as day one.

9.5.2. Kensington Health shall ensure that any decision to respond to a correction request is made by the related Privacy Officer in collaboration, with legal counsel if applicable. Under the guidance of the Chief Privacy Officer, Kensington Health shall review all correction requests. Each correction request shall be assessed on its own merits.

9.6. Extensions of Time

9.6.1. Kensington Health may extend the time limit for processing correction requests beyond the period if:

- processing the request within the time limit would unreasonably interfere with Kensington Health's operations, or
- external consultations are necessary to comply with the request that cannot reasonably be completed within the time limit, in which case the time limit may be extended for the number of days set out in PHIPA.

9.6.2. If the time limit for processing a correction request is extended, Kensington Health shall notify the requestor of the extension before expiration of the initial time period.

9.7. Determining Correction Requests and Response to Requestor

9.7.1. Kensington Health is obligated to correct PHI where an individual, to the satisfaction of Kensington Health, confirms that the record is in fact inaccurate or incomplete and the individual gave the necessary information to Kensington Health to correct the record.

9.7.2. Kensington Health may refuse to correct PHI that it did not create or that is a professional opinion or an observation of a health care provider.

9.7.3. If a correction is refused on such a basis, Kensington Health will inform the individual of the refusal, the reasons for the refusal and the individual's right to file a complaint regarding the refusal to the IPC.

10. PRINCIPLE 10: Challenging compliance with Kensington Health' Privacy Policy and Practices

10.1. Any individual may submit a concern or complaint concerning compliance with this Policy to:

Chief Privacy Officer
25 Brunswick Ave
Toronto ON | M5S 2L9,
privacy@kensingtonhealth.org, or 1-437-828-9300.

10.2. Kensington Health will also investigate and respond to complaints or inquiries and inform individuals who make inquiries or lodge complaints of other available complaint procedures.

10.3. A log of complaints will be maintained by the Chief Privacy Officer.

10.4. If a complaint is found to be justified, Kensington Health will take appropriate measures to rectify the matter.

10.5. A person may also submit a concern or complaint to the Information and Privacy Commissioner of Ontario by contacting:

Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON | M4W 1A8
Phone: 416-326-3333 or 1-800-387-0073

DEFINITIONS

Agent:
Means any person who is authorized by Kensington Health to perform services or activities on behalf of Kensington Health with respect to PHI for the purposes of Kensington Health, and not the agent's own purposes, whether or not the agent has the authority to bind Kensington Health, whether or not the agent is employed by Kensington Health and whether or not the agent is being paid by Kensington Health. Kensington Health' agents could include: employees, volunteers, consultants, vendors, contractors, and any other person working on behalf of Kensington Health.

Circle of Care:
The ability of certain HICs to assume an individual's implied consent to collect, use or disclose PHI for the purpose of providing health care to that individual.

Collect:
To gather, acquire, receive or obtain PHI by any means and from any source.

Consent:
Voluntary agreement to the collection, use or disclosure of PHI for defined purposes. Consent can be either *express* or *implied* and can be provided directly by the individual or by a personal representative.

Consent directive:
The express instruction of an individual not to use or disclose his or her PHI by either expressly withdrawing or withholding consent. It is commonly referred to as the "lock-box" for the purposes of PHIPA.

Disclose:
To make PHI available or to release it to a third party or to another person.

Express consent:
Can be given orally, electronically or in writing. Referred to as simply 'Consent' throughout all privacy policies and procedures.

Kensington Foundation:
Not-for-profit charitable foundation that provides financial support to the programs and services delivered by Kensington Health

Health information custodian (HIC):
A person or organization listed in PHIPA that, as a result of his, or her or its power, duties or work, has custody or control of personal health information.

Identifying information:
Information that identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

Implied consent:
Consent that can be reasonably inferred from an individual's action or inaction.

Kensington Health:
Which includes a group of affiliated programs including, but not limited to, The Kensington Eye Institute (including The Kensington Vision & Research Centre, The Kensington Cancer Screening Clinic and The

Kensington Diagnostic Imaging Centre), The Kensington Health Centre (including Kensington Gardens, The Second Mile Club, and The Kensington Hospice), The Kensington Research Institute and The Eye Bank of Canada (collectively all of the foregoing shall be referred to as, “Kensington Health”. “we,” “us” and “our”).

PHIPA:
The Personal Health Information Protection Act, 2004 and any regulations thereunder.

Personal Health Information (PHI):
Personal Health Information means identifying information about an individual in oral or recorded form, if the information is about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision-makers on behalf of the individual.

Personal Information (PI):
Any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title, business contact information or job description.

Privacy breach:
Any inadvertent or intentional theft or loss of PHI; unauthorized collection, use or disclosure of PHI; unauthorized modification or destruction of PHI; or any non-compliance with this Policy or other privacy-related policies, procedures and protocols.

Research:
Means a systematic investigation designed to develop or establish principles, facts, or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.

Substitute decision-maker:
A person who is authorized under PHIPA to consent on behalf of the individual to the collection, use or disclosure of personal health information about the individual

Third party service providers:
Means a person, institution, corporation or other entity providing services to Kensington Health and accessing or potentially accessing PHI.

Use:
To handle or deal with PHI in the custody or control of Kensington Health, but does not include the sharing of the PHI with third-parties external to Kensington Health (this is a disclosure). Sharing of PHI between Kensington Health and an agent of Kensington Health is a use of PHI, not a disclosure.

COMPLIANCE

Kensington Health's Chief Privacy Officer is responsible for protecting the collection, use and disclosure of personal health information. Any questions about this policy and procedure should be directed to:
Chief Privacy Officer
25 Brunswick Avenue Toronto ON M5S 2L9
privacy@kensingtonhealth.org or 1-437-828-9300

SUPPLEMENTAL INFORMATION

Cross Reference:
CORP-CPS-03.001a Lockbox Request Form
CORP-CPS-03.001b Terms of Reference - Privacy Committee
CORP-PRI-01.001 Access Management Policy

CORP-PRI-03.001 Confidentiality Policy
CORP-PRI-03.003 Computer Access, Information Security & Internet System Use
CORP-PRI-03.004 Consent Management Policy
CORP-PRI-04.001 Device Loan Policy
CORP-PRI-05.001 Employee & Agent Privacy Policy
CORP-PRI-05.002 Electronic Medical Record Policy
CORP-PRI-14.001 News Media & Photography Policy
CORP-PRI-16.001 Personal Health Information Policy
CORP-PRI-16.002 Privacy Breach Management Policy
CORP-PRI-16.003 Privacy Education & Training Policy
CORP-PRI-16.005 Privacy Risk Management Policy
CORP-PRI-18.001 Research Privacy Policy
CORP-PRI-18.002 Retention & Destruction of PHI Policy
CORP-PRI-19.001 Social Media Policy
CORP-PRI-19.002 Service Provider Agreement Policy
CORP-PRI-22.001 Video & Electronic Surveillance Policy

Source

The Personal Health Information Protection Act (PHIPA), 2004
The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000
Canadian Standards Association Model Code for the Protection of Personal Information
Information and Privacy Commissioner of Ontario (IPC)
Long-Term Care Homes Act, 2007
Home Care and Community Services Act, 1994
Independent Health Facilities Act
Health Care Consent Act, 1996
Trillium Gift of Life Network Act, R.S.O.1990

End Notes

[1]PHIPA SS.3 (1)4(ii)
[2]PHIPA SS.3 (4)7(vii)
[3]PHIPA SS.3 (1)2
[4]PHIPA SS.3 (1)4(i)