Privacy & Confidentiality of Information

1.0 Introduction

In the course of carrying out its patient care, research, teaching and administrative functions, the Hospital for Sick Children (SickKids or the Hospital) may process PI and PHI relating to its patients, research participants, families, visitors, donors, staff, contractors, etc. within its custody and control. SickKids is firmly committed to protecting and preserving all personal information (PI), personal health information (PHI) and other confidential information that is collected, used, disclosed, and retained under its custody and control**.**

SickKids' obligations regarding PHI and PI are outlined in the following two pieces of provincial legislation: the Personal Health Information Protection Act, 2004 (PHIPA), and the Freedom of Information and Protection of Privacy Act, 1990 (FIPPA), respectively. Regulated professionals may have additional privacy obligations as set out by their professional college.

This policy is based on ten internationally recognized standards, called the privacy principles, which have been adopted as the basis for Canadian privacy statutes and regulations. The ten privacy principles are:

1. Accountability
2. Identifying Purposes for Collection
3. Consent for Collection, Use, and Disclosure
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness about Information Policies and Practices
9. Individual Access
10. Challenging Compliance

2.0 Definitions

Agent: an agent is defined in relation to a Health Information Custodian, and means a person who acts for, or on behalf of the custodian with appropriate authorization. An agent is acting for the purpose of the custodian, and not for their own. Agents are also included in the definition of “Staff” below.

Collection: The process of gathering, acquiring, receiving, or obtaining personal information, personal health information or private and confidential information, whether directly from the person or patient, or from any other source such as tests, images, samples, specimens, or other care providers. Generally, information is considered to be *collected* the first time SickKids gathers, acquires, receives, or obtains the information. Once collected, any further access, viewing, handling or otherwise dealing with the information is generally considered to be a *use*.

Confidential Information: Confidential information is all information of a sensitive nature in any format, which is created, received, or disclosed by SickKids during its business, including corporate and proprietary information, and physical and electronic records in the custody of agents retained by SickKids. Confidential information is

categorized into one of three security levels: high sensitivity, moderate sensitivity or low sensitivity. More information on the levels can be found in the Information Security policy.

Consent: Voluntary agreement with what is being done or proposed. Consent can be “express” or "implied". Express consent is the explicit indication of agreement and can be given orally or in writing. Express consent for the collection, use or disclosure of PHI, whether it is obtained verbally or in writing, must be documented and retained in the patient’s health record. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual and the facts of a particular situation. Consent, whether express or implied, must be knowledgeable; related to the information that will be collected, used, or disclosed; and not be obtained through deception or coercion. For consent to be knowledgeable, the consenting individual must understand the purpose of the collection, use or disclosure and know they can choose to give or withhold consent.

Digital Solution: Digital Solutions include both hardware and software solutions and services, including virtual care platforms, wearable devices, virtual reality, and databases for the collection, use, and disclosure of Identifying Information. These can include web-based applications as well as mobile apps.

Direct Identifier: Information that is unique to a single individual and can be used to identify them, either by itself or in combination with other readily available sources of information. Examples include an individual’s name, email address or health card number.

Disclosure: To make information available or to release it to another person, organization or health information custodian outside of the organization.

Executive Sponsor: Individual at the senior management level who is responsible for providing strategic direction, allocating resources, and ultimately responsible for the initiative's success. Executive Sponsors must ensure digital solutions are configured and used in compliance with internal policies, laws and regulations.

Health Information Custodian (HIC): a health information custodian is a person or organization described in PHIPA who has custody or control of personal health information as a result of or in connection with performing the person’s or organization’s powers or duties or the work. For the purpose of this policy, health information custodian has the same meaning as defined in Section 3 of PHIPA. SickKids is a HIC.

Identifying Information: Identifying information is information, for which it is reasonably foreseeable in circumstances, that can be used, on its own or with other information, to help identify an individual. Simply put, it is any information related to an identifiable person. Identifying information can include direct or indirect identifiers or a combination of the two.

Indirect Identifier: Information that is not unique to a single individual on its own but, when combined with other indirect identifiers, can be used to identify an individual. Examples include age, height, highly visible characteristics of the individual (ethnicity or race), etc.

Patient: Throughout this document, “patient” is understood to mean either the patient or, if applicable, a person legally authorized to make decisions on the patient’s behalf, such as the substitute decision maker (SDM).

Personal Health Information (PHI): Oral or recorded identifying information about someone that is related to a person’s physical or mental health or family history or health care an individual receives, including who provided the health care. For the purpose of this policy, personal health information has the same meaning as defined in Section 4 of PHIPA.

Personal Information (PI): Recorded information about an identifiable individual. For the purpose of this policy, personal information (PI) has the same meaning as defined in Section 2 of FIPPA.

Privacy: The right of individuals to control when, how, and to what extent their personal information is collected, used and disclosed, and ensure its security from unauthorized use or disclosure.

Privacy Breach: A privacy breach happens when personal health information or personal information is collected, used, disclosed, or disposed of in a way that does not comply with PHIPA or FIPPA.

Process: A general term used to describe how information is handled and includes the collection, retention, storage, use, access, disclosure, and destruction of information.

Staff: Refers to all hospital employees, volunteers, Agents, members of the medical, dental, nursing or professional staff of the Hospital, trainees including post-doctoral fellows, as well as housekeeping staff, students and volunteers who are employed by, work at, or are receiving training at SickKids, or are otherwise carrying out activities on behalf of SickKids.

Use: To view, handle, modify or otherwise deal with information. Access to and the act of de-identifying information is considered a "use" under PHIPA.

3.0 Policy

This policy applies to all SickKids staff, vendors, contractors, consultants, agents, and related entities who, on behalf of or for the purposes for or benefit of SickKids, collect, use, disclose or have access to PI and/or PHI, as defined above, which is in the custody or control of SickKids. Individuals who fall into these groups must respect the privacy rights of individuals and maintain the confidentiality and security of sensitive information to SickKids' standards. This is consistent with and supplementary to any applicable professional "codes of conduct" or "codes of ethics". Professional staff are additionally governed by their professional standards for privacy and confidentiality. Managers are accountable for ensuring staff receive proper training on this and other privacy-related policies and how to apply these policies in their day-to-day work.

3.1 Employee Privacy
This policy also applies to the collection, use, and disclosure of employee personal information. SickKids is committed to protecting the privacy of its employees. Employee personal information will only be collected, used, and disclosed as required in the course of hiring, employment, and termination processes. Employees who have requests or concerns regarding their SickKids employee records should contact the Privacy Office. SickKids may electronically monitor employees' online activities as described in the SickKids Electronic Monitoring policy.

4.0 Guidelines

SickKids will conduct itself according to the following privacy principles.

Principle 1 – Accountability
SickKids is responsible for PI/PHI under its custody and/or control and has designated a privacy officer to be accountable for its compliance with these principles, internal privacy policies and privacy laws. The privacy officer's duties may include:

- facilitating the hospital's compliance with privacy laws and regulations, including PHIPA and FIPPA, internal policies;
- updating/revising privacy policies and procedures as required;
- advising staff on matters impacting the privacy of individuals;
- conducting privacy impact assessments and privacy audits of information use;
- periodic assessing of the hospital's information collection, use and disclosure practices;
- responding to inquiries from the public about the hospital's information practices; and

- responding to requests to access information in the hospital's custody and/or control, and process individual requests for correction of a record of personal health information.
- The Privacy Officer can be contacted via email at Privacy.Office@SickKids.ca.

Privacy Office staff at SickKids may act on behalf of the privacy officer.

Principle 2 – Identifying Purposes for Collection

SickKids, at or before the time PI/PHI is collected, will identify the purposes for which it collects information through a notice of collection, or with express consent, where required by statute. The main purposes are:

- the delivery of patient care;
- the administration and management of the hospital, including the hiring and credentialing of staff;
- to conduct approved research;
- to compile statistics; and
- to ensure compliance with legal and regulatory requirements.

All notices shall be clear, specific and reviewed periodically to ensure currency and accuracy.

Collection of PI/PHI for Research:

Collection of PI/PHI for research must be approved by the SickKids Research Ethics Board or delegated REB of Record to ensure the highest ethical standards of consent, use, and disclosure. See the Free and Informed Consent in Research document for more information.

Principle 3 – Consent for Collection, Use, and Disclosure

SickKids maintains extensive procedural guidance governing consent through the Consent to Treatment policy which is incorporated into this policy by reference, and which should be consulted for specific instances of SickKids obligations regarding the obtaining of patient consent for the use or disclosure of their personal information during and after the regular course of patient care. obligations regarding the obtaining of patient consent for the use or disclosure of their personal information during and after the regular course of patient care.

The consent of the individual or substitute decision-maker (SDM) is required for the collection, use or disclosure of their PI/PHI, except where it may be inappropriate to seek consent due to legal, medical or security reasons. SickKids will make reasonable efforts to ensure that individuals are advised orally or in writing (through the use of website notices, signs and consent forms) about the collection, use or disclosure of their PI/PHI. If SickKids requires the consent of an individual or SDM, it must meet the following legal requirements:

1. The consent must be of the appropriate person;
2. The consent must be knowledgeable. This means that the individual must know the purposes of the collection, use, or disclosure as described in this policy;
3. The consent must not be obtained through deception or coercion;
4. The individual must be given the option to withdraw consent, but the withdrawal will only be on a going-forward basis.

Indirect Collection

SickKids will endeavor to collect all personal health information about an individual directly from the individual except as otherwise consented to by the individual (e.g., through a SDM), or as permitted or required by law. Indirect collection is not permitted except in limited circumstances: where the information to be collected is necessary for providing patient care and it is not reasonably possible to collect directly from the individual in an accurate or timely fashion, SickKids will collect the information from another person or entity permitted to disclose the information.

Collection for New Purposes:

If PI/PHI that has already been collected is to be used for a purpose not previously identified, the consent of the individual will be obtained, unless the new purpose is permitted or required by law. For example, if information was collected for the provision of care and will be used for research, consent is generally required.

Consent Directives:
PHIPA permits SickKids to assume an individual's implied consent to collect, use or disclose the individual's PHI for the purpose of providing or assisting in the provision of care to the individual, unless the individual has expressly withheld or withdrawn such consent. A disclosure includes healthcare institutions outside of Canada where an individual is receiving care.
If an individual has expressly withheld or withdrawn consent to use or disclose their PHI, staff are not permitted to use (i.e., view, modify, etc.) the information for the purpose of providing or assisting in the provision of care, unless:

- the staff member has obtained express consent from the individual; or
- it is an emergency **and** express consent cannot be obtained in a timely manner.

See the Lockbox policy for more information.

Principle 4 - Limiting Collection
SickKids will only collect PI/PHI by fair and lawful means, and:

1. limit its collection of PI/PHI to that which is necessary for a lawful purpose identified by SickKids;
2. not collect more PI/PHI than is reasonably necessary for the purpose; and
3. will not collect PI/PHI if non-identifying information will serve the purpose.

Principle 5 – Limiting Use, Disclosure, and Retention
SickKids will not process, retain, or disclose PI/PHI for purposes other than those for which it was collected, except with consent or as required by law. SickKids will:

1. limit its use, disclosure and retention of PI/PHI to that which is necessary for a lawful purpose identified by SickKids;
2. not use, disclose, and retain more PI/PHI than is reasonably necessary for the purpose; and
3. not use, disclose, and retain PI/PHI if non-identifying information will serve the purpose.

Staff are accountable for ensuring sensitive information is only used and disclosed for authorized purposes and to authorized individuals. Staff may not use (i.e., access, view, handle) PI/PHI unless they have a legitimate clinical or business "need to know" directly related to their role and responsibilities at SickKids. If in doubt, staff should ask their supervisor or contact the Privacy Office. See the Disclosure of Personal Health Information policy for more information. Only the Health Information Management department can authorize the removal of any original hard copy charts from SickKids premises.

Use of PHI for Education Purposes
Access to and use of PHI for purposes related to educating staff on the provision of health care is a permitted use under PHIPA. However, SickKids requires the establishment of a need to know the information, and oversight (i.e., approval) from a supervisor *before* accessing/using PHI for this purpose. This applies to all staff unless the primary purpose of your role is educating staff on the provision of health care (e.g., Nurse Educator). Engaging in self-guided learning initiatives without prior approval is not permitted. Note: PHIPA does not permit the collection or disclosure of PHI for education purposes.

Use/Disclosure of PHI for New or Secondary Purposes:
PI/PHI will not be used or disclosed for purposes other than those for which it was collected, except with the express consent of the individual or as permitted or required by law. For example, PHI may be used for Research if it has been approved by the SickKids Research Ethics Board or delegated REB of Record. See the Research Involving Participants for more information.

De-identification of PI/PHI

SickKids may use PI or PHI to de-identify or anonymize it. We may also engage with vendors to perform this task on our behalf and they may use the de-identified data for their own purposes. De-identification involves modifying the information to remove identifying features or details. De-identified information may be used for non-care purposes, such as quality improvement initiatives at SickKids. SickKids will take steps to mitigate risks associated with the potential re-identification of PI and PHI. For instance, SickKids' contracts require all persons using and/or receiving de-identified information to adhere to this privacy policy and acknowledge that they are prohibited from making any attempts to re-identify the individual whose information was de-identified. If you are engaging with a vendor who will access the data and wants to use it for their own purposes, reach out to Legal Services.

Minimum Retention of PI
FIPPA requires that personal information used by SickKids be retained for at least one year following its last use. See the Records Creation, Retention and Destruction policy for more information.

Use of Social Media Platforms and PHI
SickKids Staff are prohibited from posting or sharing any PHI on social media platforms. Patient information, with or without the patient's name and including photos or videos, is never to be posted on or referred to on any public forum, including websites, blogs and social media without expressed and documented consent. If Staff members wish to share any information, they should consult the Communications and Public Affairs office. See the Use of Social Media Platforms by Staff policy for more information.

Principle 6 - Accuracy
SickKids will take reasonable steps to ensure PI/PHI in our control is as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used or disclosed. SickKids may only disclose inaccurate, incomplete or outdated PI/PHI if, at the time of the disclosure, the limitations on the accuracy, completeness or up-to-date character is clearly set out for the recipient. The extent to which PHI is required to be accurate and up-to-date depends on the purposes of the information. SickKids does not undertake efforts to update PHI unless such a process is necessary to fulfill the purposes for which the information was collected.

Principle 7 - Safeguards
SickKids must take steps that are reasonable in the circumstances to ensure that PI/PHI is protected against theft, loss and unauthorized use or disclosure. These safeguards will be reasonable in the circumstances and commensurate to the level of risk. SickKids uses the following categories of safeguards to protect information:

- physical safeguards (e.g., locking filing cabinets and rooms);
- administrative safeguards (e.g., policies, contracts, privacy training, etc.); and
- technical safeguards (e.g., multifactor authentication, encryption, audits, etc.).

SickKids will protect PI/PHI regardless of the format in which it is held.

Mandatory Annual Privacy Training and Confidentiality Attestation
SickKids requires all staff, students, and volunteers to complete privacy and security training during orientation and annually thereafter as a condition of employment. Upon successful completion of the training, staff must complete a confidentiality pledge.

Privacy Reviews of Digital Solutions Processing Identifying Information
The Privacy Office advises on the procurement, configuration and implementation of digital solutions (or new features for existing applications like Epic) when the solutions are intended to include employee information, personal information and/or personal health information. We support this by:

- Providing and rating mandatory and rated privacy criteria for RFPs;
- Assessing vendors/solutions during procurement;
- Conducting and disseminating privacy impact assessments (PIA);
- Supporting communications with external PIA consultants; and
- Working with teams to mitigate privacy risks before going live.

Executive Sponsors of a Digital Solution must contact the Privacy Office to determine whether the Privacy Office needs to review the Digital Solution prior to implementation. To help determine whether the Privacy Office should be engaged, Executive Sponsors can complete the Privacy Review Needs Assessment for Digital Solutions. If a privacy review is required, Executive Sponsors must complete the Privacy & Information Security Intake Form For Digital Solutions form. The Privacy Office will determine the need for a privacy impact assessment (PIA) based on factors like the sensitivity of the information, the amount of information that will be processed, if SickKids is a Health Information Network Provider under PHIPA, etc. The PIA will assess whether there are adequate physical, administrative and/or technical safeguards. Where a Digital Solution has been implemented without input from the Privacy Office, contact the Privacy Office immediately.

Once a Digital Solution is implemented, Executive Sponsors must contact the Privacy Office if there will be substantive changes to the solution that would change our understanding of it. This may include the processing of new or additional identifying information; new integrations; or the introduction of new functionality.

Staff Obligation to Report Privacy Incidents
Staff are required to report privacy incidents to the Privacy Office. Incidents may include suspected or actual breaches of privacy laws, internal privacy policies, contractual obligations, etc. Reports can be made directly to Privacy.Office@SickKids.ca; through the Safety Reporting System under "Privacy/Confidentiality" (see the Safety Reporting policy) or through the hospital's Whistleblowing System. Incidents will be reviewed by the Privacy Office and will be dealt with in accordance with established SickKids practices. The manager of the responsible area or individual named may be contacted in order to help manage the breach. Any SickKids staff whose action results in an unauthorized collection, use or disclosure of PI/PHI may be subject to sanctions (see Appendix 1).

Information Security
Details and procedures for ensuring security of information can be found in the Information Security policy.

Disposal and Destruction of PI/PHI
Care will be used in the disposal or destruction of PI/PHI, to prevent unauthorized parties from gaining access to the information. Details on secure retention and destruction of PI/PHI can be found in the Records Creation, Retention and Destruction policy.

Principle 8 - Openness about Information Policies and Practices
SickKids will make readily available to individuals specific information about its information management policies and practices. SickKids does this through a written statement made available to the public. This statement will include a description of:

- the ways and reasons PI/PHI is collected, used and disclosed;
- descriptions of shared electronic systems through which PI/PHI may be disclosed;
- how individuals can obtain access to or request correction of their information;
- how to contact the SickKids Privacy Office for questions or complaints about how data is managed; and
- a description of how to make a complaint to the Information and Privacy Commissioner of Ontario.

Individuals will be able to acquire this information without unreasonable effort and will be made available in a form that is generally understandable. New SickKids staff and any other individual doing work at SickKids will be made aware of and be subject to this policy during their orientation.

Principle 9 - Individual Access
Upon request, an individual or SDM of that individual will be informed of the existence, use and disclosure of their PI/PHI in the custody/control of SickKids and will be given access to it. SickKids will respond to such requests within 30 days and at minimal or no cost to the individual. SickKids will be provided in a clear and readable format to the individual.

Staff Access to Their Own PI/PHI and PI/PHI of Personal Associates

Staff who have authorized access to clinical and/or corporate systems are prohibited from accessing their own information or information belonging to a personal associate unless the purpose is directly related to the staff's role and responsibilities at SickKids. Staff wishing to access their, or their family's information, must request access through existing practices. For example, requests to access PHI can be directed to Health Information Management and managed according to requirements outlined in PHIPA. Access to PHI may also be obtained through MyChart, the hospital's patient portal.

Auditing and Monitoring Access to PHI Program
SickKids will take reasonable steps to ensure that processes are in place to review system control and audit logs to detect and deter unauthorized use or access to PHI. The Privacy Office may monitor use of any of its Digital Solutions but conducts regular audits in the hospital's electronic medical record, Epic. Audits include proactive audits (e.g., random patient and same last name) and reactive audits (e.g., consent overrides, high profile patients, in response to allegations and/or complaints). We follow the Ontario Hospital Association guidance and schedule when conducting audits.

Executive Sponsors are responsible for ensuring the requirements of audit logs below are in place for all Digital Solutions in their portfolio.

Requirements of Audit Logs
These audit logs **must** capture the following information:

1. the **type of information** that was viewed, handled, modified or otherwise dealt with;
2. the **date and time** on which the information was viewed, handled, modified or otherwise dealt with;
3. the **identity of all persons** who viewed, handled, modified or otherwise dealt with the PHI; and
4. the **identity of the individual** to whom the PHI relates.

Digital Solutions that do not or cannot comply with the above, must be reviewed by the Privacy Office.

If the criteria below are met, Executive Sponsors are responsible for conducting regular audits for the Digital Solution. Executive Sponsors must contact the Privacy Office for guidance on creating auditing protocols for the specific Digital Solution.

Requirements for Conducting Audits
Auditing protocols must be put in place for all Digital Solutions that meet the following criteria:

- contains PHI; **and**
- facilitates general user-based access, that does not include "super-users" (e.g. IT administrators); **and**
- allows a record or part of a record of PHI to be viewed, handled, modified or otherwise dealt with; **and**
- includes at least one of the features below:
    - has non-SickKids users (i.e., used by users who are not SickKids staff); **or**
    - has more than 10 internal users (i.e., users who are SickKids staff); **or**
    - includes PHI for more than 20 patients; **or**
    - includes more than 5 direct identifiers belonging to an individual.

Access to PHI for Inpatients
When a request is made to access the chart of an inpatient, the process may be facilitated by any staff member. Staff will direct requesting individuals to complete a Request of Information (ROI) form to be submitted to Health Information Management (HIM). HIM can provide a copy of the available medical records on file. SickKids may offer to have a clinical member of staff meet with the patient or family to review the requested information. Individuals may also make a formal FOI request for access to their PI under FIPPA. See the Disclosure of Personal Health Information and Freedom of Information policies for more information.

Denying Access to PI/PHI
In certain situations, SickKids may not be able to provide access to any or all of the PI/PHI it holds about an individual. Access to information may be denied where an exception applies under FIPPA or PHIPA. Exceptions are limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions in the case of PHI may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation purposes.

Principle 10 - Challenging Compliance
An individual will be able to challenge SickKids' compliance to the above principles to its Privacy Officer. The privacy officer, or delegate, will investigate all complaints. If a complaint is found to be justified, SickKids will take appropriate measures. Complaints may also be made directly to the Office of the Information and Privacy Commissioner of Ontario.

Challenging Accuracy of Records of PHI
An individual can challenge the accuracy and completeness of their PHI and have it amended as appropriate. Amendments of PHI will generally not involve deletions or alterations of the original record but would take the form of addendums to the record. Where appropriate, the amended information will be shared with third-parties who have access to the information. When a challenge is not resolved to the satisfaction of the individual, the hospital will record the substance of the unresolved challenge.

If an individual believes their PHI in a SickKids record is incorrect, they can request a correction. If SickKids disputes the correction, the individual shall have an opportunity to provide the Hospital with a statement of disagreement that shall be attached to the record. Authorized staff must read and disclose this statement when accessing or sharing the related information.

Correcting/Amending Other Records
Employees wishing to correct or amend their records of PI should reach out to their manager or Human Resources. Other individuals wishing to correct or amend their information should email privacy.office@sickkids.ca.

5.0 Related Documents

The following section identifies policies and other guidelines that should be followed to ensure compliance with the ten privacy principles.

Principle 1 - Accountability
Code of Conduct
Observers
Responsible Conduct of Research

Principle 2 / 4 - Identifying Purposes for Collection & Limiting Collection
Criminal Record Checks and Employment Reference Checks
Documentation
Electronic Employee Files
Workplace Injury, Illness and Incident Response and Reporting

Principle 3 - Consent for the Collection, Use, and Disclosure
Consent to Treatment
Free and Informed Consent in Research
Guide for discussing virtual care and obtaining consent for email communication
Guidelines for Bioethics Consultations

Lockbox
One Drive, SharePoint Online and Teams Acceptable Use Policy and Guideline
Release of Information to the Media and General Public
Research Involving Participants

Principle 5 - Limiting Use, Disclosure, and Retention
Disclosure of Personal Health Information
Quality Improvement Projects
Records Creation, Retention and Destruction
Release of Information to the Media and General Public
Research Involving Participants
Use of Social Media Platforms by SickKids Staff

Principle 6 - Accuracy
Caring Safely: Error Prevention iLearn

Principle 7 - Safeguards
Confidential Waste Guidelines
Communicating with Patients and Caregivers
Electronic mail (E-mail) and Instant Messaging (IM) usage
Hardware Decommissioning
High-Profile Patient Privacy, Security, and Safety Guidelines
Information Security
Information Technology Acceptable Use
Mobile Device Security Policy
Paper Recycling Guidelines
Records Creation, Retention and Destruction
Remote Access
SickKids Electronic Monitoring Policy
Safety Reporting
Theft / Loss Prevention and Reporting

Principle 8 - Openness about Information Policies and Practices
SickKids External Privacy Webpage “Privacy & Your Rights”

Principle 9 - Individual Access
Disclosure of Personal Health Information
Freedom of Information

Principle 10 - Challenging Compliance
Disclosure of Harm Related to Patient Safety Events
Management of Patient Safety Events
Safety Reporting

6.0 References

Freedom of Information and Protection of Privacy Act, 1990
The Information and Privacy Commissioner of Ontario website.
Ontario Hospital Association
Personal Health Information Protection Act, 2004
Privacy Review Needs Assessment for Digital Solutions

7.0 Contacts

Privacy Office: privacy.office@sickkids.ca
Communications and Public Affairs Office: communications.publicaffairs@sickkids.ca

Appendix 1 – Guideline for Determining Level and Discipline Response to a Privacy Breach

In the event a staff member violates SickKids' privacy policies and/or the *Personal Health Information Protection Act* ("PHIPA") and/or the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), this Guideline defines the level of the breach (based on intent, severity and the staff member's history of privacy breaches) and determines the corresponding sanction. This Guideline is in accordance with the Information and Privacy Commissioner's ("IPC") direction to health information custodians outlined in the "Detecting and Deterring Unauthorized Access to Personal Health Information" guidance document.

SickKids uses a just culture approach to determine the appropriate sanction based on the nature of the breach. Sanctions may include, but are not limited to coaching/education, training, suspension, and termination. If required by law, a privacy breach will be reported to a staff member's professional/regulatory body. SickKids may exercise its discretion to terminate the placement of a student, volunteer or observer upon a breach of this policy. The existing channels for appealing such decisions apply for medical, dental, and scientific staff members. Please see the procedures outlined in the SickKids By-Laws, found on the SickKids intranet. For more information, refer to the Code of Conduct policy.

Any collection, use, or disclosure of PHI in contravention of PHIPA may result in fines of up to $200,000 for individuals and up to $1,000,000 for SickKids upon conviction. Individuals may also be subject to Administrative Monetary Penalties (AMPs) issued by the IPC. SickKids will not cover or insure individuals for fines resulting from the collection, use or disclosure of PHI in contravention of PHIPA and/or other hospital policies.

A. Breach Level

Level I Breaches (Inadvertence, Negligence)
Level 1 breaches are unintentional violations of privacy / security policies or legislation that may be caused by lack of knowledge or training, environmental factors, carelessness, or other human error, and include:

- Accidently accessing High or Moderately Sensitive information[1], including personal information ("PI") or personal health information ("PHI"). that is not required to carry out work-related duties;
- Inadvertently disclosing PI or PHI to the wrong person;
- Using improper channels to obtain access to PI or PHI that you are otherwise authorized to access;
- Leaving your computer unattended while you are logged into a system that includes High or Moderately Sensitive information, including PI or PHI;
- Discussing High or Moderately Sensitive information, including PI or PHI, or leaving such information unattended, in a public area;
- Second incident of any Level I breach, depending on severity (does not have to be the same breach).

Level II Breaches (Intentional, "Knew or Ought to Have Known", Repeated Level 1 offence)
Level II breaches are intentional breaches and/or violation of known policies and legislation relating to access, use, and disclosure of PI or PHI. These include situations where the employee ought to have known that their actions would violate policies or legislation. Examples include:

- Repeated violations or third incident of any Level I breach, depending on severity (does not have to be the same breach);
- Accessing ConnectingOntario for a non-care purpose;
- Collecting, using or disclosing PHI for a research purpose without approval from a Research Ethics Board.

[1] all information of a sensitive nature in any format which is created, received or disclosed by SickKids in the course of its business, including corporate and proprietary information and including physical and electronic records in the custody of agents retained by SickKids. Confidential information is categorized as: high sensitivity, moderate sensitivity or low sensitivity, in accordance with the Information Security policy.

- Intentionally accessing or using High or Moderately Sensitive information, including PI or PHI, for a purpose that is out of scope of their SickKids job description.

Level III Breaches (Personal gain, Malice, Serious repeated offence)
Level III breaches are intentional violations of policies or legislation for personal gain or to cause patient or organizational harm and include:

- Second incident of any Level II breach, depending on severity (does not have to be the same breach);
- Intentional and unauthorized use or disclosure of High or Moderately Sensitive information, including PI or PHI.
- Collecting PI or PHI under false pretenses;
- Accessing, using and/or disclosing High or Moderately Sensitive information, including PI or PHI, for commercial advantage, personal gain or malicious harm;
- Failure to cooperate with the Privacy Office in any investigation or proceeding;
- Failure to comply with a Privacy Office resolution or recommendation.

B. Sanction

The sanctions set out below are to be used as guidelines for determining discipline and corrective action when a staff member is found to have violated SickKids' privacy policies and/or the PHIPA/FIPPA. Depending on the circumstances, including but not limited to risks to patients/ staff/ SickKids, sensitivity of the information at issue, volume of individuals affected, surrounding environment, actions and behavior of the violator, and history of violations, a staff member's actions or conduct may warrant bypassing any or all of the steps outlined in this Guideline and additional sanctions not outlined in this Guideline may also be appropriate. In addition, decisions in respect of discipline should consider the "Management of Staff Involved in Healthcare Associated Harm: A Fair and Just Culture" policy.

Level I[2]

1. a. Verbal and / or written reminder of obligations or letter of expectations (to be recorded by supervisor); and/or
   b. First written warning in staff member's personnel file.
2. Education on privacy policies and law.
3. Possible report to applicable Regulatory College.
4. Possible report to the Information and Privacy Commissioner.

Level II

1. a. Final written warning in staff member's personnel file; and/or
   b. Suspension of employment / privileges.
2. Education on privacy policies and law.
3. Report to applicable Regulatory College.
4. Report to the Information and Privacy Commissioner.

Level III

1. Termination of employment/privileges.
2. Report to applicable Regulatory College.
3. Report to the Information and Privacy Commissioner.

C. Privacy Office Contact Information

[2] Records of Level 1 incidents shall be expunged from a staff member's personnel records, five (5) years following the date of the incident.

Privacy Office: privacy.office@sickkids.ca