INDIGENOUS PRIMARY HEALTH CARE COUNCIL

INDIGENOUS DATA GOVERNANCE

PRIVACY AND SECURITY HANDBOOK

2023

DRAFT Data Privacy and Security Handbook

DRAFT version 1.2

Prepared in November 2022

Table of Contents

Introduction

This handbook was designed to support the implementation of the Indigenous Primary Health Care Council's (IPHCC's) Data Governance Framework. It can be utilized by organizations positioned at either the national (i.e. 'macro'-), provincial/regional (i.e. 'meso'-), or local (i.e. 'micro'-) levels of governance and contains sample privacy policies, privacy breach procedures, a public privacy notice, safeguard guidelines for patient information, access and correction procedures related to the release of patient information, and lockbox procedures. Resources are intended to be customized and by Health Information Custodians (HICs) and adopted by organizations to ensure the overall privacy and security of Indigenous data.

About the IPHCC's Data Governance Framework

The IPHCC's Data Governance Framework was created in 2022 and established a coherent set of principles, objectives, roles, and responsibilities to govern the data, stories, knowledge, and insights that Indigenous Primary Health Care Organizations (IPHCOs) collectively create, collect, hold, handle, and share. Through the framework, which continues to evolve, the IPHCC aims to support its members to collect, manage, and share information that supports evidence-informed decision-making and continuous quality improvement, tells individual and collective stories on behalf of the sector, and supports advocacy for change that will improve health outcomes and wellness for Indigenous people and communities in Ontario.

Development process

This handbook was introduced in October 2023 to support the implementation of the IPHCC Data Governance Framework. Content was developed by health privacy experts to ensure adherence to Ontario's Personal Health Information Protection Act (2004), which outlines how personal health information is collected, used and disclosed within the province's health sector.

The SGAR model

The Secure, Govern, Act, Report (SGAR) model outlined in the IPHCC's Data Governance framework summarizes a framework for the respectful and sensitive handling of Indigenous Data. The model addresses the unique considerations of Indigenous data, which includes personal, cultural, and traditional knowledge, and is a critical element in respecting and upholding the sovereignty of Indigenous communities over their data.

Fundamental to SGAR is its 'Secure' element, which emphasizes the importance of protecting Indigenous data through robust privacy and security guidelines. It involves applying encryption and secure storage methods, establishing strict access controls, and conducting regular security audits to safeguard the data throughout its lifecycle. This handbook will support organizations in implementing many of these requirements.

How to use this handbook

This document should be reviewed by designated Privacy Officers and implemented in collaboration with relevant designated parties responsible for ensuring overall compliance with privacy legislation. Highlighted text is intended to be examined and tailored according to the specifics of each organization.

Implementation considerations

This handbook is supported by the IPHCC's Data Governance indicator framework and Data Governance Policy handbook, which were collectively designed to support implementation of its Data Governance Framework and are available separately.

It is highly recommended that the implementation of the policies summarized here take place in collaboration with Indigenous Elders and other representatives of communities, and with designates of organizational leadership and clinical staff.

Limitations of this handbook

Although this handbook was designed as a template for organizations to ensure full PHIPA compliance, it does not constitute legal advice. Once the document has been customized, organizations are advised to ensure a full review of the document by a legal professional prior to implementation to ensure appropriateness.

Appendix A: Sample privacy policy

[NAME of IPHCO]

Privacy Policy

We are committed to patient[1] privacy and to protecting the confidentiality of the health information we hold.

[NAME of IPHCO] is a health information custodian (HIC) under the *Personal Health Information Protection Act, 2004* (PHIPA). We are accountable and liable for compliance with PHIPA and the protection of health records.

In this Privacy Policy, we use the language of "Team Members" to capture the commitment that [NAME of IPHCO] and all our staff, affiliated physicians, volunteers, students and vendors and any other agents will abide by this Privacy Policy and to reflect our shared commitment to protecting personal health information.

This Privacy Policy acts as the articulation of privacy practices and standards to guide all Team Members. There are additional privacy procedures and guidelines that are included by reference to this Privacy Policy and are listed at Appendix A. All Team Members agree to abide by those procedures and guidelines as well.

Principle 1 – Accountability for Personal Health Information

[NAME of IPHCO] is responsible for any personal health information we hold.

The Privacy Officer is the [Executive Director or other position?]. The Privacy Officer is accountable for compliance with this Privacy Policy and compliance with PHIPA.

Our commitment to privacy is demonstrated by adherence to our privacy policies and procedures to protect the personal health information we hold and by educating our staff and any others who collect, use or disclose personal health information on our behalf about their privacy responsibilities.

Principle 2 – Identifying Purposes for Collecting Personal Health Information

We collect personal health information for purposes related to direct patient care, administration and management of our programs and services, patient billing, administration and management of the health care system, research, teaching, statistical reporting, quality improvement, meeting legal obligations and

[1] We have used the term "patient" throughout the policy. It is possible that we hold personal health information about individuals who are not officially [NAME of IPHCO] patients or who are former patients, and this policy would apply equally to those individuals.

as otherwise permitted or required by law.

We may de-identify health information and sell it or otherwise allow it to be used by third parties. [ONLY INCLUDE THIS IF YOU DO THIS]

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

Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information

In general, we require consent in order to collect, use, or disclose personal health information. However, there are some cases where we may collect, use or disclose personal health information without consent as permitted or required by law.

Implied consent (Disclosures to other health care providers for health care purposes) – Circle of Care

Patient information may be released to a patient's other health care providers for health care purposes (within the "circle of care") relying on implied consent and without requiring the express written or verbal consent of the patient as long as it is reasonable in the circumstances to believe that the patient wants the information shared with the other health care providers. No patient information will be released to other health care providers if a patient has stated they do not want the information shared (for instance, by way of the placement of a "lockbox" or "consent directive" on their health records).

A patient's request for treatment constitutes implied consent to use and disclose their personal health information for health care purposes, unless the patient expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct patient care if authorized by PHIPA):

Within [NAME of IPHCO]:

- Interprofessional health providers (Nurse Practitioner, Registered Nurse, Dieticians, Social Workers, Pharmacists and other clinical staff) [NOTE: edit as applicable]
- Our affiliated physicians
- Medical students and residents or nursing or other allied health care students

Outside of [NAME of IPHCO]: (among others)

- Regulated health professionals or social workers in solo practice or group
- Hospitals
- Community Health Centres
- Indigenous health service providers and Aboriginal Health Access Centres
- Long-term care homes and retirement homes
- Ambulance and paramedics

- Pharmacies
- Laboratories
- Home and community care service providers
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care
- Supportive housing
- Public health [NOTE: edit list as applicable to key clinical partners with whom you share health information]

Sharing within the circle of care includes through shared electronic health systems such as the [NAME] Ontario Health Team, and local, regional and provincial programs. [NOTE: edit to include shared systems that you use.]

For clarity – the following groups are NOT in the circle of care and we do not share personal health information about our patients with them relying on implied consent. That does not mean we never disclose to these individuals and groups - but we only do so if we have express consent or if we are otherwise permitted or required by law to disclose:

- Teachers and schools (however, psychologists, social workers, nurses, psychiatrists, speech-language pathologists, occupational therapists, physiotherapists, or audiologists affiliated with schools may be in the circle of care if they are providing health care)
- Children's Aid Societies
- Police
- Landlords
- Employers
- Spiritual leaders/healers
- Insurance companies

Express consent

Patients may provide a verbal or written consent if they wish for [NAME of IPHCO] to release their information to their external health care providers or to any other third parties including lawyers, insurance companies, family, or employers. See our "*Access and Correction Procedures – Release of Patient Information*".

No Consent

There are certain activities for which consent is not required to collect, use or disclose personal health information. These activities are permitted or required by law. For example, we do not need consent from patients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services
- Do financial reporting and process for compensation
- Engage in quality improvement, error management, and risk management activities

- Participate in the analysis, administration and management of the health care system
- Engage in some research projects (subject to certain rules, such as obtaining research ethics board approval and having research contracts)
- De-identify health information to provide to third parties (sometimes for compensation)
- Teach, train and educate our Team Members and others
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations

A list of mandatory reporting obligations is found in our "*Access and Correction Procedures – Release of Patient Information*".

If Team Members have questions about using and disclosing personal health information without consent, they can ask the Privacy Officer.

Withholding or Withdrawal of Consent

If consent is sought, a patient may choose not to give consent ("withholding consent"). If consent is given, a patient may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

Lockbox – Consent Directive

PHIPA gives patients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within [NAME of IPHCO], our affiliated physicians' offices and Family Health Organization or by external health care providers. Although the term "lockbox" is not found in the privacy legislation, lockbox is commonly used to refer to a patient's ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes. See the "*Lockbox Procedures*" for details of how the lockbox works.

Principle 4 – Limiting Collection of Personal Health Information

We limit the amount and type of personal health information we collect to that which is necessary to fulfill the purposes identified. Information is collected directly from the patient, unless the law permits or requires collection from third parties. For example, from time to time we may need to collect information from patients' family members or other health care providers and others.

Personal health information may only be collected within the limits of each Team Member's role. Team Members should not initiate their own projects to collect new personal health information from any source without being authorized by [NAME of IPHCO].

Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information

Use

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be used within the limits of each Team Member's role. Team Members may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" as part of their position. If a Team Member is in doubt whether an activity to use personal health information is part of their position – they should ask the Privacy Officer. For example, looking at health records out of personal curiosity or a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise is not permitted.

Disclosure

Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be disclosed within the limits of each Team Member's role. Team Members may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position. If a Team Member is in doubt whether an activity to disclose personal health information is part of their position – they should ask the Privacy Officer.

Retention

Health records are retained as required by law and professional regulations and to fulfill our own purposes for collecting personal health information.

We follow the Canadian Medical Protective Association (CMPA) and College of Physicians and Surgeons of Ontario (CPSO) recommendations to retain health records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (age 18). In some cases, we keep records for longer than this minimum period.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely. Please see our "*Safeguards Guidelines for Patient Information*".

Principle 6 – Accuracy of Personal Health Information

We will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about a patient.

Principle 7 – Safeguards for Personal Health Information

We have put in place safeguards for the personal health information we hold, which include:

- Physical safeguards (such as confidential shredding bins, locked filing cabinets and rooms, and clean desks);

- Organizational safeguards (such as permitting access to personal health information by staff on a "need-to-know" basis only); and
- Technological safeguards (such as the use of passwords, encryption, audits, back-up, and secure disposal).

We take steps to ensure that the personal health information we hold is protected against theft, loss and unauthorized use or disclosure. The details of these safeguards are set out in the "*Safeguards Guidelines for Patient Information*".

We require anyone who collects, uses or discloses personal health information on our behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

Care is used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information. We take care if we transfer files to a medical storage company.

Principle 8 – Openness about Personal Health Information

Information about our policies and practices relating to the management of personal health information is available to the public, including:

- Contact information for our Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to personal health information we hold, and making requests for its correction;
- A description of the type of personal health information we hold, including a general account of our uses and disclosures; and
- A description of how a patient may make a complaint to our Privacy Officer or to the Information and Privacy Commissioner of Ontario.

Principle 9 – Patient Access to Personal Health Information

Patients may make written requests to have access to their records of personal health information, in accordance with the "*Access and Correction Procedures – Release of Patient Information*".

We will respond to a patient's request for access within reasonable timelines and costs to the patient, as governed by law. We will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Patients have a right to ask for their records to be corrected if they can demonstrate that the records we hold are inaccurate or incomplete in some way for the purposes for which we hold that information. In some cases, instead of making a correction, we may offer a patient an opportunity to append a statement of disagreement to their file.

Please Note: In certain situations, we may not be able to provide access to all the personal health information we hold about a patient. Exceptions to the right of access requirement will be in accordance with law. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

Principle 10 – Challenging Compliance with Our Privacy Policies and Practices

Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officer:

Contact information

We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information.

We will investigate all complaints. If a complaint is found to be justified, we will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with privacy rules and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
www.ipc.on.ca

Breach of Privacy Policy, Procedures or Guidelines

Failure by Team Members to adhere to this Privacy Policy and its related procedures and guidelines may result in corrective action being taken. Such corrective action may include, but is not limited to: retraining, loss of access to systems, suspension, reporting conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring agency, school or institution, termination of contract, restriction or revocation of privileges, and immediate dismissal. Additional consequences include notification of affected persons, fines, prosecutions or lawsuits.

Supporting Privacy Procedures and Documents

The following procedures and documents are incorporated into the Privacy Policy and must be followed by [NAME of IPHCO] and all staff, affiliated physicians, students, volunteers, and vendors:

	Last Updated
Privacy Breach Procedures	October 2023

Public-Friendly Privacy Notice	October 2023
Safeguards Guidelines for Patient Information	October 2023
Access and Correction Procedures – Release of Patient Information	October 2023
Lockbox Procedures	October 2023

Appendix B: Sample privacy breach procedures

[NAME of IPHCO]

Privacy Breach Procedures[2]

These procedures are part of our *Privacy Policy*.

Report

All privacy complaints, incidents, and actual or potential breaches must be reported immediately to the Privacy Officer.

Privacy Breach

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA) or our privacy policies. The most obvious privacy breaches happen when patient information is lost, stolen or accessed by or sent to someone without authorization.

For example:

- Our server is hacked and held ransom after an email with a virus is opened
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of patient records is not delivered to the correct address
- An unencrypted USB key with an Excel spreadsheet with patient information or Word files is lost
- Patient biological samples are lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A Team Member talks about a patient with a personal friend
- A Team Member takes a photograph or video or other recording of a patient without the knowledge of the patient or without consent
- Team Member sends an email to a "help desk" attaching a worksheet with patient information but does not check the email address and instead of sending the attachment internally – sends it to the last help desk emailed which is at a bank
- Health records to be disposed of are recycled and not shredded

[2] Based on the Information and Privacy Commissioner/Ontario "Privacy Breach Protocol". Available online: https://www.ipc.on.ca/health-organizations/responding-to-a-privacy-breach/privacy-breach-protocol/

- Out of curiosity, a Team Member reviews a neighbour's health record
- A student or any other Team Member looks at health records of patients on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise
- A fax with patient information is misdirected to a business where the fax number was entered incorrectly
- Health information is given to the media without consent
- A Team Member makes a copy of an ex-spouse's health record without it being part of the Team Member's position to do so
- Team Members discuss patients in hallways and lunchrooms and other patients overhear (even colleagues overhear)
- Team Member releases information to another health care provider when a patient has said they don't want that provider to know
- Team Member releases information to a spouse when the patient doesn't want that spouse to know
- Team Member releases information to a child's parent when the child is capable of making their own decisions and said don't tell my parents
- Email messages containing PHI sent to the wrong patient
- Unauthorized clinical users copied on a message sent to a patient
- Unauthorized clinical users reviewing patient requests and messages without their consent
- Scheduling or appointment confirmation or reminder notification for a virtual visit includes an excessive amount of personal health information
- Virtual video visit launches from a public space
- Wrong patient is invited to participate in or attends a video virtual visit
- Wrong clinical user invited to or attends a multi-person video virtual visit
- Video virtual visit launched in error after a patient virtual visit is cancelled
- Sharing information (e.g. test results) for the wrong patient during a video virtual visit
- A video virtual visit is recorded without authorization

Privacy Breach Protocol

The following steps will be taken by the Privacy Officer (or delegate) if they believe there has been a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate Team Members are immediately notified of the breach, including the physicians whose patients are potentially affected by the privacy breach.
- Address the priorities of containment and notification as set out in the following steps.
- Consider engaging legal counsel, the Canadian Medical Protective Association (CMPA), or a privacy breach coach if appropriate.

- Consider whether notification to the Information and Privacy Commissioner/Ontario (IPC/O) (www.ipc.on.ca) is required and if not required is advisable. As time passes, the Privacy Officer will revisit this need to report on an ongoing basis. It may be premature to report if unclear whether there has been a breach or if unclear of the scope of the breach. The Privacy Officer may need to keep the IPC/O apprised throughout this process.

- Consider when to notify the insurer (which may be a condition of coverage) and other key internal stakeholders.

- Consider whether to notify the police.

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it

- Retrieve and secure any personal information that has been disclosed or inappropriately used or collected (including all electronic or hard copies). This might include attending at the scene to determine whether there are any other records in public.

- Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to collect, use or receive the information. Obtain the person's contact information in the event that follow-up is required.

- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords or identification numbers, temporarily shut down a system, suspend an individual or group's access to the system, implement security, institute a lockbox or restriction to the file).

- Consider notifying or updating the IPC/O and/or legal counsel and/or CMPA if appropriate.

- Consider whether calling the police to report a theft or crime is appropriate.

Step 3: Clarify the facts

- Consider whether there is sufficient expertise to conduct an internal investigation or whether a specialist (such as a privacy or IT security specialist) is required.

- Determine the scope of the breach:
    - Details of the incident and how it was discovered
    - Number of people affected
    - Who was involved
    - Dates
    - Type of incident (such as:)
        - Unauthorized use
        - Unauthorized disclosure
        - Hacking, malware, security breach
        - Lost/stolen mobile device
        - Lost/stolen hard copies
        - Fax to wrong number
        - Refused access or correction request

        - Email to wrong recipient

- Determine how it happened and who was involved and why.

Step 4: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- At the first reasonable opportunity, any affected patients (or others whose personal health information has been affected) will be notified. We give careful consideration to whether affected individuals need to know immediately (especially where despite our efforts, the breach is ongoing or where the information in question is of a highly sensitive nature or there is reason to believe that it will be used in a malicious way).

- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s)).

    - For example, notification may be in person or by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at their next appointment.
    - In some cases, a public notice will be the most efficient and effective method of notice.
    - We focus on considerations such as:
        - The potential privacy impact of calling the individual's home or sending a letter
        - Whether the affected individual will be coming in to see a health care provider very soon and could be told in person
        - Whether anyone affected is in a vulnerable state of health or deceased or a child or incapable to make information decisions such that notice would be given to a substitute decision-maker and consider the best way to manage those sensitive issues

- Provide details of the extent of the breach and the specifics of the personal health information at issue.

- Advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term, including any steps taken to:

    - Reduce potentially harmful effects on the individual; and
    - Prevent a similar breach from happening

- Provide affected individuals with contact information for a Team Member who can provide additional information.

- Advise affected individuals of their right to complain to the IPC/O.

- Establish a plan to address what clinical and administrative staff and others should do if they receive calls about the privacy breach.

- Consider notifying the IPC/O especially if required by law to do so and legal counsel and CMPA if appropriate. Consider whether it is necessary to call police.

Step 5: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
    - Ensure the immediate requirements of containment and notification have been addressed.
    - Review the circumstances surrounding the breach.
    - Review the adequacy of existing policies and procedures in protecting personal health information.
    - Address the situation on a systemic basis.
    - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure Team Members are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider notifying the IPC/O and/or legal counsel and/or CMPA as appropriate. Consider whether it is necessary to call police.
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach and any related obligations to report to regulatory colleges.

Step 6: Recordkeeping

- Keep a record of all privacy complaints, incidents and breaches including investigations, notifications and remedial action taken.
- Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information must be submitted to the IPC/O annually, due on or before March 1 for the previous calendar year. The IPC/O provides an electronic form and guidance for submitting the statistical report on its website.

Notifying the IPC/O

We abide by the obligations to notify the IPC/O as required by law. We take guidance from the IPC/O based on its interpretation of the reporting obligations: https://www.ipc.on.ca/health-organizations/report-a-privacy-breach/

Appendix C: Sample public privacy notice

[NAME of IPHCO]

Privacy Notice

We are committed to promoting privacy and protecting the confidentiality of the health information we hold about you.

YOUR HEALTH RECORD

Your health record includes information relevant to your health including your date of birth, contact information, health history, family health history, details of your physical and mental health, record of your visits, the care and support you received during those visits, results from tests and procedures, and information from other health care providers.

Your record is our property, but the information belongs to you.

With limited exceptions, you have the right to access the health information we hold about you, whether in the health record or elsewhere.

You can request a copy of your record. If you need a copy of your health record, please contact us in writing at: <address>, or ask your physician or other health care provider who will explain the process. A copy will be provided at a reasonable fee. In rare situations, you may be denied access to some or all of your record (with any such denial being in accordance with applicable law).

We try to keep your record accurate and up-to-date. Please let us know if you disagree with what is recorded, and in most cases we will be able to make the change or otherwise we will ask you to write a statement of disagreement and we will attach that statement to your record.

CONFIDENTIALITY

Everyone here is bound by confidentiality. We have to protect your information from loss or theft and make sure no one looks at it or does something with your information if they are not involved with your care or allowed as part of their job. If there is a privacy breach, we will tell you (and we are required by law to tell you).

OUR PRACTICES

We collect, use and disclose (meaning share) your health information to:

- Treat and care for you
- Provide appointment or preventative care reminders to you and/or send patient surveys to you
- Update you of upcoming events, activities and programs
- Coordinate your care with your other health care providers including through shared electronic health information systems such as Ontario Health Teams, Ontario Laboratory

Information Systems (OLIS), HealthLinks, Connecting Ontario, and local, regional and provincial programs
- Deliver and evaluate our programs
- Plan, administer and manage our internal operations
- Be paid or process, monitor, verify or reimburse claims for payment
- Conduct risk management, error management and quality improvement activities
- Educate our staff and students
- Dispose of your information
- De-identify your information and sell the de-identified information to a third party for research and other purposes [ONLY INCLUDE IF YOU DO THIS. MODIFY PURPOSE AS NECESSARY]
- Seek your consent (or consent of a substitute decision-maker) where appropriate
- Respond to or initiate proceedings
- Conduct research (subject to certain rules)
- Compile statistics
- Allow for the analysis, administration and management of the health system
- Comply with legal and regulatory requirements
- Fulfill other purposes permitted or required by law

Our collection, use and disclosure (sharing) of your personal health information is done in accordance with Ontario law.

YOUR CHOICES

You have a right to make choices and control how your health information is collected, used, and disclosed, subject to some limits.

We assume that when you come to receive health care from us, you have given us your permission (your consent) to use your information, unless you tell us otherwise. We may also collect, use and share your health information in order to talk with other health care providers about your care unless you tell us you do not want us to do so.

There are other cases where we are not allowed to assume we have your permission to share information. We may need permission to communicate with any family members or friends with whom you would like us to share information about your health (unless someone is your substitute decision-maker). For example, we will also need your permission to give your health information to your school or your boss or to an insurance company. If you have questions, we can explain this to you.

When we require and ask for your permission, you may choose to say no. If you say yes, you may change your mind at any time. Once you say no, we will no longer share your information unless you say so. Your choice to say no may be subject to some limits.

BUT there are cases where we may collect, use or share your health information without your permission, as permitted or required by law. For example, we do not require your permission to use your information for billing, risk management or error management, or quality improvement purposes. We also do not

need your permission to share your health information to keep you or someone else safe (in order to eliminate or reduce a significant risk of serious bodily harm); or to meet reporting obligations under other laws such as for health protection of communicable diseases, child safety, or safe driving.

CONSENT DIRECTIVE – LOCKBOX

You have the right to ask that we not share some or all of your health record with one or more of our team members or ask us not to share your health record with one or more of your external health care providers (such as a specialist). This is known as asking for a "lockbox". If you would like to know more, please click here [add link] or ask us for a copy of our "**Patient Lockbox Information Brochure: How to Restrict Access to your Health Record".** If you request restrictions on the use of and disclosure of your health record, a member of our team will explain your choices and potential repercussions for those options.

WHO DECIDES

You may make your own decisions if you are "capable". Your health care provider will decide if you are capable based on a test the law sets out. You may be capable of making some decisions and not others. If you are not capable – you will have a substitute decision-maker who will make your information decisions for you. Who can act as a substitute decision-maker and what they have to do is also set out in law.

For children, there is no magic age when you become able to make your own decisions about your health information. If you are under the age of 16, there are some additional rules to know:

> If you are under the age of 16, your parent(s) or guardian will also be allowed to make some decisions about your health record. But they won't be able to make decisions about any records about treatment or counseling where we asked for your permission alone.

We encourage you to share information with your family and other caregivers to have supports you need. We also encourage you to ask your health care provider questions to find out more about privacy and your family and caregivers.

FOR MORE INFORMATION OR COMPLAINTS

If you would like a copy of our Privacy Policy, please click here [add link] or ask us for a copy.

We encourage you to contact us with any questions or concerns you might have about our privacy practices. You can reach our Privacy Officer at: <contact information>

If, after contacting us, you feel that your concerns have not been addressed to your satisfaction, you have the right to complain to the Information and Privacy Commissioner of Ontario. The Commissioner can be reached at:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
1-800-387-0073
or visit the IPC website via www.ipc.on.ca

Appendix D: Sample safeguards

[NAME of IPHCO]

Safeguards Guidelines for Patient Information

These guidelines are part of our *Privacy Policy*.

We hold a lot of personal information about our patients.[3] This information is sensitive and valuable to our patients and we are obliged by law to treat it carefully. As part of our duties we must all take steps to keep patient information safe and make sure that it can be accessed only by those who need to see it for a proper reason.

This applies equally to our electronic medical record, paper copies of health records, reports, test results voice messages, and emails and any other ways patient information can be recorded. We have to protect this information from loss, theft, and unauthorized access including any kind of disclosure to the wrong people.

Following these guidelines will minimize the risk of patient information falling into the wrong hands which could cause harm and distress to patients and legal consequences. We require everyone who is affiliated with us, including all staff, physicians (and their staff), volunteers, students and vendors (collectively "Team Members") to follow the best practices described here. Every Team Member has a role in keeping our patients' information secure, and we expect everyone to fulfill that role.

Restricted Access to Patient Information

Access to patient information is provided on a need-to-know basis as appropriate to the Team Member's role and purpose for access. Team Members will have access to only the minimum amount of personal health information necessary to perform their duties.

No snooping!

Team Members must not access any health records unless authorized - which means only for legitimate reasons. **Team Members may not access health records of their spouses, children, parents, friends or neighbours, work colleagues or anyone else unless that person is under the Team Member's direct care or the Team Member is authorized as part of their official duties (or if covering the shift or tasks for someone who is authorized).** Team Members may only access their own health record (if applicable) through the normal patient access channels and not directly. [NOTE: This is optional – do you allow your staff who are patients to have direct access to their own health records?]

Team Members must not:

- Access patient information for "self-education" or out of personal interest

[3] We have used the term "patient" throughout these guidelines. It is possible that we hold personal health information about individuals who are not patients, and the safeguards guidelines would apply equally to those individuals.

- Edit, cut-and-paste, delete from or otherwise change any health records except for legitimate reasons

Team Members should know that all access to the electronic medical record is logged and audited.

Accounts and Passwords

Our information technology systems are protected by the use of personal accounts and passwords. Individual accounts are given access to information required by the account holder.

We require all Team Members to:

- Use only their own user account and password
- Not permit anyone else to use their account
- Help maintain security by choosing hard-to-guess passwords
- Contact the Privacy Officer if they suspect any kind of computer misuse

A good privacy password is a mix of numbers, upper and lower case letters and symbols. Avoid using your name in a password.

An unauthorized person trying to gain access to our health records may not be obvious. Data breaches have occurred in other organizations after "confidence tricks" convinced individuals to reveal passwords or other information to intruders, for example claiming to be the "IT helpdesk". Never send your user ID or passwords via email. Never tell anyone your password no matter who they say they are. If anyone you do not know requests information from you, you must verify their identity and their reason for asking, first. If you are left in any doubt contact the Privacy Officer immediately.

Under no circumstances should new users' ids and passwords be communicated by email. The system also forces the new user to create a new unique password when they log in for the first time.

Physical Security On-Site

We hold a large amount of patient information in printed format - on paper, in files and binders. Daytimers, schedules and notebooks may also contain patient information and are confidential just like our electronic medical record and paper patient files.

Access to patient information is permitted by individuals who require the information to do their authorized jobs. If patients or visitors are in areas where patient information is kept or in other private areas, politely challenge them as to their business. If there is any doubt as to someone's purpose, they should be asked to leave.

Patient information in paper format should be kept in a locked cabinet, container or room. If a filing cabinet or room where patient information is stored is not in constant use, it should be locked.

Where records are on desks in occupied rooms or paper inboxes they should be turned over so they cannot be read by someone nearby.

Patient identifiable labels on files should not be visible to visitors.

Patient information that is being stored before secure destruction will be kept separate and clearly marked.

Sending Patient Information

Special care must be taken when sending correspondence about a patient or containing patient information to anyone outside of our team - including to another health-care provider, to a third party, or to the patient.

Please note, sending a patient's chart number still constitutes identifiable health information. Merely removing a patient's name from a record does not necessarily anonymize the record.

In addition to this policy, physicians and interdisciplinary health providers (collectively, "clinicians") need to follow their own regulatory College's directives on confidentiality, security of personal health information and communicating with patients to ensure privacy is protected.

External Emails and Text Messages

Because of the insecure nature of emails, Team Members are not permitted to include patient information in any email sent to a recipient other than to a [NAME of IPHCO] email address or Team Member's phone, except as set out below.

Patients

Clinicians may send or give permission to a Team Member to send emails to their patients **with patient's consent** for the purposes of:

- Reminding patients about appointments and follow-up visits;
- Providing information about upcoming programs and events;
- Diagnostic imaging or other testing requisitions;
- Sending information or resources requested by a patient; or
- For requesting feedback to programs, groups or services that a patient may have participated in. [NOTE: edit permitted purposes as applicable]

Any other information communicated with a patient via email will be done on a limited basis and through an approved, secure and encrypted method. No emails to patients should be sent through unapproved programs such as "gmail".

This is important because it:

- Decreases the chances of typos in entering email addresses
- Ensures that a copy of the email is recorded in the patient's chart for continuity of care and legal purposes
- Ensures that the email is sent from an approved email address so that automatic reply functionality is working properly
- Ensures that any information not intended for the patient is not accidentally sent (such as can be the case with the "reply all" functionality of regular email chains.

Except in rare circumstances (such as an emergency where there is no other reasonable option), email (especially unencrypted email)[4] should not be used to communicate diagnoses, provide information about test results or transmit other personal health information that will require a follow up. Clinicians must take care to consider the sensitivity of the information being conveyed over email (especially unencrypted email), the purpose of the transmission, and the urgency of the situation. Clinicians should also consider that as the volume and frequency of emails increase – so too does the risk inherent in communicating by email.

We only communicate by email from professional email accounts. We do not use personal email accounts to communicate with patients.

We recommend to patients that they use a password-protected email address that only they can access.

If unencrypted email is to be used for the authorized purposes, the following steps must be undertaken: [NOTE: Review carefully – these are optional]

- The Team Member must register with the Privacy Officer as a patient email user;
- The patient must sign a Patient Consent and Release for Email Communication and it must be documented in the patient's health record (see Appendix A);
- There must be a disclaimer message at the end of the email message being sent (see Appendix B) providing notice that the information received is confidential and instructions to follow if an email is received in error;
- The Team Member (or email method) must have an automatic response email for all incoming email messages (see Appendix C);
- Before sending, the Team Member must check the email address carefully to confirm it is going to the correct recipient (NOTE: email programs that "autofill" the recipient field can insert an address you did not intend to send to) – the following steps can help avoid misdirection:
    - verify the recipient's identity by sending a test message in advance and asking for confirmation to ensure the message reaches the intended recipient;
    - confirm email addresses are up to date;

[4] Encryption should be used for emails to and from patients that contain personal health information including by encrypting or password-protecting document attachments and sharing passwords separately through a different channel or message. Encryption must also be used when emailing personal health information to other health information custodians.

    - ensure that the recipient's email address corresponds to the intended address; and
    - regularly check pre-programmed email addresses to ensure that they are still correct;
- The Team Member should avoid using the "reply-all" feature if responding to an email from a patient and limit the number of recipients to the minimum necessary;
- To avoid mistakes, the Team Member must check to see if there are any unexpected attachments to the email that will be sent (by clicking on "preview" to see the email content or otherwise reviewing the email before sending);
- If appropriate, the email message must be copied and entered into the health record or the clinician must write a note in the health record summarizing the clinically relevant information from the email communication; and
- The email may only include the minimum amount of personal health information necessary for the purpose with the disclosure of personal health information in subject lines and message contents minimized to the greatest extent possible.

For group emails (that is, emails to more than one patient such as for flu clinics or patient satisfaction surveys), check to make sure the content is correct before sending including for any attachments that have been accidentally included. Large emails have an increased risk of privacy breaches and extra care must be taken.

As part of protecting information communicated by email, we also:

- inform patients of any email address changes; and
- store personal health information on email servers only for as long as is necessary to serve the intended purpose. For example, if email communication is documented in the patient's record, it may not be necessary to retain duplicate copies of the information on an email server. Likewise, we ensure that all copies of emails containing personal health information on portable devices are securely deleted when they are no longer needed and are documented in the patient's record.

The Privacy Officer ensures that we:

- restrict access to the email system and to email content on a need-to-know basis;
- use strong access controls to email accounts used by clinicians; and
- remind employees, other agents, and patient of the risks associated with phishing to avoid falling prey to malware, spyware, or other forms of social engineering.

Similar issues arise with the use of text messages. At this time we do not allow clinicians or Team Members to send texts to patients or texts containing personal health information to anyone inside or outside of [NAME of IPHCO]. OR If you communicate with patients by text, please contact the Privacy Officer for recommendations.

Sending emails and texts to other health care providers outside [NAME of IPHCO]

Unencrypted email and text messaging should not be used routinely for communicating with external health care providers. Consider all the issues discussed in these guidelines for communicating with patients and internally within [NAME of IPHCO]. Extra care should be used to only include the minimum amount of personal health information necessary for the purpose.

Emails Sent within [NAME of IPHCO]

It is preferable to send messages about patients through the electronic medical record functionality wherever possible.

If sending emails within [NAME of IPHCO], limit the personal information included to the minimum necessary. Refer to patients by their initials rather than using their full names, if it is possible to do so.

When using the "reply-to" feature there is a risk of including more information than necessary by including a copy of the original email. Therefore, it may be preferable start a new email rather than responding to an email thread.

Carefully check the recipient before hitting the send button. Email programs that autofill the recipient field can insert an address you did not intend to send to.

Avoid using the "reply-all" feature and limit the number of recipients to the minimum necessary.

Spreadsheets containing patient lists and other personal health information should only be sent as attachments to email to staff within [NAME of IPHCO] with the greatest caution. Such email and attachments should never to be sent to people outside of [NAME of IPHCO].

Accessing Email on a Mobile Device

Approval must be obtained to have access to [NAME of IPHCO] email address on a mobile device (such as a smart phone). If permission is obtained, the following steps must be undertaken:

- Team Members must have permission from the Privacy Officer;
- The device must be password protected and ideally subject to a strong level of encryption;
- The device contents must be able to be erased remotely if lost or stolen (that means, all content from the device can be remotely deleted by the device owner);
- A "Return if Lost" sticker must be put on the device; and
- Any loss of the device must be reported immediately to the Privacy Officer to assess exposure and remotely delete the contents of the device if necessary.

Facsimile (Faxes)

- Misdirected faxes are easy to send and difficult to correct. They make up a significant proportion of privacy breaches. Therefore, when sending patient information by fax, carefully check the fax number - multiple times - to ensure it is correct.
- Include a cover sheet stating for whom the fax is intended. The cover sheet must ask a recipient to call if information is received in error.
- Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.
- After sending a fax, collect and keep a confirmation receipt. If there is any question about a wrong number being used the receipt will make it much easier to check and to retrieve information sent to the wrong place.
- A privacy breach occurs whenever patient information is sent to a third party without the patient's authorization or without being otherwise permitted or required by law. There can be particularly significant consequences in cases where clinicians repeatedly send patient information to a third party improperly.
- In the event of a misdirected fax containing patient information, it is important to ask the wrong or unintended recipient to confirm **in writing** that the information was destroyed and not kept or shared with anyone. This should then be documented in the patient's chart.
- Clinicians should use their judgment when it comes to implementing the *Privacy Breach Procedures* as a result of a misdirected fax. For single instances of a fax that is misdirected to another health care provider, ensuring that the recipient securely destroyed the fax may be sufficient. Clinicians may choose to put a reminder in the chart to discuss the breach (and actions taken to correct it) next time the patient visit the clinic. Clinicians should be aware that they may face increased consequences if they do not implement the full *Privacy Breach Procedures* whenever a breach occurs.
- Please report all stray faxes to the Privacy Officer. And situations where there are repeated stray faxes must be reported to the Privacy Officer to assess whether a report to the Information and Privacy Commissioner is required and how to notify affected individuals.
- If you receive a stray fax (meaning you receive a fax that was not intended for anyone at our organization), please notify the sender of their error as soon as you discover it. If you notice a pattern of such stray faxes received from the same sender in error, please notify the Privacy Officer.

Social Media

Team Members are advised to avoid posting information about patient-specific cases online and are advised against providing medical or other clinical **advice** online. Regulatory colleges and professional liability indemnity providers recommend that clinicians avoid posting comments in internet discussion forums or other online groups to avoid the perception of providing medical or patient-specific health care **advice**. While it may be acceptable to provide general health-related **information** for public or professional educational purposes, those purposes should be clearly identified and clearly marked as not providing advice.

Telephone

Patients may ask us to relay their own health information to them by telephone. Calling a patient at home or at work or leaving messages is an everyday reality that carries a real risk to our patients' privacy. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, ask patients every time they register for an appointment to check that their contact information is up to date so we have their most recent telephone numbers (and home address – see mail below). Ask if we can leave a message with someone or on an answering service and confirm the number.

If we have the patient's consent to leave a message and you are answered by a machine, listen for clues that you may have misdialed before leaving a message. For example, if the message repeats a name or number other than the one you expected to hear. If you are in any doubt leave a message only to say to call the office.

If a patient calls us we must take steps to confirm the caller's identity before providing information. Our patients expect it. If we are in doubt as to the identity of the caller, we can confirm the caller's identity by asking questions such as:

- What is your full name?
- What is your date of birth?
- When was your last appointment with us?
- What is your health card number?

If speaking on the phone with a patient in a place other than the office, Team Members should ensure that no one can overhear the conversation (for example, if at home, no family members of the Team Member or, if anywhere else such as outside or in a coffee shop, no passersby or others nearby).

Mail

Sometimes it is necessary to send patient information by mail or courier. When sending information in the mail, check the address to make sure it is correct. Also, mark the envelope or package "Attention <name>" on the outside to make sure it is opened only by the intended recipient.

Make sure that no health information can be read through the envelope or window, and consider whether there are any logos or other markings on the envelope that may identify the nature of the content enclosed.

For highly sensitive information, send by registered mail and obtain a tracking number and follow up with the patient to make sure it was received. When sending less sensitive patient information via mail, a tracking number is not mandatory, but should be used depending on the sensitivity of the health information being sent. Envelopes should always be stamped CONFIDENTIAL.

The easiest way to prevent the chances that a patient's mail will be lost or stolen (without using a tracking number system) is to call the patient and ask them to pick up the letter at the office. If they are not able

to attend, the patient's home address can be confirmed at that time, and they will have notice that they will receive a letter in the next few days.

Virtual Care

For video visits, we are now using the following technology:

<list technology such as …>

- Ontario Telehealth Network
- *

Please do not use other technology or personal devices without asking your <role of who can override policy>.

Do not use personal email, unencrypted text messaging, or free cloud-based videoconferencing platforms to communicate with patients. Use only approved email, messaging, and videoconferencing accounts, software, and equipment.

Do not post publicly your meeting ID, Room ID or other consultation identifiers (such as on websites or social media posts).

When using videoconferencing for virtual care, clinicians should:

- address accessibility concerns if any regarding captioning or screen readers and remind patients of steps that they can take to protect their privacy such as joining from a private location and using a secure internet connection;
- join the videoconference from a private location – i.e. using a closed, soundproof room or an otherwise quiet and private place with window coverings as required;
- use a secure internet connection;
- use headphones rather than the speaker on the device to prevent being overheard by others;
- watch where screens are positioned to prevent others from seeing;
- once logged into the videoconference:
    - check the meeting settings to ensure the meeting is secure from unauthorized participants;
    - not record the meeting unless it is necessary and the patient provides express consent;
    - at the start of an initial visit, verify the identity of the patient. In the event of a new patient encounter, compare the patient's image with a photo on file or ask the patient to hold up their health card to the camera for confirmation;
    - introduce yourself and any others who are present on the health care provider side of the interaction and ensure the patient consents to the presence of any additional individuals;
    - inquire if anyone is accompanying the patient and confirm the consent of the patient; and
    - <if platform allows> remind the patient that they can blur their background if they do not want the clinician or clinician(s) to see more than is needed to participate in the videoconference.

- use sufficiently high-quality sound and resolution to ensure you can collect information (including verbal and non-verbal cues) that is as accurate and complete as is necessary for the purpose of providing health care.

Please also ensure that safeguards guidelines below for working from home or other remote sites are followed when providing virtual care from home or other remote sites.

Documentation

Clinicians must ensure they are making appropriate notes and documentation of all care provided virtually as they would an in-person visit. Do not use any recording function for the virtual visit unless it is necessary and you have express patient consent. Remind patients also not to record on their end. If you need to take a photograph or make a recording, you must have the individual patient's permission and you will need to take precautions to properly document the recording in the usual electronic health information system or record.

Administrative Safeguards for Virtual Care

All Team Members including employees and other agents must attend training on the use of secure email, messaging, and videoconferencing platforms.

The Privacy Officer ensures that we:

- regularly maintain authorizations on a need-to-know basis
- are aware of their ongoing obligation to avoid collecting, using or disclosing more personal health information than is necessary
- use confidentiality agreements that contain explicit provisions dealing with Team Members' obligations when using secure email, messaging, or videoconferencing to deliver virtual health care
- monitor and address cybersecurity threats, for example by:
    - updating software regularly
    - providing ongoing security training to team members to dupport the detection of phishing attempts
    - conducting regular threat risk assessments
- review, maintain, and monitor audit logs

Working from Home or Other Remote Sites

Our *Privacy Policy* and its related procedures and guidelines continue to apply when working from home and other remote sites. The following additional considerations apply.

Because of the serious risk of loss or theft, patient information will only ever be removed from the premises by those Team Members who have a real need to do so to carry out their duties (for example, Team Members who have been authorized to work from home, which may include conducting virtual patient appointments, or who provide care to patients at other sites such as home visits or community settings). This applies to electronic files, paper copies and information on mobile devices such as laptops,

smart phones, disks and memory sticks (USB keys and portable hard drives), printers, scanners and any other formats.

For electronic files, remote access to patient information should be through our secure server (our virtual private network), where we can protect it. Every time patient information is saved to a mobile device there is a chance it may be lost or stolen. Therefore, we will do this only when absolutely necessary to carry out our jobs and if so, only on an encrypted mobile device.

Do not use unsecured WiFi to access our secure system.

Where there is no choice but to take information off-site, patient information will be de-identified if possible. Note: merely removing someone's name from a record does not necessarily anonymize the record.

If patient information must remain identifiable when off site (or if new patient information must be collected and documented outside the secure server):

- For paper records:
    - Keep papers in a locked box or bag for transport and do not leave files in your car or public transit.
    - Patient information should not be stored at home except in very limited circumstances and if the Team Member is required to keep paper copies of patient information at home, it must be held securely and care should be taken to avoid family or friends or other visitors from having any access. **Do not leave paper that has personal health information on it available to anyone else in your home**.
    - Do not print records containing patient information at home unless absolutely necessary.
    - Paper records no longer needed must be either shredded with a cross-cut or confetti shredder on site (meaning at home or other remote work location) or brought back to the workplace for secure destruction. Do not put paper records containing personal information in the garbage or recycling.
- For electronic records:
    - Only save to a mobile device with strong encryption. Strong encryption is more than just password protected. If you are not sure how to encrypt a mobile device, ask a Privacy Officer.
    - If patient information must remain identifiable and there are no encrypted mobile devices to use, unencrypted mobile devices containing personal health information must not be left on the seat or in the trunk of an unattended car, even for just a few moments.
- Steps should be taken to avoid drawing attention to patient materials or unencrypted mobile devices (such as keeping them in an unmarked bag or container).
- When transporting patient information, go directly to the destination, making the journey as short as practicable.

Devices

- Please use one of our computers issued to you. If you have to use a personal device, please speak with your supervisor first – Team Members must have authorization to do so.

- Use only trusted secure devices to access PHI via web-based systems (e.g. ClinicalConnect – NOTE: edit as necessary to reflect web-based systems used to access PHI). This means the devices are running up-to-date patches and antivirus software. Patches include the operating system, internet browser, and internet browser add-ons such as Java and Adobe Flash.
- Public devices (such as those found in hotels and libraries) are non-trusted devices – do not use public devices to access PHI via web-based systems.
- Do not lend technology containing personal health information to anyone without authorization.
- Keep devices safe and secure from loss or theft and if it is lost or stolen erase the contents of the device remotely, if possible.
- Report to a Privacy Officer immediately a lost or stolen personal device that has access to the workplace network and/or email and/or that contains patient information.

Technology

[Note: If you are unsure whether the device or software that you are using complies with any of the below requirements, please talk to the Privacy Officer.]

- Use only approved email, messaging, and videoconferencing accounts, software, and equipment.
- Use firewalls and protections against software threats.
- Regularly update applications with the latest security and anti-virus software.
- Encrypt data on all mobile and portable storage devices, both in transit and at rest.
- Use our virtual private network to remote into our office computer system.
- Do not use public or unsecured WiFi to access our secure system.
- Sign in and out of the secure remote server each time of use and not have a saved password to the secure remote server on any device that others could utilize.
- Do not download personal health information records on your own personal device or any other devices. Patient information should only be stored in the EMR and <other authorized places>.
- Check the "Temporary Downloads" or "Scanned Files" before signing off a device to ensure nothing work related was accidentally saved on a personal device or in the wrong place on a work device. If it was, delete the work-related record from the personal device/unauthorized place.
- Lock your computer when it is not in use by you or when left unattended.
- Use and maintain strong passwords.
- Do not share your passwords with family members or anyone else.
- Review and set default settings to the most privacy protective setting.
- Verify and authenticate a patient's identity before engaging in an email exchange, chat, or videoconference.
- Do not click on anything strange or weird emails. Especially related to "invoices" or "change your password". These are likely hacking attempt emails.

Remote workspaces

- Keep all technology containing personal health information, such as desktop computers and servers, in a secure location.

- Keep portable devices containing personal health information, such as smartphones, tablets, and laptops, in a secure location, such as a locked drawer or cabinet, when they are unattended.
- Restrict office access, use alarm systems, and lock rooms where equipment used to send, receive or store personal health information is kept.
- Physically segregate and restrict access to servers to only authorized persons.
- Take care that people with whom you share space cannot see or overhear your work conversations, including virtual visits, and work product on screens or paper.
- Lock your computer when not in use by you or when left unattended.
- Do not share your passwords.
- Protect your own personal privacy when working remotely by blocking your personal/home number and not using personal email addresses to communicate with patients or colleagues. There are different ways to block your number depending on your phone. Ask your telecom provider or check their website for how you can block your number when using it for virtual visits. If you are using a landline, *67 will block your number.

Updating our Team Member Data

On a monthly basis, [NAME of IPHCO] will update Team Member information with key community partners such as <name> Hospital and Hospital Report Manager to reduce the number of reports wrongly received by [NAME of IPHCO] for Team Members who have moved on such as physicians, locum physicians, and nurse practitioners.

Filing Patient Information

Care should always be taken when tagging and filing electronic records or uploading paper copies of patient information to a patient's electronic health record to ensure the information relates to the correct patient. Check patient names and dates of birth carefully.

When patient information is filed in the wrong health record, it should be corrected immediately. It may be appropriate to choose *not* to enact the *Privacy Breach Procedures* when a test result is filed in the wrong chart, if a clinician feels confident that the misfiled information was not accessed by another healthcare provider to make healthcare decisions on behalf of the patient, and that no other patient would have had access to the information (for example, through a request for a copy of the chart). If it is possible that the information could have been used to make treatment decisions or could have been shared with an unauthorized third party, then the *Privacy Breach Procedures* should be enacted.

Destroying Patient Information

When patient information is no longer needed we must make sure it is destroyed securely. Different methods of destruction are appropriate depending on how the data is stored:

Material	Appropriate Method of Destruction
Paper (e.g., printouts, faxes, letters, labels, etc.)	Shredding
CDs, DVDs, disks, USB keys	Shredding or breaking into pieces

Audio or video tapes	Shredding
Pictures, slides	Shredding
Medication containers (bottles and bags) with ID labels	Shredding of label (or container) or return to supplier along with unused medications
IV bags	Label goes in shredding
Electronic devices with memory storage (e.g., laptops, PCs, printers, photocopiers, dictaphones)	Data wiping prior to redeployment or return to vendor – lease company

When personal health information is destroyed, we document details of the destruction (date, method, etc.) in a PHI destruction log. We retain the PHI destruction log indefinitely.

Never recycle any paper or media that contains personal information. Never treat any paper that has been printed with personal information as reusable for scrap.

Third Party Vendors

When we hire outside contractors to do data entry or provide information systems or to store, transport or destroy patient information, we only use those that are bonded and insured and maintain a verifiable commitment to confidentiality. We make sure that the contractor uses the methods documented in the contract we have with them.

We only select contractors who commit under contract to:

- Agree to be a PHIPA agent of the [NAME of IPHCO] if they will be handling our patients' personal health information or agree to comply with the prescribed requirements for service providers in PHIPA's regulation[5]
- Hold and follow written privacy policies and procedures saying how material is to be kept safe in transit, storage and destruction as applicable
- Have insurance coverage for their liabilities under contract
- Require their own personnel to sign confidentiality agreements
- Have appropriate training for their personnel on privacy policies and the procedures to implement them

Logging and Auditing in Electronic Medical Record

[5] If a vendor is supplying services to enable us to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, we ensure that they agree that they will not:

1. use any personal health information to which they have access in the course of providing the services except as necessary in the course of providing the services;
2. disclose any personal health information to which they have access in the course of providing the services; and
3. permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the vendor.

Logging

Our electronic medical record logs user access. The logs include for every instance in which a record or part of a record of personal health information is viewed, handled, modified or otherwise dealt with [NOTE: Check with your EMR provider – not all EMRs do this – this is what the IPC recommends your system be able to log and what will be required by amendments to PHIPA]:

- The identity of the individual to whom the personal health information relates
- The type of information that was viewed, handled, modified or otherwise dealt with
- The identity of all persons who viewed, handled, modified or otherwise dealt with the personal health information
- The date and time on which the information was viewed, handled, modified or otherwise dealt with
- The fact of an override of a consent directive on the system (that is, if a lockbox has been overridden)

Our logs are kept indefinitely.

Audits

We conduct random and targeted audits of our electronic medical record on a monthly basis.

Access audits can be performed on any patient record at the request of the Privacy Officer or at the request of a patient.

Access audit requests by patient

Patients may request an access audit on their own medical record, or the record of a patient for whom they are the substitute decision-maker.

Random audits

Monthly, an audit of electronic medical record activity is performed by the Privacy Officer or delegate on randomly selected patient charts or charts identified as at high risk for unauthorized access. High risk patients may be patients who are famous, related to staff or for any other criteria chosen by the Privacy Officer or delegate.

Audits of individuals on request

When an unauthorized access has been suspected or reported of an EMR user, an audit of their access will be performed.

Records of all audits will contain the following information:

- Reason for audit (e.g. request or random selection)
- Date range selected for audit
- Description of unauthorized or questionable activity and results of inquiry

Inquiry of unauthorized or questionable activity

Unauthorized or questionable activity will be brought to the attention of the Privacy Officer to determine the next course of action.

Unauthorized or questionable activity may be investigated in any of the following ways:

- Contact the user and ask for the reason for access
- Contact the patient to inform them of the unauthorized access
- Perform an additional audit to determine if there has been any further unauthorized access

A determination will be made if it constitutes a breach.

Appendix A - Patient Consent and Release for Email

We are now able to offer the use of email for communicating with you, including for:

- Appointment reminders
- Sharing routine test results
- Sending you forms for tests (labs, x-ray, ultrasound etc.)
- Giving you educational and health promotion resources
- Clinic Newsletters
- Patient satisfaction surveys
- Verifying your contact information
- Asking for health card information
- Sending you our policies
- Giving to specialists or other health care providers to contact you when we refer you

Please read to the bottom of this page and the next page to submit your consent.

If you would like to receive our emails, please update your address book to accept emails from **<your [NAME of IPHCO] email address>** and don't forget to check your junk/spam folder.

There are some limits on what and when we can email you, which we will explain here.

- Email communication is not a substitute for meeting with your health care provider. Although technology is changing, the best way to share information with your health care provider is in person.

- Please tell us which email address you wish us to use. You must to keep this up-to-date and tell us of any changes to your email address.

- Email should never be used in an emergency. **If you have a medical emergency, you should call 9-1-1 or go to your nearest hospital emergency room or health care provider immediately**.

- Email should never be used for urgent problems (where you need a response from us by a certain time). If you have an urgent issue, you should make an appointment to see your health care provider.

- We do not read our email messages 24 hours per day 7 days per week. We cannot guarantee any particular response time for an email. If you require a response to an email message, please call the office.

- Emails should be short. If you have a problem that is complex – please call the office instead.

You should not use email to tell us about sensitive health information. Please tell us if there are certain issues or types of information that you do not wish to discuss by email.

Unless you tell us otherwise, we may share your email address with specialists and other health care providers to whom we refer you so they can contact you.

There are some privacy risks in communicating by email:

- Email may not be secure. While we try to protect our emails we cannot guarantee the security and confidentiality of any email you send to or receive from us. As the message leaves [NAME of IPHCO] it is sent across the internet and it could be intercepted and read.

- More than just your health care provider may need to read your email. Administrative staff supporting your health care provider and people providing coverage for your health care provider (like a locum doctor) may also read any email you send.

- Emails may be filed on your health record depending on the content of the email message and can become a permanent part of your health record. As part of your record, emails may be shared within our team or third parties, with your consent or if we are permitted or required by law (including with other health care providers and insurance companies).

- Email is easy to forge, easy to forward (sometimes accidentally and to many people) and may exist forever.

- We recommend you give us a personal email address that only you read. We recommend that you use an email address and system that is password protected. If you give us a family email address or share your email address with anyone else, you should know that other people may also receive or read emails we send to you.

If you use a work email address, your employer may have a right to archive and look at emails sent from their systems. We recommend you avoid using a work email address.

- [NAME of IPHCO] is not responsible for information loss due to technical failures.

[NAME of IPHCO] may choose not to deal with you by email if you are not able to follow our email rules.

Patient Agreement and Release	
I have read and fully understand this consent and release form. I understand the risks associated with using email with [NAME of IPHCO] and I accept those risks. I understand the limits set out for using email and I agree to follow those limits. I understand if I no longer wish to communicate with [NAME of IPHCO] by email, I will tell my health care provider or the front desk staff person. **I agree that [NAME of IPHCO] (which for this agreement and release includes [NAME of IPHCO] staff, agents, directors, officers, and any affiliated physicians and their staff, agents, directors and officers) shall not be responsible for any personal injury including death, or privacy breach (outside the control of [NAME of IPHCO]) or other damages as a result of my choice to communicate with [NAME of IPHCO] by email and I release and hold harmless [NAME of IPHCO] from any liability relating to communicating with me by email.** If I had any questions about this form, I asked those questions and agree that my questions have been answered. I understand I have the right to have legal advice about signing this form and what it means to me and have either sought that advice or have chosen not to seek such advice.	
Patient Name (and if Substitute Decision-Maker – please add your name too) (please print):	
Signature:	Date:

Appendix B – Email Disclaimer Message

This e-mail message is confidential and is intended only for the persons named above. If you have received this message in error, please notify the sender immediately and securely delete/remove it from your computer system. Any reading, distribution, printing or disclosure of this message if you are not the intended recipient is strictly prohibited. Thank you.

Appendix C – Automatic Response Email

Thank you for your message.

- If you are experiencing a medical emergency, please contact 9-1-1 or go to an emergency department or local hospital.
- All appointments are made by phone to * (insert #) and I cannot accept email requests for new appointments.
- I do not monitor this email address 24 hours a day/ 7 days per week. There may be a delay in my ability to respond to your message.

Appendix E: Sample access and correction procedures

[NAME of IPHCO]

Access and Correction Procedures – Release of Patient Information

These procedures are part of our *Privacy Policy*.

The [NAME of IPHCO] is a custodian of all patient health records (including the electronic medical record). However, the information in the health record belongs to the patient and the patient has a right of access to that information and the right to direct us to share that information or not share that information with others, subject to some exceptions.

These *Access and Correction Procedures* address five activities:

- Patient[6] requests for access to their own health records ("**access**")
- Patient requests to correct their own health record ("**correction**")
- Requests to share information with other organizations or health care providers with express consent or implied consent ("**circle of care**")
- Requests to transfer patient files to a new health care provider or organization ("**transfer**")
- Third party requests for a copy of a patient's health record ("**release of information**") such as from lawyers, insurance companies and police

Consent and "Authorized Persons"

When consent is required under these procedures, the following authorized persons may give consent:

1. The patient, if the patient is capable - we verify the identity of a patient by checking picture identification
    a. **Please note for capable patients under the age of 16**: If a patient is capable and also under the age of 16, the patient may consent AND the patient's parent or person who has lawful custody may also consent. BUT the parent or person with lawful custody may not consent if the information to be disclosed relates to "treatment" (as defined under the *Health Care Consent Act, 1996*) about which the child has made their own decision or "counseling" (as defined under the *Child, Youth and Family Services Act, 2017*) about which the child participated on his or her own. (That means if a child consented to the care on their own, a parent cannot consent to the release of that information on behalf of the child). And if there is a disagreement between a capable child and the parent about the release of information, the capable child's wishes prevail. If staff have questions about consent for children, please ask the Privacy Officer.

[6] We have used the term "patient" throughout these procedures. It is possible that we hold personal health information about individuals who are not patients or who are former patients and these procedures apply in those cases as well. Requests for access may also come from a patient's substitute decision-maker or "authorized person" as identified in these procedures.

2. A substitute decision-maker, if the patient is incapable. Please refer to section 26 of PHIPA which lists the hierarchy of individuals/agencies that can act as substitute decision-makers:

   These substitute decision-makers will have documentation to show their legal authority:

   - The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual (please ask to see a copy of the documentation).
   - The individual's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual (please ask to see a copy of the documentation).
   - The individual's representative appointed by the Consent and Capacity Board, if the representative has authority to give the consent (please ask to see a copy of the documentation).

   These substitute decision-makers only have to state their family relationship unless there has been a court process changing their rights:

   - The individual's spouse or partner.
   - A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent [Note: This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent.]
   - A parent of the individual with only a right of access to the individual.
   - A brother or sister of the individual.
   - Any other relative of the individual.

   We verify the identity of a substitute decision-maker by checking picture identification and other documentation as identified above.

3. The estate trustee, in the case of a deceased patient
   a. We verify the identity of the estate trustee by reviewing a will or the notarized "Certificate of Appointment of Estate Trustee with a Will" or "Certificate of Appointment of Estate Trustee without a Will". A copy of this documentation must be kept. If the deceased patient does not have an estate trustee, consent can be obtained from the person who has assumed responsibility for the administration of the deceased person's estate – if documented in writing (see Appendix A). If in doubt, ask the Privacy Officer.

Consent Options

When consent is required, patients may withhold or withdraw consent. If patients decide to withhold or withdraw consent, that decision will be documented in their health record.

If the patient requests restrictions on the use of and disclosure of their health record, then the patient's physician and/or the Privacy Officer meets with the patient to discuss what is restricted and how this can be done. Restricted information can be put in a "lockbox" and the physician and/or the Privacy Officer needs to explain the repercussions of making this choice. See the *Lockbox Procedures* for information about how patients may choose not to share information with other health care providers or organizations.

Consent to Disclose Health Information to Caregivers

[NAME of IPHCO] proactively asks patients who their caregivers are and with whom they would like their health information shared.

A patient can authorize someone other than themselves to communicate with staff regarding their health information using a consent form (see Appendix B for example).

If someone other than the patient delivers the form, we will contact the patient to verify their consent.

Alternatively, a patient may ask that their verbal consent for sharing information with caregivers be documented in their chart.

If a patient has given us permission to share their health information with someone, they should know that the consent remains in their chart until they instruct us otherwise.

Copies versus Originals

Because we are custodians of the health record, originals of health records are not given to patients or released to other health care providers or third parties (except in rare situations if originals are required by law). In most situations, only copies are released. Patients may ask to view original documents as set out below.

PROCEDURES:

Please note, front line administrative staff will not dispense any patient information themselves, unless directed to do so by the patient's physician or clinician who is the author of the record or the Privacy Officer.

1. Patient Access to Information

With limited exceptions, we are required by law to give patients[7] access to their records of personal health information within 30 days (subject to a time extension of up to an additional 30 days if necessary and with notice to the person making the request).

a. Informal Patient Access

From time to time we will agree to give part of a patient's health record to a patient directly without engaging in a formal request for access. For example, sometimes a patient needs a list of medications or a copy of particular test results. A clinician decides whether to release this information informally and who can do that on their behalf (e.g. another clinician, front line or administrative staff). Usually a chart note will be made to document what the patient received.

[7] Patients and "authorized persons" as defined in these procedures may be given access to health records.

Also, it is good practice to stamp "Patient Copy" to alert that a document has been released to the patient directly (this protects us in case of patient losing information).

b. Written Requests

Patients may ask for additional records of personal health information.

i. Patient requests for their own information should be made in writing. Staff should encourage patients to use the "Patient Request for Access to Health Records" form available on the [NAME of IPHCO] website. [What do you use as your normal request form?]

ii. If a request for access is made to a health care provider, they should direct the patient to our usual process for release of records. Because records may be difficult to read and interpret and may mislead or alarm a patient, patients will be encouraged to review the records with their physician or other health care provider (or delegate) so the information can be explained.

iii. If a patient wishes to read the original health record, someone must be present to ensure the records are not altered or removed.

iv. Patients may not make notes on the original health record or remove originals from the health record or otherwise alter their health records.

v. If a patient requests a copy of a health record, copies may be given and fees may be applied in accordance with the fee framework approved by the Information and Privacy Commissioner of Ontario. [NOTE: If you have a fee schedule, mention it here.]

vi. The original of the written request for access shall be placed with the patient's records and must contain the following:

- A description of what information is requested
- Information sufficient to show that the person making the request for access is the patient or other authorized person
- The signature of the patient or other authorized person and a witness to the signature
- The date the written request was signed

vii. A notation shall be made in the record stating:

- What information or records were disclosed
- When the information or records were disclosed
- By whom the information or records were disclosed

c. Telephone Requests

Only limited information should be given out over the telephone to a patient, as it may not be possible to verify that patient's identity. See the *"Safeguards Guidelines for Patient Information".*

d. Walk-in Requests

A signed consent is required for access to a patient's record. Patients may be requested to return at a later date to pick up authorized information.

2. Denying Patient Access to Health Records

In certain situations, we may choose not to provide a patient with access to all or part of a health record. Exceptions to the right of access requirement must be in accordance with law and professional standards. Reasons to deny access to a health record (or part of a health record) may include:

- The information is subject to a legal privilege that restricts disclosure to the individual
- The information was collected or created primarily in anticipation of or for use in a proceeding (and that proceeding and any appeals have not been concluded)
- The information was collected or created in the course of an inspection, investigation or similar procedure authorized by law or undertaken for the purpose of the detection, monitoring or prevention of a person's receiving or attempting to receive a benefit to which the person is not entitled under law (and the inspection or investigation have not been concluded)
- If granting access could reasonably be expected to:
    - Result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to the individual or another person
    - Lead to the identification of a person who was required by law to provide information in the record
    - Lead to the identification of a person who provided information explicitly or implicitly in confidence (if it is appropriate to keep that source confidential)

Patients must be told if they are being denied access to their own health records. In some situations, we may advise a patient that we can neither confirm nor deny the existence of a record. We get legal advice in such cases. If denied information, patients have a right to complain to the Information and Privacy Commissioner of Ontario, and must be told of this right and how to reach the Commissioner's office.

3. Correction of Health Records

A clinician may edit or correct any note they author.

If an error was due to an administrative error (such as a patient's record is misfiled in another patient's record or there is a data entry error) and is noticed by administrative staff, that error may be fixed by the administrative staff so long as the error is identified before the health care provider had the opportunity to act on it and before anyone else received it externally. If the entry or record has been in the chart for more than a day in error, staff must notify the physician involved and any other clinical staff involved in

that patient's care that it is in the chart in error. If any action was taken based on the false information by any staff member, the erroneous information must be scanned into the chart and attached to a note indicating the error and the deletion. In such cases, seek legal advice.

Requests for Correction

We have an obligation to correct personal health information if it is inaccurate or incomplete for the purposes it is to be used or disclosed.

Patients may request that their health information be corrected if it is inaccurate or incomplete. Such requests must be made in writing and must explain what information is to be corrected and why.

We must respond to requests for correction within 30 days (or seek an extension). Corrections are made in the following ways:

- Striking out the incorrect information in a manner that does not obliterate the record or
- If striking out is not possible:
    - Labelling the information as incorrect, severing it from the record, and storing it separately with a link to the record that enables us to trace the incorrect information, or
    - Ensuring there is a practical system to inform anyone who sees the record or receives a copy that the information is incorrect and directing that person to the correct information.

The record will not be corrected if:

- The record was not originally created by a Team Member and we do not have the knowledge, expertise or authority to correct the record, or
- The record consists of a professional opinion which was made in good faith.

Where we choose not to correct a record, the patient must be informed in writing. The patient will have the choice to submit a statement of disagreement. If the patient submits such a statement, it will be scanned onto the health record and released any time the information that was asked to be corrected is released.

Where we choose not to correct a record, patients have a right to complain to the Information and Privacy Commissioner of Ontario.

4. Release of Information to Health Care Providers

a. Express Consent

Should a patient wish their other health care providers working externally to [NAME of IPHCO] to have access to the patient health record, the patient can provide a written statement of consent to this effect (release of information):

The following is the process for releasing health records to a third party health care provider or organization relying on a patient's express consent: [NOTE: is this how its done?]

1. Record the date of the request in the health record
2. Advise the patient's physician of the request
3. If release of information to the third party organization is authorized by the physician:
    a. Select and photocopy/print requested specific information
    b. Do not photocopy/print the entire health record unless required
    c. Prepare an official cover letter that will accompany the released information
    d. Send out/mail-out requested information
    e. Scan the letter of request, patient's consent, and a copy of the covering letter and save in the patient's health record
    f. Costs associated with release of information will be invoiced by [NAME of IPHCO] [Note: or modify as appropriate]
4. If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the physician:
    a. Inform the patient who made the request of the problem in writing (or in person or by phone as appropriate), such as:
        - The request is not sufficient to identify the patient
        - The request is unclear or unspecific
        - The request does not have the required consent
    b. Document the date, time of the call, name of the person with who contact was made, a brief summary of the conversation and comments made by the requester.

b. Implied Consent – Circle of Care

We may also release information to a patient's other health care providers and organizations for health care purposes (within the "circle of care") without the express written consent of the patient as long as it is reasonable in the circumstances to believe that the patient wants the information shared with other health care providers and organizations. However, no information will be released to other health care providers and organizations if a patient has stated they does not want the information shared.

The following is the process for releasing health records to a third party health care provider relying on a patient's implied consent:

1. Record the date of the request in the health record
2. Advise the physician of the request
3. If release of information to the third party health care provider is authorized by the physician:
    a. Select and photocopy/ print requested specific information
    b. Do not photocopy/print the entire health record unless required
    c. Prepare an official cover letter that will accompany the released information

d. Send out/mail-out requested information
e. Record the verbal request for information
f. If there is a cost associated with release of information, it will be invoiced by [NAME of IPHCO] [Note: or modify as appropriate]

4. If the request is incomplete, unclear or we have been advised by the patient not to disclose relying on implied consent, or the request is otherwise not authorized by the physician:
    a. Inform the patient who made the request of the problem in writing (or in person or by phone as appropriate), such as:
        - The request is not sufficient to identify the patient
        - The request is unclear or unspecific
        - The request does not have the required consent
        - Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

5. Transfer of Patient Records to a New Health Care Provider

If the patient is moving to another practice and wishes their files to be transferred, the patient should be encouraged to see their new physician or health care provider and sign a consent form with them for the release of information. If this is not possible, however, the patient may sign a copy of the Release of Medical Information Form. Clinical health records are transferred only with a written request signed by the patient (or patient's authorized person). A verbal request is not sufficient to transfer health records.

Originals of records are never sent as they are our property and must remain accessible to us.

When a Release of Medical Information form comes in to transfer patient records, staff should pull the patient's health care record, place the transfer request on the front and put it in the appropriate physician's box. The physician is responsible for responding to the request as soon as possible by either:

- Writing a summary of the patient's pertinent medical history or
- Directing staff regarding the relevant information to copy from the patient's health care record.

A copy of the Request of Medical information form should be filed in the patient's health care record with the date of transfer marked on this form.

When mailing the file, the envelope will be to the attention of the provider and marked "Confidential".

6. Third Party Requests for Release of Information (to Non Health Care Providers)

Should a patient wish their lawyer, insurance company, employer, landlord or other such persons or agencies to have access to the patient health record, the patient must provide a written statement of consent to this effect, which will be written to [NAME of IPHCO] and then directed to the patient's physician or directly to the physician. We will not process verbal third party requests for release of

information to anyone who is not a health care provider. These requests must be in writing. No information will be released without the express consent from the patient or the authorized person (unless permitted or required by law. See below "Permitted or Mandatory Release of Information"). Third party requests not accompanied by appropriate consent will be returned with an official letter, outlining proper and complete consent requirements.

Any third party request for release of information shall include:

1. The name, address and telephone number of person/agency requesting the information
2. The full name, address and date of birth of the person about whom the information relates
3. A specific description about the type and amount of information to be released
4. A consent for release of information form signed by the patient (or patient's authorized person)

The following is the process for releasing health records to a third party with consent of the individual patient:

1. Record the date of the request in the health record
2. Advise the patient's physician of the request
3. If release of information to the third party is authorized by the physician:
    a. Select and photocopy/print requested specific information
    b. Do not photocopy/print the entire health record unless required
    c. Prepare an official cover letter that will accompany the released information
    d. Send out/mail-out requested information
    e. Scan the letter of request, consent, and a copy of the covering letter and save in the patient's health record
    f. Costs associated with release of information will be invoiced by [NAME of IPHCO] [Or modify as appropriate]
4. If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the physician:
    a. Inform requester of the problem in writing (or in person or by phone as appropriate), such as:
        - The request is not sufficient to identify the patient
        - The request is unclear or unspecific
        - The request does not have the required consent
        - The date the patient's consent was signed is not recent; while legally still accurate, you may ask why it has taken a length of time for it to be provided.
    b. Document the date, time of the call, name of the person with who contact was made, a brief summary of the conversation and comments made by the requester.

7. Permitted or Mandatory Release of Information

We may release personal health information to a third party if "permitted or required by law". A list of mandatory disclosures is included at the end of this document (see Appendix C).

Any time a mandatory disclosure is considered, the Privacy Officer and the patient's physician are to be informed PRIOR to reporting. Legal advice may be sought.

Police/OPP/RCMP

There is a natural tendency to want to cooperate with the police and assist them in their investigations. However, this must be balanced against patients' right to privacy and the right to confidentiality of their personal health information.

The fact that a patient is suspected of being a victim of a crime or suspected of having committed a crime is not a recognized reason for breaching the patient's right to confidentiality. However, there is a recognized exception ("discretion to warn") to patient confidentiality where there is a significant risk of serious bodily harm to someone (either the patient or someone else) **and if it is genuinely believed that disclosing information to police could eliminate or reduce that risk.**

Otherwise, personal health information will only be released to police upon the presentation of one of the following documents:

- A consent for release of information form signed by the patient or authorized person
- A valid court order (or other legal document) requiring the release of information to the police
- A coroner's writ requiring the release of information to the police

Each document must be reviewed carefully before information may be disclosed to police (to ensure the disclosure is **permitted or required** by law). This review should be done by appropriate staff, such as the patient's physician and/or the Privacy Officer before any information is released. The documentation from the patient, police, court or coroner will be scanned into the chart. Legal advice should be sought as necessary.

Children's Aid Society (CAS)

Everyone has a mandatory duty to report a "child in need of protection" to the CAS under the *Child, Youth and Family Services Act, 2017*. Information may be sent to the CAS to explain the reason for the report.

Where the CAS is the legal guardian of a child, the CAS should be treated as any other parent or guardian would be in response to a request for access to or disclosure of the health records.

Any documentation from CAS claiming authority to release information to the CAS must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the patient's physician and/or the Privacy Officer before any information is released. The documentation from CAS will be scanned into the chart. Seek legal advice as appropriate.

Regulatory Colleges

Under the *Regulated Health Professions Act, 1991* and other health profession specific legislation, regulatory Colleges may have the authority to review patient records as part of investigations or quality assurance practices. Any documentation from a regulatory College claiming legal authority to release information to the College must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required**

by law). This review should be done by the patient's physician and/or the affected clinician and/or the Privacy Officer before any information is released. The documentation from the regulatory College will be scanned into the chart.

Other Authorities

Certain legislation gives government agencies and others authority to review patient records (such as immigration, the Ministry of Health, workplace safety and insurance and others). Any documentation from an agency claiming legal authority to release information to the agency must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the patient's physician and/or the Privacy Officer before any information is released. The documentation from the agency will be scanned into the chart.

Lawyers

Most lawyers' letters require patient consent for the release of information to a lawyer. **Do not release information to a lawyer without patient consent unless you have some other documentation to state that [NAME of IPHCO] is required by law to disclose the information.** Any documentation from a lawyer claiming legal authority to release information to the lawyer must be reviewed carefully before information may be disclosed (in most cases the lawyer is asking for the record – not advising the patient's physician and/or [NAME of IPHCO] that it is required by law to release the record). This review should be done by the patient's physician and/or the Privacy Officer before any information is released. The documentation from the lawyer will be scanned into the chart.

Communicable Disease

The *Health Protection and Promotion Act* requires certain health care providers and organizations to report all communicable diseases to the local Public Health Unit. Reporting is done by the patient's physician or delegate as soon as possible after the diagnosis is made.

Appendix A

Attestation of Estate Trustee or Estate Administrator

Under the *Personal Health Information Protection Act, 2004* (PHIPA)

Identification of Deceased Individual (Please Print Clearly)

Last Name: _____

First Name: _____

Date of Birth: _____

Date of Death: _____

Home Address (at time of death): _____

By signing below, I, _____,
First Name, Last Name (Please Print Clearly)

ATTEST to the following:

1. I am the Deceased's (select one):

   ___ Spouse or partner
   ___ Child
   ___ Parent
   ___ Sibling (brother or sister)
   ___ Other: _____ (describe relationship)

2. I have assumed responsibility for the administration of the Deceased's estate (meaning making burial and funeral arrangements and dealing with the Deceased's financial matters).

3. To the best of my knowledge, the Deceased died without a Last Will and Testament (Will) (or the Deceased died with a Will but that Will did not name a valid Executor) **and** there is no court-appointed Administrator for the Deceased's estate.

4. I know of no one else who has assumed or intends to assume responsibility for the administration of the Deceased's estate.

Authorization for a Copy of or to Disclose Personal Health Information

On the basis of my authority as attested to in this document:

☐ I would like my own copy of the Deceased's personal health information (describe information)

Or

☐ I consent to [NAME of IPHCO] disclosing the Deceased's personal health information to:

_____

_____

for the following purposes: _____

_____.

I understand the purposes for disclosing this personal health information to the person(s) noted above. I understand that I can choose not to give this permission.

_____
Signature

_____
Date (YYYY/MM/DD)

Appendix B

[NAME of IPHCO]

SHARING HEALTH INFORMATION WITH A CAREGIVER

Please fill in this form so we can share information with your support people as you choose.

1. Patient providing authorization (PLEASE COMPLETE IN FULL)

Name – Last, First MI		☐Patient is providing VERBAL CONSENT (office use only)
Street Address (and mailing if different)		Telephone # (xxx) xxx-xxxx
City	Province	Postal Code
Date of Birth mm/dd/yyyy		Patient # (office use only)

2. The person listed below is authorized to access my health information:

Name – Last, First MI		☐Patient is providing VERBAL CONSENT (office use only)
Street Address (and mailing if different)		Telephone # (xxx) xxx-xxxx
City	Province	Postal Code
Relationship with patient (eg: spouse, partner, parent, guardian, child, sibling, or other substitute decision-maker)		

The additional person listed below is also authorized to access my health information:

Name – Last, First MI		☐Patient is providing VERBAL CONSENT (office use only)
Street Address (and mailing if different)		Telephone # (xxx) xxx-xxxx
City	Province	Postal Code
Relationship with patient (ie: spouse, partner, parent, guardian, child, sibling, or other substitute decision-maker)		

3. INFORMATION TO BE RELEASED:

☐ All Information (including telephone/verbal communication)

☐ ONLY for the following subject:

_____

☐ ALL information EXCEPT the following subject:

_____

4. This authorization will remain in effect until revoked by you in writing. If you wish to limit the duration of this authorization, please specify end date: ☐_____

Signature of Patient _____ Date _____

Witnessed/documented by: _____(staff initials)

Appendix C - MANDATORY DISCLOSURES

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Child in need of protection	Information about a "child in need of protection" (e.g. suffering, abuse or neglect). Only information that is reasonably necessary to make the report should be shared. Ongoing information sharing after the report has been made should only be done with express consent or as permitted or required by law (such as a court order for the patient health record)	Any person including a person who performs professional or official duties with children	Relevant Children's Aid Society	*Child, Youth and Family Services Act, 2017*, s. 125.
Missing persons	Records that will assist in locating a missing person	Any person specified in an order to produce records made by a judge or justice of the peace A person to whom an officer makes an urgent demand in writing	Members of a police force	*Missing Persons Act, 2018*, ss. 4 and 5

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Sexual abuse	Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of the allegation, name of the health care professional and name of the allegedly abused patient • The patient's name can only be provided with consent • You must include your name as the individual filing the report	All regulated health providers	Registrar of the suspected health care professional's regulatory College	*Regulated Health Professions Act*, Schedule 2, ss. 85.1, 85.3. See also, *Social Work and Social Service Work Act*, ss. 43 and 44
Loss or Theft of Benzodiazepines and Other Targeted Substances	Any loss or theft of a targeted substance or of a licence or permit within 10 days of discovery	Pharmacists, physicians, dentists, nurse practitioners, midwives, podiatrists, and person in charge of a hospital (among others)	Minister of Health	Benzodiazepines and Other Targeted Substances Regulations, s. 72(1), enacted under the *Controlled Drugs and Substances Act*
Loss or theft of narcotics	Any loss or theft of narcotics within 10 days of discovery	Pharmacists, physicians, dentists, nurse practitioners, midwives, podiatrists, and person in charge of a hospital	Minister of Health	Narcotic Control Regulations, s. 55(g) and s. 63(c), enacted under the *Controlled Drugs and Substances Act*
Safe driving	Name, address and condition of a person (over the age of 16) who	Physicians, nurse practitioners	Registrar of Motor Vehicles	*Highway Traffic Act*, s. 203(1).

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
	has a condition that may make it unsafe for them to drive	and optometrists		
Air crew	Information about flight crew members, air traffic controllers or other aviation license holders who have a condition that may impact their ability to perform their job in a safe manner (likely to constitute a hazard to aviation safety)	Physicians and optometrists	Medical advisor designated by the Minister of Transport	*Aeronautics Act*, s. 6.5(1)
Seaman	Information about a seaman	Physicians, surgeons, hospital official	If requested by the seaman's employer	*Merchant Seamen Compensation Act*, s. 48
Railway workers	Information about patients who work in the railway industry who have a condition that may put the safety of rail travel at risk	Physicians and optometrists	A railway designated Organization	*Railway Safety Act*, s. 35(2)
Fraud	Information about health care fraud (including an ineligible person receiving or attempting to receive an insured service; an ineligible person obtaining or attempting to obtain reimbursement by OHIP for money paid for an insured service; or an ineligible person in an application, return or statement made to OHIP	Physicians and registered nurses in the extended class, podiatrist, chiropractor, midwife, optometrist, dentist, dental surgeon, operator of a physiotherapy facility, hospital, facility whose primary	General Manager of OHIP	*Health Insurance Act*, s.43.1(1) and Health Fraud Regulation, s.1

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
	or the General Manager giving false information regarding his or her residency	function is the provision of insured services, laboratory, specimen collection centre		
Queue jumping	Information about an individual offering to pay, confer, charge or accepting a benefit in exchange for improved access to health care	Physicians, registered nurses in the extended class, podiatrists, midwives, optometrists, dentists, dental surgeons, licensees under the Independent Health Facilities Act, hospital or private hospital	General Manager of OHIP	*Commitment to the Future of Medicare Act*, ss. 17(1) and 17(2) and General Regulation, s 7(1)
Reportable or communicable disease	Information about a patient who has (or may have) either a "reportable" or "communicable" disease. The report should include the patient's: • Name and address in full, • Date of birth in full, • Sex, and • Date of onset of symptoms	Physicians and registered nurses in the extended class and hospital, children's residence, child care centre, home for special care, long-term care home, psychiatric facility (and others)	Medical Officer of Health of the appropriate health unit	*Health Protection and Promotion Act*, s. 26 and Reporting Regulation, s.1(1)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Communicable disease	Name, address of a patient receiving care and treatment for a communicable disease but who is neglecting or refusing to comply with the treatment regime	Physicians and registered nurses in the extended class	Medical Officer of Health	*Health Protection and Promotion Act*, s. 34(1)
Rabies	Animal bites or animal contact that may result in humans contracting rabies	Physicians and registered nurses in the extended class (and other persons with information about animal bites)	Medical Officer of Health	*Health Protection and Promotion Act* and Communicable Diseases Regulation, s. 2(1)
Immunizations	Instances of adverse reactions to immunizations	Physicians, nurses, and pharmacists	Medical Officer of Health of the appropriate health unit	*Health Protection and Promotion Act*, s.38(3)
Communicable disease	Information about a child whose eye have become reddened, inflamed or swollen within two weeks of birth possibly due to a communicable disease. Report must be in writing and include: • The name, age and home address of child (or if not at home, where the child can be located) • The conditions of the eye that were observed	Physicians or other health care professionals who have attended the birth of a child	Medical Officer of Health	*Health Protection and Promotion Act*, s. 33(1) and Communicable Diseases Regulation, s. 1 para. 2)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Birth	Births	Physicians and midwives (or nurses if neither of the above are present at birth)	Registrar General	*Vital Statistics Act*, ss. 8, 9.1 and General Regulation, ss. 1(1) and 19(1)
Death	Facts surrounding the death of an individual in prescribed circumstances (e.g. violence, negligence or malpractice). Information requested for the purpose of an investigation	Any person with information about the circumstances of the death	Coroner or designated Police Officer	*Coroners Act*, s. 10(1)
Death	Deaths	Physicians and registered nurses in the extended class		*Vital Statistics Act*, s. 21(1) and General Regulation, ss. 35(2) and 35(3) *Health Protection and Promotion Act*, s. 30.
Occupational assessments	Reasonable conclusions of an occupational illness	Physicians who conduct medical examinations or supervise clinical tests for workplace safety	The worker's employer, the joint health and safety committee and the Provincial Organization	*Occupational Health and Safety Act* and the Designated Substances Regulation, ss. 29(2), 29(3), 29(6) and 29(7).
WSIB	Information requested by the WSIB about workers claiming benefits under the Workplace Safety and Insurance Act	All health care providers	Workplace Safety and Insurance Board (WSIB)	*Workplace Safety and Insurance Act*, s. 37(1)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
Self-report of offence	Information if you yourself are found guilty of an offence to include • Your name • The nature and description of the offense • The date you were found guilty of the offense • The name and location of the court where you were found guilty of the offence • The status of any appeals	All regulated health care providers	Registrar of your regulatory College	*Regulated Health Professions Act*, Schedule 2, ss. 85.6.1(1) – (3)
Self-report of professional negligence or malpractice	Information if you yourself are found guilty of professional negligence or malpractice to include • Your name • The nature and description of the finding • The date the finding was made • The status of any appeals	All regulated health care providers	Registrar of your regulatory College	*Regulated Health Professions Act*, Schedule 2, ss. 85.6.2(1) – (3)
Employer report if end of professional relationship	A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professionals' privileges, employment or practice for reasons	Employer or person who offers privileges to a member	Registrar of the college of the regulated health care professional	*Regulated Health Professions Act*, Schedule 2, s. 85.5(1), 85.5(3)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
	of professional misconduct, incapacity or incompetence			
Employee death or critical injury at workplace	Immediate notice of death or critical injury and within forty-eight hours after the occurrence, a written report of the circumstances of the occurrence containing such information and particulars as the regulations prescribe: (a) the name and address of the employer; (b) the nature and circumstances of the occurrence and of the bodily injury sustained; (c) a description of the machinery or thing involved, if any; (d) the time and place of the occurrence; (e) the name and address of the person who was critically injured or killed; (f) the names and addresses of all witnesses to the occurrence; (g) the name and address of the physician or surgeon, if any, who is attending to or attended	Employer	Immediate notice to an inspector under the Act, the joint health and safety committee, health and safety representative, and the trade union, if any; report within 48 hrs to Director	*Occupational Health and Safety Act*, s. 51 and Regulation 67/93, Health Care and Residential Facilities**,** s. 5(1)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
	to the injured or deceased person; and (h) the steps taken to prevent a recurrence			
Employee involved in accident, explosion, fire or violence causing injury at workplace	Within four days of the occurrence, written notice of the occurrence containing the prescribed information and particulars: (a) the name and address of the employer; (b) the nature and circumstances of the occurrence and of the bodily injury sustained by the worker; (c) a description of the machinery or thing involved, if any; (d) the time and place of the occurrence; (e) the name and address of the worker who was injured; (f) the names and addresses of all witnesses to the occurrence; (g) the name and address of the physician or surgeon, if any, who is attending to or attended to the worker for the injury; and	Employer	1. The joint health and safety committee, the health and safety representative and the trade union, if any. 2. The Director, if an inspector requires notification of the Director	*Occupational Health and Safety Act*, s. 52 and Regulation 67/93, Health Care and Residential Facilities, s. 5(2)

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
	(h) the steps taken to prevent a recurrence			
Allegations of privacy breach by staff member or agent	1. The employee or agent is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee 2. The employee or agent resigns and the health information custodian has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee	Health information custodian	The College of the health care practitioner under the *Regulated Health Professions Act, 1991* and the Information and Privacy Commissioner of Ontario	*Personal Health Information Protection Act, 2004*, s.17.1(2) and (4), and General Regulation, s. 6.3(1)5-6
Allegation of privacy breach	Theft or loss or the unauthorized use or disclosure of personal health information	Health information custodian	Individual whose personal health information was compromised and Information	*Personal Health Information Protection Act, 2004*, ss.12(2)(a) and 12(3) and

Quick reference	What information must be disclosed	Who must disclose	To whom disclosure must be made	Authority
			and Privacy Commissioner of Ontario	General Regulation, s. 6.3(1)2

Appendix F: Sample lockbox procedures

[NAME of IPHCO]

Lockbox Procedures

These procedures are part of our *Privacy Policy*.

They apply to our staff, affiliated physicians, students, volunteers, and vendors ("Team Members").

Ontario's health privacy law, the *Personal Health Information Protection Act* ("PHIPA"), provides individuals[8] with the right to make choices about, and control how, their personal health information ("PHI") [9] is collected, used, and disclosed.

PHIPA gives patients the opportunity to restrict access to any or their entire PHI by one or more Team Members or by external health care providers. Although the term "lockbox" is not found in PHIPA, lockbox is commonly used to refer to a patient's ability to withdraw or withhold their consent for the use or disclosure of their PHI for health care purposes. The lockbox provisions of PHIPA are found in sections 37(1)(a), 38(1)(a), and 50(1)(e). The lockbox does not extend to other uses or disclosures that are permitted or required under PHIPA or other legislation.

These *Lockbox Procedures* will help our Team Members understand and fulfill their role when addressing lockbox requests and providing care to patients who have implemented a lockbox. Lockboxes may affect our clinical practice because access to information about patients may be restricted, and we may be asked not to share PHI with other health care providers inside or outside of [NAME of IPHCO].

Requests for a Lockbox

Any current or former patient[10] may request a lockbox to restrict sharing of all or some of their PHI by one or more Team Members or by external health care providers.

When patients ask about lockboxes, it is important for Team Members to address their concerns about the confidentiality of their PHI. Note that some patients may want to control who can access their PHI, but may not know to use the term "lockbox." Patients may want a lockbox when they use words such as "restrict," "limit," "don't tell," "exclude," "shield," or "block" when talking about their PHI. For example, patients may want a lockbox if they ask their health care provider or other Team Member:

[8] It is possible that we hold PHI about individuals who are not patients or who are former patients, and the *Lockbox Procedures* would apply equally to those individuals.

[9] "PHI" is broadly defined under PHIPA. In our context it will mainly relate to a patient's health record and we have used "health record" interchangeably with PHI throughout these procedures. It is possible that we hold other PHI about an individual outside the health record and the *Lockbox Procedures* would apply equally to that information, wherever it resides.

[10] An individual's substitute decision-maker may also request a lockbox and such requests are processed in the same manner.

- Not to tell their specialist that they are being treated at [NAME of IPHCO]
- Do I have to share my information with that person?
- To exclude certain clinical staff from seeing their information
- To “shield” their information
- To “restrict” their health record
- Not to let their family members or neighbours who work with [NAME of IPHCO] or the Family Health Organization look at their health record

Patients may initiate the process for a lockbox by speaking with their physician or by contacting the Privacy Officer. Patients must submit their request for a lockbox in writing. Patients will be asked to complete a “Patient Lockbox Request” form. The completed form must be submitted to the Privacy Officer or delegate.

The “Patient Lockbox Information” brochure should be given to patients who want more information. This brochure discusses the purpose, implications, and limitations of implementing a lockbox.

Lockbox requests can vary considerably. A patient may request that:

- Only some of the documents in their health record be locked
- All of their health record be locked
- All documentation created in the future be locked
- Only one Team Member be restricted from accessing PHI
- Several Team Members be restricted from accessing PHI
- All Team Members be restricted from accessing PHI
- One or more external health care providers not be given their PHI

Although PHIPA does not require that we lock documentation that does not yet exist, in practice, refusing to lock future documents may result in frequent lockbox requests from a patient. For this reason, we will, where appropriate and if requested, lock documents as they are created. An example might be where a patient requests a future lockbox because one of their family members (or former spouse or partner) is a Team Member.

When patients request a lockbox, it often means they have concerns about their PHI and how it is being used and/or disclosed. Patients should be reminded that:

- We take privacy seriously and keep all PHI confidential and secure
- PHI is only accessed by Team Members on a need-to-know basis
- We conduct privacy audits to ensure compliance with the need-to-know policy

- Where PHI is accessed without authorization, appropriate steps will be taken to prevent a reoccurrence and there would be disciplinary consequences
- PHI is disclosed only to external health care providers with whom the patient wants their PHI shared (unless the disclosure is otherwise permitted or required under PHIPA without consent, or by another law)

Sometimes a patient requests a lockbox when a lockbox is not necessary to resolve the patient's concern. For example, a lockbox is not necessary to restrict the sharing of PHI with non-health care providers (e.g., family, employers, insurers) because we need the patient's express consent (either in writing or if verbal, as documented by us) to share information with such recipients (unless, for example, a family member acts as the patient's substitute decision-maker). If a patient does not want us to share information with non-health care providers – we will not do so unless there is legal authority to do so.

As another example, if patients disagree with the information in their health records they can ask for a correction and/or append a statement of disagreement to the record. See the *Access and Correction Procedures*. For that reason, they may not need a lockbox to solve their concerns about the accuracy of the information in their health record.

Implications of Implementing a Lockbox

If a patient chooses to move forward with a lockbox request, it is important that they understand the possible implications of the lockbox. There may be implications and risks to the patient and to their care. The Privacy Officer or delegate or the patient's physician should discuss implications and risks with the patient. Examples may include:

- The patient not receiving the best possible service because health care providers may not have access to PHI that they need in order to provide the best possible care in a timely manner.
- The patient may have to undergo duplicate tests, procedures and/or health history questions, as applicable, if existing information is unavailable.
- We use a multidisciplinary team approach to providing care. Although each lockbox request is considered on a case-by-case basis, generally, a patient's choice to implement a lockbox should not prevent a team from providing care as per their standards of practice.
- There may be circumstances where clinicians providing health care cannot provide care in a manner that meets professional standards of practice if they do not have sufficient information. Such clinicians may have to assess whether they can continue to provide care to a patient if there is insufficient information. However, the decision to discontinue care to a patient is a significant one and would only be made after thorough consideration of all the relevant information. Clinicians will try to maximize patient choice about how their PHI is used and disclosed while at the same time allowing all of the clinicians to uphold their commitments to deliver a high quality patient care and to meet their obligations to their regulatory colleges.

There may be other risks specific to particular patients, which should be explored and discussed with patients directly.

Decisions to Implement a Lockbox

The Privacy Officer or delegate will review, respond to, implement, and administer lockbox requests (including on behalf of a physician, where applicable). Because the choice to implement a lockbox may have implications for the patient's care, if applicable, the patient's primary health care provider (e.g. physician) must be involved in processing the request as appropriate.

The practical methods of implementing lockboxes are varied; therefore, lockbox requests are considered on a case-by-case basis. A decision to implement a lockbox will be based on the practicality of the solution, technological feasibility, and the specific circumstances.

The Privacy Officer or delegate will notify in a timely manner any patient who made a lockbox request of the decision made in respect of the lockbox. If a decision has been to deny a lockbox request, the patient will be informed of the right to make a complaint to the Information and Privacy Commissioner of Ontario.

Lockbox Exclusions

A lockbox is limited under PHIPA to those providing care to the patient. It does not operate to prevent administrative functions from being carried out or the use or disclosure of PHI for other authorized purposes. For example, even where a lockbox is in place, it will not prevent [NAME of IPHCO] from engaging in legally permissible activities such as:

- Obtaining or processing payments
- Planning services
- Quality improvement
- Disposing of information
- Complying with a court order
- Litigation
- Research (with research ethics board approval)
- Teaching Team Members to provide health care

The above actions are permitted under sections 37-50 of PHIPA.

A lockbox does not prevent a Team Member from using or disclosing PHI where there is a legal obligation to do so (for example, to fulfill mandatory reports to the Children's Aid Society or to the Ontario Ministry of Transportation). Team Members may also use or disclose PHI if there are reasonable grounds to believe that using or disclosing the information is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. There may be other circumstances where the

use or disclosure of PHI is required or permitted by law. The Team Member should consult with the Privacy Officer when in doubt.

Identifying a Lockbox

Before reviewing a patient's PHI, Team Members must always check to see if a lockbox has been applied.

- In the electronic medical record (EMR), you will not be able to view anything but the demographics for a patient for whom a lockbox has been implemented and from which you are excluded. [TRUE?]

Team Members should be aware of how records are made subject to a lockbox and what a lockbox looks like. If you have questions, ask the Privacy Officer.

[NOTE: edit the highlighted text below to your lockbox environment]

Electronic Records:
If a patient has implemented a lockbox on their chart or part of their chart, a lockbox message "Private" will appear in red when a user attempts to open the chart or locked note through the EMR.

If the whole chart is locked:
In the EMR there will be the word "Private" in red at the top of the chart under the demographic information for patients who have implemented a full chart lockbox.

If the lockbox applies to the Team Member opening the chart, then the electronic system will restrict access to that patient's records by blocking everything but the demographic sections. The rest of the chart will not be accessible to that user. Only a physician or nurse practitioner can change the privacy settings on a patient's chart to break a lockbox.

The demographics section of the chart may be visible even if the whole chart is locked, which includes:

- Patient name, address, date of birth
- Physician, last billed date, roster status, next visit (if booked) and age

This is still PHI and must be respected.

If a lockbox restriction pertains to specific Team Members, their access will be restricted to the rest of the patient's record or to a specific note.

A list of unauthorized or "locked" persons will appear in the EMR.

Parts of the demographic window outlined above can also be made Private by opening the patient demographic window and holding down the Alt and Shift keys while right clicking in the fields to be marked private.

If individual notes are locked:
Where individual notes in the chart are marked Private, the note will be collapsed and look as follows: "Private – Double click on the note to view in an emergency (Click to expand)"
When you click on it:

- *A window pops up that says: "Override Note Policy"*
- *When you click on this it shows who is allowed access to this note and who is not*
- *Only a physician or nurse practitioner has the ability to undo the privacy settings of the note*

Paper Records:
If the entire health record is subject to a lockbox, it will be in a sealed envelope (signed across the seal by the Privacy Officer or delegate) with a label affixed to it that reads "Lockbox" and a "Lockbox Notification Alert" form will be apparent and will include a list of unauthorized or "locked" persons.

If a portion of the health record is subject to a lockbox, the relevant portion will be in a sealed envelope (signed across the seal by the Privacy Officer or delegate) with a label affixed to it that reads "Lockbox" and a "Lockbox Notification Alert" form will be apparent and will include a list of unauthorized or "locked" persons.

"Breaking" the Lockbox

If a Team Member is authorized to access information that is otherwise "locked", the following instructions explain how to access the PHI.

Electronic Records:
The only people who can break a lockbox are the Privacy Officer or physicians and nurse practitioners. To "break" a lockbox, the Privacy Officer, a physician or nurse practitioner would click on the note or chart that is locked and click on the "Override Note Privacy" to access the note. The user must provide a reason for the Override (breaking the lockbox) and a message is sent automatically to the Privacy Officer to advise them that access to the chart was granted. Emergency Access will be granted for 30 minutes. A locked note (that cannot be deleted) is added to the patient chart to indicate that the lockbox was broken. Access to the health record is then available.

The other option to view a private record is to modify the patient's privacy settings. Privacy settings can only be modified by a physician or nurse practitioner and can be set for individual users and expiration dates can be set on this access (for example, if reception needs access to scan the chart then access can be granted to one receptionist and that access can be set to expire at the end of the day.

Paper Records:
To "break" a lockbox, a Team Member would open the sealed envelope and remove the paper records. Access to the health record is then available.

Any Team Member who accesses PHI that is protected by a lockbox must document on the patient's health record the reason and authorization for "breaking" the lock. All information subject to a lockbox will be monitored and there will be random audits of such files. If Team Members are in doubt about whether they are legally permitted to break a lockbox, they should contact the Privacy Officer.

For paper health records, if the lockbox restrictions continue after the lock has been broken for a specific purpose, the PHI should be "locked" again in another sealed and signed envelope by the Privacy Officer or delegate. The electronic record will continue with the assigned lockbox restrictions until they are removed.

Of course, a patient may choose to withdraw a lockbox request or unlock PHI in a lockbox. That decision must be in writing and must be documented on the health record. The Privacy Officer will implement the change.

Notice to External Health Care Providers

If a patient's lockbox instructions state that the patient does not want all or some PHI shared with an external health care provider, we will not disclose PHI to the restricted external health care provider unless:

- We are permitted or required by law to do so (for example, we need to disclose the PHI to the external health care provider in order to reduce or eliminate a significant risk of serious bodily harm to the patient or to another person or persons).
- The external health care provider has provided us with written proof of the patient's express consent to the disclosure.

If we are prevented from disclosing PHI relevant to the provision of care to an external health care provider because of a lockbox, we have an obligation to notify the receiving health care provider that not all the relevant PHI has been provided. As a note, the receiving health care provider is then able to explore the matter of the "locked" information with the patient and seek consent to have the locked information shared.

Audits

The Privacy Officer or delegate will conduct audits of locked health records to ensure compliance with patient lockbox instructions and to determine whether there has been inappropriate access to locked information. Any apparent unauthorized access to locked information will be investigated.

The EMR has a built-in Audit Report that generates a list of users who overrode the privacy lockbox and accessed a specific patient's records within a specific timeframe. If specific information is needed, an authorized person will access the Transaction Log.[TRUE?]

Breach of Privacy

Unauthorized access by a Team Member to a patient's health record constitutes a breach of privacy and may result in disciplinary action up to and including termination of employment or contract.

If there is a lockbox on a patient' health record and a Team Member is excluded from accessing the PHI, it is a considered a breach for that Team Member to access the PHI without specific authorization from the physician or the Privacy Officer or delegate or unless otherwise permitted or required by law to use or disclose the information (such as in an urgent situation in order to prevent a significant risk of serious bodily harm).

[NAME of IPHCO] is obliged to notify any affected patient(s) of a privacy breach and their rights and will do so in accordance with the requirements of PHIPA.

Attachments

Appendix A – Patient Lockbox Information Brochure

Appendix B – Patient Lockbox Request Form

Appendix C – Lockbox Notification Sheet [this would only be for paper records – you have to make your own]

Appendix A

Patient Lockbox Information Brochure:

How to Restrict Access to your Health Record

You have a right to make choices and control how your health information held by [NAME of IPHCO] is collected, used, and shared, subject to a few exceptions.

You have the right to ask that we not share some or all of your health record with one or more of our staff members involved in your care, or ask us not to share your health record with your external health care providers (such as a hospital or specialist). This is known as asking for a "lockbox".

What is in your health record?

Your health record includes information such as your health history, care we have provided, family history, your medications and results from lab tests and notes from your physician, other health care providers within [NAME of IPHCO] or your other external health care providers. If you would like a copy of your health record, please contact <add contact information>.

Who sees your health record?

Only team members who provide health care and services to you and team members who do administrative tasks to support health care are authorized to look at your health information, and only when they need to see that information to do their job.

We use your health information to make sure we can give you the best care. Your health information is shared only within your "circle of care"— meaning the physicians, nurse practitioners, nurses, social workers, dieticians, occupational therapists, hospitals, specialists, community services providers <add or delete professions and organizations to reflect your circumstances> and other people and organizations that help with your care — unless we are permitted or required by law. We will not share your health information with anyone else — for example, your family or friends, employer, school or insurance company — unless we get your permission (known as "express consent") to do so or unless we are permitted or required by law (see "Lockbox Exceptions" below).

What is a "lockbox"?

It's not exactly a "box" – and it doesn't have a lock. And a lockbox can mean different solutions depending on your request. Generally speaking, a lockbox means that all or part of your health information will be separated from our usual filing systems. If it is an electronic record, it will have additional restrictions of access. If it is a paper record, it will go into a sealed envelope. While all our health records are safely and securely stored, a lockbox will restrict the access to your health information from certain people or institutions.

Are there risks to having a lockbox?

There are some risks to putting your health information in a lockbox that you should consider before making your decision:

- Your health care providers may not have the information they need to give you the best possible care in a timely manner.
- Your health care providers may not have enough information to safely provide you with services and so may not be able to offer you care.
- It may be harder for your health care providers to share your information in an emergency.
- There may be errors in assessments, treatment or medications if the people providing care do not have enough information or do not have the right information about you.
- You may have to undergo duplicate tests, procedures and health history questions if existing information is unavailable.
- You may not benefit from the wide range of services we can offer you.
- There may be other risks specific to you and your request, which we will discuss with you.

You can ask us questions about the specific risks that could come up depending on your choices.

Lockbox Exceptions

Under the law, there are times when we are allowed to or must collect, use, or share personal information about you — without your permission — even if your information is otherwise "locked".

If your information is already in a lockbox, the "lock" may be broken and your information may be used or disclosed as permitted or required by law. We have provided some examples, but there may be other situations where the use or disclosure of your information is permitted or required by law. We may use or share your health information <u>without your permission</u> in order to, for example:

- Report a child in need of protection to the Children's Aid Society
- Make reports to the Ministry of Transportation or Public Health or other mandatory reports
- Protect you or someone else if we believe there is a significant risk of serious harm
- Obtain or process payments
- Plan our services
- Engage in quality improvement exercises
- Dispose of information
- Comply with a court order
- Defend ourselves in litigation
- Engage in research (as long as we have research ethics board approval)
- Teach our staff to provide health care

If you have questions about how we can use or share your health information, you can ask a team member or the Privacy Officer**.**

How do you request a lockbox?

You can discuss any concerns regarding the privacy and confidentiality of your health information and your lockbox options with your physician or health care provider or the Privacy Officer. In some cases, you may not need a lockbox in order to protect your information and we can discuss alternatives or options with you. For instance, you do not need a lockbox to prevent health care professionals who are not involved in your care from viewing your personal information as these professionals are not within your "circle of care" and are therefore already not permitted to access your information on the basis of our policies and privacy laws.

You can submit your lockbox request in writing using our "Patient Lockbox Request" form, which you can get from your physician or health care provider or the Privacy Officer. The completed form should be given to your physician or health care provider or the Privacy Officer.

Lockbox requests are processed on a case-by-case basis. The Privacy Officer will review and respond to lockbox requests and will speak with your physician or health care provider. We may not be able to accommodate every request – but we will explain any limits with you. We will tell you when your lockbox is in place. You can also request that your lockbox be removed at any time by contacting your physician or the Privacy Officer.

Privacy Officer

<address and contact information>

Information and Privacy Commissioner/Ontario:[11]

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8 Canada

Telephone
Toronto Area: 416-326-3333
Long Distance: 1-800-387-0073 (within Ontario)

Appendix B

Patient Lockbox Request

Instruction for Patients

[11] The office responsible for reviewing the privacy-related decisions and practices of health care institutions, such as family health teams, investigating privacy complaints made under the access, privacy and personal health information laws, and educating the public about such laws and access and privacy issues.

You have the right to ask that we not share some or all of your health record with our staff and/or associated health care providers or ask us not to share your health record with your external health care providers (such as a hospital or specialist). This is informally known as asking for a "lockbox".

Before signing this form, please read our *Patient Lockbox Information Brochure: How to Restrict Access to your Health Record*. If you have any questions, please ask your physician or the Privacy Officer.

PATIENT INFORMATION (please print)

Last Name: _____ First Name: _____ Middle Initials: _____

Date of Birth: _____
(yyyy/mm/dd)

Mailing Address: _____

Telephone #: _____

IF YOU ARE MAKING THE REQUEST AS A SUBSTITUTE DECISION-MAKER (SDM), WE REQUIRE THE FOLLOWING INFORMATION ABOUT YOU: (please print)

Last Name: _____ First Name: _____

Mailing Address: _____

Telephone #: _____

Relationship to Patient: _____

LOCKING DETAILS

Please indicate below at which level you would like for your health record to be locked:

- ❑ Complete health record (everything)
- ❑ Specific visit: (enter date) _____
- ❑ Specific range of dates: from _____ to _____
- ❑ Other (Please provide as much detail as possible) _____

PATIENT ACKNOWLEDGMENT

I have read the *Patient Lockbox Information Brochure: How to Restrict Access to your Health Record.* The lockbox has been explained to me. The risks of placing a lockbox on records have been explained to me. I have had the chance to ask questions and my questions have been answered.

_____ _____ _____

(Name of Patient or SDM) **(Signature)** **(Date: yyyy/mm/dd)**

INTERVIEW WITH PATIENT/SDM (Internal Use) **Date of Request: _____**

(yyyy/mm/dd)

OUTCOME: ❑ Complete File Lock ❑ Specific Visit ❑ Specific range of dates ❑ Excluded Employee

Details:

_____

_____

_____

Copy Provided to Patient: ❑ Yes ❑ No

_____ _____ _____

(Name of Privacy Officer) **(Signature)** **(Date)**

Appendix G: Virtual visit consent form

Virtual Visit Consent

Please use the following script called the "Virtual Clinical Visit Consent" to explain to patients what a virtual visit is and is not and ask them to verbally agree to the terms (offer them the link on the website to the form or offer to email them a written copy of the script if they would like one).

Virtual Clinical Visit Consent– Script to be Read to Patients

Before we book a virtual visit, I need to explain a few things.

Description

- We use video and audio technology so we can see and hear each other.
- We recommend you be in a quiet place for your virtual visit so that others cannot overhear the session (unless you want to include others in your visit – please tell us who is with you).
- You will be asked for details of what is happening and your health history – these questions may be very personal and sensitive.
- Details of your virtual visit will be recorded in your health record just like in an in-person visit.
- We will not make a recording of the virtual visit. We ask that you not record the visit either.

Limits

- Virtual visits are not appropriate for emergencies – please call 9-1-1.
- If it is determined that you need a physical exam, you may still have to be assessed in person.
- Virtual service may not be available indefinitely – we may need to stop offering it at any time.

Privacy

- We have taken appropriate steps to preserve your privacy.
- However, we cannot provide you with the same guarantee of security and confidentiality as if you were seen in person.
- Virtual care has some privacy and security risks that your health information may be intercepted or unintentionally disclosed through physical or electronic eavesdropping or hacking or there could be technical failures.
- We recommend you take steps to participate in the virtual visit in a private setting, use an encrypted email service if available, and you should not use an employer's or someone else's computer/device as they may be able to access your information.
- Our staff who are doing the virtual visit may be working from home – they will also try to find a quiet place away from others in their household.

Risks

- It is possible there could be a problem with the technology and your session could be cut short or interrupted.
- The quality of the video or audio may not be good enough for a health care provider to assist you virtually or could negatively impact the quality of the care you receive.

You can withdraw your consent to participate in virtual care at any time.

A copy of this information is available on our website or I could email it to you.

Do you have any questions?

Are you happy for me to book you a virtual visit based on those limits and risks? [NOTE TO STAFF: Record consent in the chart]