System Coordinated Access
Privacy Guide

Find us on the web: **www.systemcoordinatedaccess.ca/privacy**

Published: December 2017

Guide Index

Personal Health Information Protection Procedure Guide

Appendices

Incident Management Artifacts

Privacy Supporting Documents

In Ontario, the law governing the privacy of Personal Health Information is called the Personal Health Information Protection Act, 2004 (PHIPA). The law establishes mandatory rules and responsibilities for the management of Personal Health Information (PHI) and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.

Purpose:

This Guide will provide you with the support required to meet the regulatory obligations of PHIPA in a way that guides you through practical daily operations. The guide was structured around the 10 Fair Information Principles of the Canadian Standards Association's Model Code for the Protection of Health Information and meets the Privacy by Design fundamentals.

The Privacy Policy has been created to comply with the requirements established by the Ministry of Health and Long-Term Care (MOHLTC), Connecting Ontario and the Information Privacy Commissioner of Ontario and is intended to ensure alignment with eHealth Ontario.

The organization has implemented these controls to the best of our ability given the system functionality available to us. We agree to take actions reasonable to ensure compliance with these policies and processes under the authority provided to us.

The format has been categorized to align with the 10 Privacy Principals and eHealth Ontario Connecting Ontario Privacy Policies as follows:

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

Definitions:

Personal Health Information (PHI) is generally defined as any identifying information about an individual in oral or recorded form that relates to their physical or mental health. Examples include family health history, health card number, and any information that identifies an individual and links them to a health care provider.

Personal Information (PI) or sensitive **personal information** (SPI), as used in **information** security and privacy laws, is **information** that can be used on its own or with other **information** to identify, contact, or locate a single person, or to identify an individual in context.

Health Information Custodian (HIC) is a person or organization – named in PHIPA – that delivers health care services, as defined in PHIPA. Examples are Physicians, hospitals, pharmacies, laboratories, community care access centres and Long Term Care Facilities.

A HIC has custody or control of PHI as a result of the work it does. The HIC has the right to deal with the PHI and create records, as well as the responsibility to maintain the confidentiality and security of the PHI. Though the HIC is the owner of the materials and systems in which information is recorded (e.g. paper charts, computers or information technology systems), patients are the owners of their PHI.

Health Information Network Provider (HINP) is an individual or organization that provides services to two or more HICs primarily to enable them to use electronic means to disclose PHI to one another. The eHealth Centre of Excellence (eCE) acts in this capacity in a number of business relationships.

IS Solution is defined as any information system that contains personal information or personal health information under the custody or control of the organization could refer to either internal electronic medical records system, provincial assets or other.

Electronic Service Provider (ESP) is an individual or organization that provides a means of storing &/or sharing PHI electronically such as the electronic medical record contained in your facility.

Provincial Asset is defined as any one or more provincial repository managed through eHealth Ontario or any other organization providing access to Personal Health Information

1. **PHIPA requires anyone who is in control of personal health information (PHI) to designate a person responsible for the protection of PHI within their facility. Privacy Contact Person: (Privacy Officer)**

    a. Responsibilities:
        i. Assess information collected and how it is used and disclosed;
        ii. Conduct a privacy impact assessment and privacy audit of information use;
        iii. Develop privacy policies, procedures and tools; and
        iv. Inform and assist with all privacy matters
        v. Follow through with direction received from Information & Privacy Commissioner of Ontario regarding the resolution of privacy issues as they are addressed in a timely manner.

2. **Consent: (Refer to Consent Management Protocol for eReferral Consent)**

    a. Implied Consent is assumed between HICs providing direct health care to resident. To assume this consent model you must provide the following:
        i. Post Privacy Statement in public area. Privacy Statement must clearly explain why you are collecting PHI and how it is used
        ii. Give patient the information they need to understand why their information is being collected and how it will be used or disclosed.
        iii. Advise patient they may withhold consent and clearly explain the advantages and disadvantages of their choice

b. Express Consent
    i. Obtain express consent if you are disclosing personal health information to someone other than a HIC or for the purpose other than providing or assisting in providing health care. Consent can be either verbal or written. Best practice suggests that verbal consent be documented in the medical record.
    ii. Patient express consent provided at time of self-referral is accomplished through the acceptance of an online consent form which is stored electronically as part of the audit log.

c. Withdrawal of Consent
    i. Patients may withdraw their consent at any time.
    ii. Patients who want to withdraw their consent must notify you that they no longer consent to your collection, use and disclosure of their personal health information.
    iii. Patient/ Substitute Decision Makers (SDM) have the right to impose a Consent Directive (Lock Box) on the access/use of their Personal Health Information (PHI) in whole or in part.
    iv. Patient/ Substitute Decision Makers (SDM) wishing to impose their right to a Consent Directive (Lock Box) must complete the **Withdrawal of Consent Form**. This form is then to be forwarded to the Privacy Officer who will incorporate it into the patient's Medical Record or Electronic Medical Record (EMR).
    v. A patient's withdrawal has no effect on information you collected, used or disclosed before the patient withdrew consent, but has effect from the time it is received.
    vi. If the withdrawal of consent will compromise patient care, be sure to discuss the effect of the withdrawal with the patient and carefully document the withdrawal and these discussions in the patient's health record.

d. Capacity to Consent
    i. To be capable of consenting, a patient must be able to understand:
        1. The information needed to make a decision on whether or not the patient should consent to the collection, use or disclosure of personal health information, and
        2. The consequences of giving, withholding or withdrawing consent.
        3. When a patient is not capable of providing consent you may get consent from a Substitute Decision Maker (SDM) (ranked in order as listed) from the patient's:
            a. Guardian (if guardian has the authority to make such decisions)
            b. Attorney for personal care or attorney for property (if the attorney has authority)
            c. Representative (appointed by Capacity Board)
            d. Spouse or partner
            e. Child, custodial parent, or children's aid society or other person legally entitled to give or withhold consent in place of a parent)
            f. Parent with access rights
            g. Brother or sister, and

h. Any other relative (related by blood, marriage or adoption).
i. If the patient has died, you can get consent from the patient's estate trustee or someone in charge of administering the patient's estate.
j. To consent for a patient, the person must be:
   - included in the list above,
   - available and capable of consenting,
   - at least 16 years old or the patient's parent,
   - willing to assume responsibility for giving or refusing consent,
   - free of any court order or separation agreement prohibiting them from having access to or consenting for the patient, and
   - the highest ranked person on the list of potential substitute decision-makers who is available and capable of consenting.

   If a patient is not capable of consenting and you cannot find anyone capable of consenting on their behalf and willing to take on this role, contact the Public Guardian and Trustee who can consent for the patient.

   The Public Guardian and Trustee can also give consent if two or more equally high-ranking substitute decision-makers disagree about whether to consent. The Public Guardian and Trustee breaks the deadlock.

4. Children and Teenagers
   Children of any age are presumed to have the capacity to consent to the collection, use and disclosure of their personal health information. Do not presume capacity if it is not reasonable.
   For children under 16, a parent or other lawful guardian may consent to the collection, use or disclosure of personal health information even if the child has capacity, unless the information relates to:
   a) Treatment within the meaning of the Health Care Consent Act, 1996 about which the child has made his or her own decision, or
   b) Counseling in which the child had participated on his or her own under the Child and Family Services Act.

   If there is a conflict between the child and the parent, the capable child's decision prevails with respect to the consent.

3. Collection:

a. We will collect personal health care information for health care purposes in compliance with the law.
b. Our Privacy Statement identifies the purpose for collection of Personal Health Care Information (PHI).

c. Collection of PHI for other than health care purposes requires express consent from patient

d. Authorized individuals in patient's circle of care will have access to PHI for the purpose of ensuring holistic care as noted in chart below:
The term "circle of care" includes but is not limited to:
- Health care practitioners and groups of health care practitioners,
- Public and private hospitals,
- Pharmacies
- Laboratories
- Ambulance services,
- Community care access corporations,
- Community service providers (defined in the Long Term Care Act)
- Psychiatric facilities
- Independent health facilities
- Homes for the aged, rest homes, nursing homes, care homes and homes for special care and
- Community health or mental health centers, programs and services whose primary purposes are providing health care
- Those who provide health care or assist in providing health care to a particular patient.

e. We will provide training to staff explaining who may collect personal health information; when consent is required, and restricting collection of personal health information to the purposes identified in our Privacy Statement. Privacy training will occur for each new hire and will be reviewed with all staff members annually.

f. The Privacy Officer will regularly review the collection practices to ensure practices are in compliance with the law.

4. Use:

a. We use personal health care information for health care purposes in compliance with the law.
b. Our Privacy Statement identifies the purpose for use of personal health care information.
c. Use of personal health information for other than health care purposes is outlined requires express consent from patient.

5. Disclosure:

a. We will disclose personal health care information for health care purposes in compliance with the law.
b. Our Privacy Statement identifies the purpose for disclosure of personal health care information.
c. Disclosure of personal health information for other than health care purposes requires express consent from patient.
d. Patient must supply express consent if Personal Health Information is to be released to an individual who is not a Health Information Custodian providing direct patient care to the

individual. Best practice is to document the express consent in the patient's medical record.

e. If the patient has a Consent Directive (Lock Box) then the Patient PHI Release Letter must accompany information forwarded to authorized individuals. It will be noted on the **Personal Health Information Release Notice** that they are receiving an incomplete medical record.

f. Fees for the collection and distribution of PHI, if required, to an authorized individual are based upon the current OMA rate and will be paid by the patient prior to release of information.

g. Guidelines for a request for access to PHI in the form of a subpoena/summons/warrant, police acting on behalf of a coroner, and related contexts.
A patient's PHI will only be released to police upon the presentation of one of the following:
A valid court order, Subpoena, Coroner's Writ, or a Search Warrant, or original written authorization from the patient allowing release of the information requested.
When possible, the signature is verified with the signature on the patient's agreement.
The information provided should only include that part of the record requested in the warrant.
The release of information should be documented on the chart including:
    - the name of the police officer requesting the information
    - the police force the police officer is affiliated with
    - the date and time
    - the information that was released to the police officer (e.g., list the report name, the dates of the report's release and any other pertinent information)
    - the documentation that was presented by the police officer for the release of information (e.g., the court order, search warrant, subpoena etc.)

h. In the case of a patient's death, PHI (including the death certificate) can only be provided to the estate trustee or executor of the will. Confirmation/proof must be received (and included into patient's medical record). Acceptable forms of proof include copy of the will (first and last page) or a legal document or lawyers letter identifying the trustee.

Refer to Appendix D for Disclosure Tables

6. Accessing Health Records:

Except under special circumstances, patients have the right to access their personal health records. Patients or their Substitute Decision Makers may request access to their personal health records in writing by completing the **Request Access to Personal Health Record Form.**

Access requests can be made through the HIC who has custody of the PHI or by contacting the HINP who will assist in facilitating the request.

When a request has been received:

a. Verify the patient's identity or SDM authority (SDM will be noted in patient's medical record as scanned document or by way of Doctors note).

b. Locate record and verify it is the correct PHI for the request by confirming name, date of birth, or health card number. If record cannot be located contact the requestor in writing asking for more information.
c. Collection and release of PHI will be completed within 30 days of receipt of written request.
d. Written notice of extension should explain when you will respond and why the extension is needed. An extension cannot exceed an additional 30 days.
e. Determine if one of the legal exceptions applies to providing access. *See Appendix E*.
f. If a legal exception applies:
    i. Tell the requestor in writing that access is being refused, in whole or in part, and why you are doing so,
    ii. Where possible, sever the record and provide access to the part of the record where no legal exception applies,
    iii. Tell the requestor about your complaints procedures, and that if the requestor is not satisfied with your resolution of the complaint, the requestor can complain to the Commissioner, and
    iv. In some circumstances, you cannot even tell the requestor that a personal health record exists.
g. If no legal exception applies arrangements can be made for viewing the personal health record in the presence of the Privacy Officer who will ensure that the record is not altered in any way.
h. Any questions regarding the personal health record should be directed to the patient's family physician.
i. Document the access in the patient's personal health record.
j. Fees, if applicable, may be charged based on cost recovery for collection and distribution of PHI.
k. Extensions: If an extension is needed in order to respond, written notice will be provided to the requestor.
l. Refusal of Access: If access is refused, written notice will be provided to the requestor.

Refer to Appendix E – Guidelines for Refusal of Access Table

7. Correcting Health Records:

If a patient or substitute decision maker has been granted access to personal health information and thinks that the record is not correct or complete, the patient or substitute decision maker may ask you, in writing by completing the **Correction to Personal Health Information Form**, to correct the record. When a request has been received:

a. Verify the patient's identity or substitute decision maker's authority.
b. Verify that the patient or SDM has a right of access to the personal health record.
c. Ensure the request for correction relates to a personal health record **created by you or your staff**.
d. The Physician who initially charted the record in question will validate the request and correct the personal health record within 30 days.

e. When making a correction you must record and date the correct information in the record and cross out the incorrect information (without obliterating it). If that is not possible, date and label the information as incorrect.
f. Advise the patient on how the correction was made and when.
g. You do not have to correct a record if:
    i. The incorrect record was not made by you and where you do not have sufficient knowledge, expertise and authority to correct this record.
    ii. If you reasonably believe that the request for correction is frivolous, vexatious or made in bad faith.
    iii. If the patient has failed to demonstrate that the record is not correct or complete, or
    iv. If the patient has not given you the information you need to make the correction.
    v. NOTE: You do not have to correct a professional opinion or observation made in good faith about a patient.
h. Fees may be charged to obtain and correct a record based on cost recovery. Patients will be given an estimate of the cost prior to the record being amended.
i. Extensions: If an extension is needed in order to respond, written notice will be provided to the requestor.
j. Refusal of Correction: If correction is refused, written notice will be provided to the requestor. Patients may contest the refusal by completing a Statement of Disagreement and forwarding to the Privacy Officer or Privacy Commissioner/Ontario.
k. If a Statement of Disagreement (SOD) has been completed, a notation will be put in the patient's medical record by the Privacy Officer.
l. The SOD will be included in release of PHI when it pertains to that particular record being disclosed and when asked in writing to be provided by an authorized individual.

8. Storage and Retention:

a. Personal health information is stored in a reasonably secured manner and in accordance with the prescribed retention requirements, if any.
b. When patients have requested access to their own personal health records, those records will be retained for as long as needed to allow the patients to exhaust any legal recourse involving the request.
c. PHI is not stored in eReferral system. The eReferral and supporting documents are deleted from the system once the recipient has unlocked the file request and accepted the referral. An audit log of the referral is available online for both the sender and recipient.

Refer to Appendix F for Retention Periods for Health Records for Physicians Tables

9. Safeguarding PHI and Disposal:

Providing safeguards to PHI is a legal requirement of PHIPA. Anyone with PHI in their custody/control is required to provide at least the following minimum safeguards:

Safeguards

a. Protect the information during collection, storage, transfer and disposal.
b. Appropriate safeguards must be in place to provide security to PHI stored electronically throughout PHI lifecycle which includes the ability to produce audit logs with specific details of who accessed PHI, when it was accessed and what PHI was viewed, printed, modified or destroyed.
c. Appropriate safeguards must be in place to provide security to PHI in paper form. Restricted access, locked cabinets and environmental considerations must be in place to ensure safety of PHI throughout PHI lifecycle.
d. The technological security (ie: passwords, encryption and firewalls) and reasonably ensure that wireless data has appropriate level of security (currently WPA2 Encryption with 32 character password. Network is not broadcasted and access is controlled to Doctors).
e. The administrative controls (ie: security clearances, access restrictions, staff training and confidentiality agreements)
f. Within reason, ensure that anyone given access to the restricted areas containing PHI are in understanding of their responsibilities to uphold Patient Privacy and have signed the appropriate **Confidentiality Agreements**.
g. Best practice suggests that removal of any equipment containing PHI from the building should be recorded on a log out sheet indicating date, person removing equipment and reason for removal.

Disposal

a. Personal health information will be disposed of in a secure manner.
b. Hard copy records will be shredded.
c. Electronic records will either be physically destroyed (ie: CD), or magnetically erased or overwritten.
d. A log will be filled out stating the names of the patients whose records where disposed of, the dates the records were disposed of and the disposal procedure. This electronic log will be kept by the Privacy Officer Indefinitely.
e. All paperwork containing PHI will be either shredded on the spot or placed in our locked shredding boxes to be shredded by the contract company hired to accommodate this requirement. Note that contract with 3rd parties who may have exposure/access to PHI must be in place clearly identifying responsibilities of 3rd party and ensuring that the 3rd party has appropriate mechanisms in place to secure PHI and train staff on appropriate handling of PHI.

10. Transfer:

a. When a patient's personal health information is transferred to another facility or physician, you must keep the original and only transfer a copy. This is a requirement of the *Medicine Act.*
b. The transferred record must be clearly marked as a copy of the original file.

c. Reasonable efforts to notify patients prior to transferring medical records will be made or as soon as possible afterwards.
d. Fees, if any, for the collection and distribution of PHI to an authorized individual are based upon cost recovery.

11. Incident Management & Communication Policy:

Incident Management is defined as the ability to provide end-to-end management of a series of events that are initiated in response to a privacy or security breach.

Incidents can originate from the HIC (participant), Non-HIC (participant), the HINP or the ESP or the incident could also be reported by the resident/patient.

The Information and Privacy Commissioner of Ontario recommends that anyone with PHI in their custody and/or control develop an incident protocol to handle any potential privacy or security breaches. The protocol enables the HICs and their partners in the same sharing environment to respond quickly and in a coordinated way during a breach. The protocol also defines the roles and responsibilities of each party to ensure that investigation and containment are effective and efficient, and remediation easier to implement.

All actual or suspected incidents are to be **IMMEDIATELY** brought to the attention of Executive Director & Privacy Lead. A determination is made of whether a breach or security incident has actually occurred. The preliminary investigation is to take place as soon as possible but no later than 3 days after report of the incident.

Privacy Analyst will keep Incident Log and all incident reports stored electronically and will review periodically to identify any patterns or trends in incidents. If patterns or trends are identified the privacy team will within a reasonable period of time, identify any administrative, physical or technical safeguards that must be implemented to prevent or minimize the risk of future incidents.

The organization's Privacy Team will work with ClinicalConnect and/or eHealth Ontario Privacy Office and the sponsored entities to identify and investigate any actual or suspected incidents and will follow appropriate incident management processes where required to remediate the incident.

A Privacy Breach is defined as:

- Inappropriate collection, use, disclosure, retention or destruction of PHI
- Any contravention of PHIPA
    - Examples:
        - Viewing PHI for a reason other than health care
        - Losing a print-out that contains patient identifying information
        - Sharing a patient's PHI with a person who is not involved in patient's care

A Security Incident is defined as:

- Security-related event that equates to potential or possible breach
- Examples:
    - An unencrypted laptop that stores PHI is stolen
    - Electronic medical reports print to the wrong destination
    - Virus or malware infection

Please note that in all incidents/breaches the disciplinary course of action will be decided upon by Participant and could result in suspension, termination, reporting to regulatory body/college and Information Privacy Commissioner of Ontario which may result in fines.

Special Note:
Incident response is a mandate of the Information Privacy Commissioner/Ontario and specific requirements must be fulfilled within a specified period of time. Participants who choose not to cooperate fully with an incident investigation are at risk of being reported to the IPC and removed from the eReferral project.

Internal Process

1. Obtain details regarding the incident or suspected incident from the person reporting it and the person suspected of causing the incident.
2. Record details on the **Incident Management Reporting Form**
3. Determine if the incident is defined as a privacy breach or security incident and follow correct incident management protocol specific to that type of incident.

Privacy or Security Breach

1. Once it has been determined that there has been a breach the incident is immediately contained by one or more of the following actions:
    a. Individual access to the system is removed
    b. Remote access to the system is disengaged
    c. Equipment is collected for evidence & re-securing

2. a) Full investigation is conducted within 3 business days. Completion of the incident report will identify the following:
    - The date and time of the incident;
    - The name of the individual(s) involved in the incident;
    - A description of the nature, scope and cause of the incident;
    - A description of the PHI which was subject to the incident;
    - If the incident involved one HIC or Non-HIC or multiple organizations
    - The measures implemented to contain the incident;
    - The measures that have been implemented or will be implanted to remediate and prevent similar incident.

    b) Incident report is given to HINP Privacy Officer if the incident involved more than one HIC or participant and a coordinated effort will be established to ensure appropriate measures

are put in place to contain and remediate the incident. The HINP will keep an Incident Registry Log of incidents for future review and lessons learned purposes.

If notice to patient is required, a decision is made as to whether the patient's physician or the Privacy Officer will provide communication. If the incident involved more than one HIC or participant the Privacy Officer for the HINP will work with all parties &/or the most responsible organization involved to coordinate notification to patient.

Notice will be incorporated into patient's medical record. Patient notification should contain the following information :

- The date and time of the incident;
- A description of the nature and scope of the incident;
- A description of the PHI which was subject to the incident;
- The name of the individual(s) that caused or contributed to the incident, where the name is determined to be relevant (e.g., intentional unauthorized collection, use or disclosure of PHI by an individual);
- The measures implemented to contain the incident;
- The name of the investigator;
- A summary of the measures that have been implemented or will be implemented to prevent similar incidents in the future;
- The steps that the patient can take to protect their privacy or minimize the impact of the incident, if applicable; and
- Information on how to make a complaint to the Information Privacy Commissioner of Ontario.

Security Incident

All security incidents not involving PHI should be immediately directed to the IT Administrator & cc'd to the Executive Director who will follow processes outlined in the Security Guide. Security incidents that do involve PHI will follow the privacy incident process noted previously.

Key Questions

There are important decisions that have to be made to properly implement your Incident Management Process. The following is a list of questions that could be used to assist your organization in implementing an internal Incident Management Process and an integrated Incident Management Process:

1. Do staff know who to report an incident to? Is there any existing incident reporting process or procedure in place? How do staff know about this process/procedure?
2. Do your residents/patients and 3rd party know whom to contact if they want to report an incident? How is this information communicated to residents/patients and 3rd parties (e.g. brochures, posters, 3rd party agreements)?
3. What is the mechanism to determine if the incident involves other HICs? Who should be conducting the triage or determination? Are there tools such as an audit log or audit reports to assist in the determination process?

4. Is the incident reporting, handling and escalation process part of any training, education and awareness for staff?
5. Do all users know the HIC's Privacy Officer's contact information?

Process Map and Process Description

The following processes describe the key elements of sustainable incident management process for each of the 3 scenarios.

Each process is represented both as a map and as written outline (table) of the steps involved. HICs/participants can use these as a reference.

The term 'process map' refers to a diagram that describes a workflow or set of connected activities. It shows who is responsible (the role names in each horizontal row), what needs to be done (the boxes), and when each activity happens (the order of the boxes).

Provided are 3 Incident Management scenarios involving privacy and security incidents:

Scenario 1 – Incident detected by the HIC
Examples could include:

- Resident/patient medical record were lost
- User account and password was compromised
- EMR was accessed inappropriately

Scenario 2 – Incident reported by resident/patient or 3rd party to the HIC
Examples could include:

- Resident/patient reports: "My ex-spouse working in your organization accessed my medical information and used it in our child custody case. Why can he/she access my medical records?"
- Someone found printed resident/patient information on HIC letterhead in a public area

Scenario 3 – Incident reported by 3rd party to ESP
Examples could include:

- The document shredding service provider reports to ESP that documents collected from shredding bins are lost on way to the depot before shredding
- ESP reports possible intrusions from unknown source into network, data may have been subject to unauthorized access

Figure 1: Scenario One Incident Detected by the HIC Management Process 1.0

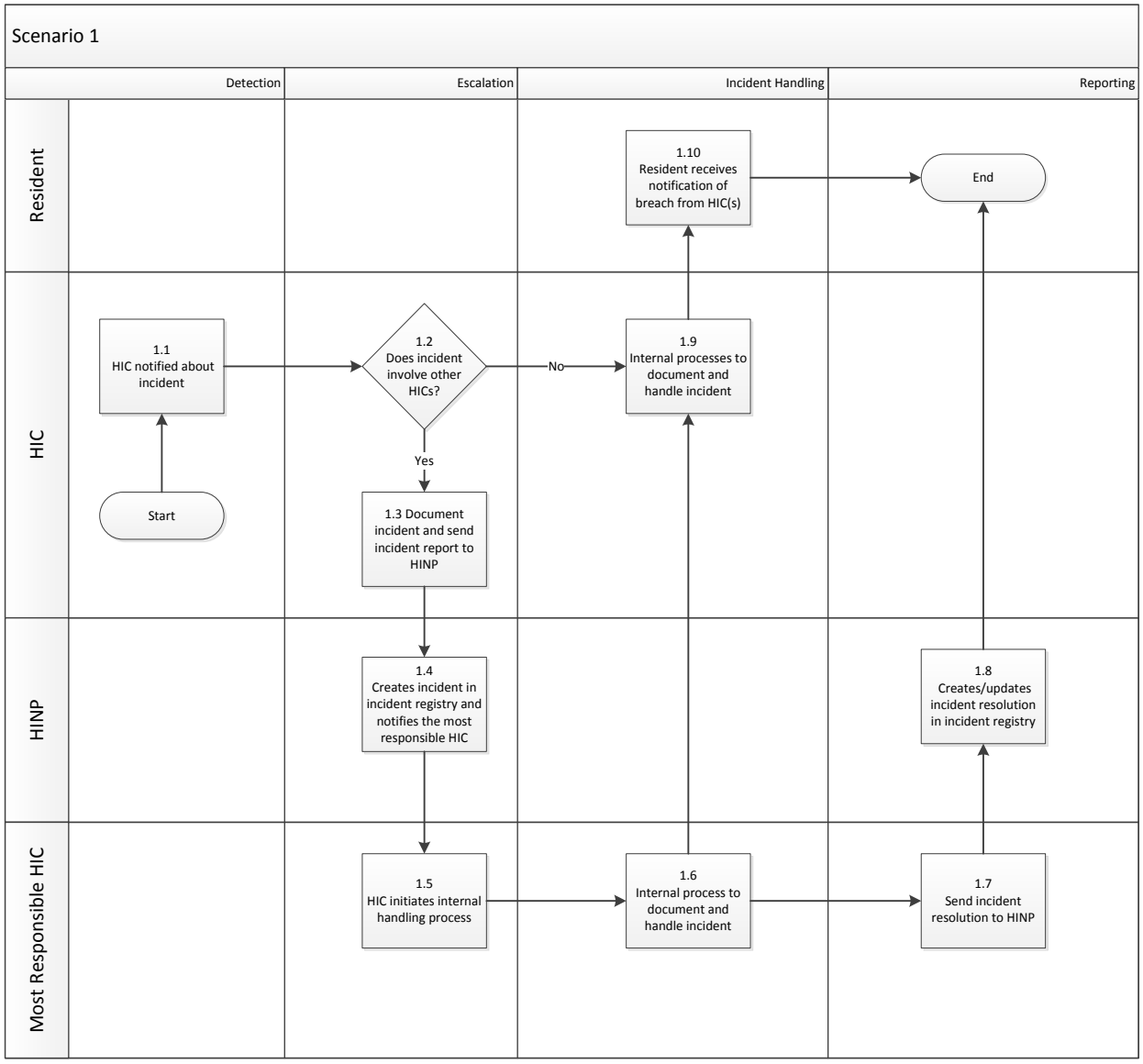

Table 1: Scenario One: Incident detected by the HIC

Ref. No.	Task/Step	Owner	Artefacts**
Scenario 1 – Incident detected by the HIC Examples could include: • Resident/patient medical record were lost • User account and password as compromised • EMR was accessed inappropriately			
1.1	The incident is detected and brought to the attention of the HIC or HIC staff. The incident is reported to the HIC Privacy Officer.	HICs	Telephone call or face to face meeting
1.2	HIC Privacy Officer triages the reported/detected incident - containment is the first priority - and determines if the incident involves other participants/HICs. • If the incident involves other HICs, HIC Privacy Officer follows HINP Incident Management Procedures (Ref 1.4) • If the incident does not involve other HICs then the Privacy Officer follows own internal incident management process (Ref 1.9)	HIC	Incident Management Reporting Form
1.3	HIC Privacy Officer documents the incident and sends the Incident Management Report Form to the HINP Privacy Officer within 3 days	HIC	Incident Management Reporting Form
1.4	HINP Privacy Officer creates an incident in the Incident Registry, initiates cooperative investigation with most responsible HIC and assists with containment if necessary	HINP	Incident Registry Log
1.5	HINP Privacy Officer and most responsible HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HINP & HIC	
1.6	HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HIC	
1.7	HIC privacy officer updates the Incident Management Reporting Form with incident resolution and sends to the HINP Privacy Officer	HIC	Incident Management Reporting Form
1.8	HINP Privacy Officer updates Incident Registry with details of incident resolution	HINP	Incident Management Reporting Form

Ref No	Task/Step	Owner	Artefacts**
1.9	HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HIC	
1.10	Resident/patient receives notification from HINP HIC regarding the privacy reach of their medical record.	HIC	Patient Notice

*Note: in a situation where multiple HICs are investigating an incident that may affect the same resident/patient, the HINP Privacy Officer is to coordinate the notification of the resident/patient, in order to avoid the resident/patient receiving multiple notifications from different HICs. The HINP will facilitate among the various HICs involved in order to develop the best notification approach for the resident/patient. This could be in the form of a joint letter.

Figure 2: Scenario 2 – Incident Reported by Resident/3rd Party to HIC Management Process 2.0

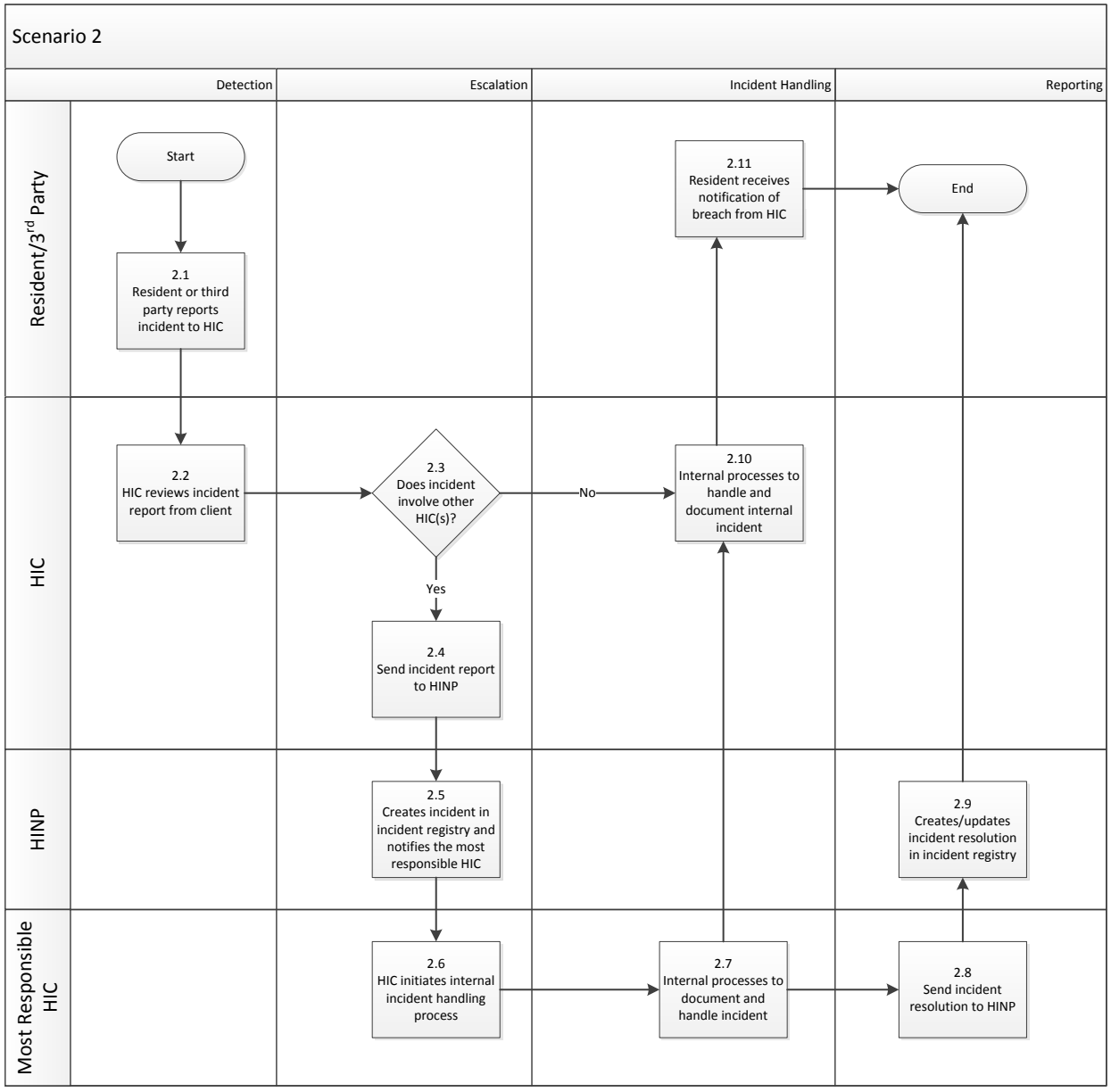

Table 2: Scenario 2 – Incident reported by resident/patient or 3rd party to the HIC

Ref. No.	Task/Step	Owner	Artefacts**
Scenario 2 - Incident reported by resident/patient or 3rd party to HIC Examples could include: • Resident/patient reports: "My ex-spouse working in your organization accessed my medical information and used it in our child custody case. Why can he/she access my medical records?" • Someone found printed resident/patient information on HIC letterhead in a public area			
2.1	Resident/patient or 3rd party contacts HIC Privacy Officer or other HIC staff to report the incident.	Resident/ Patient or 3rd Party	Telephone call or face to face meeting
2.2	• HIC Privacy Officer reviews the Incident Report from client	HIC	
2.3	HIC Privacy Officer triages the reported/detected incident - containment is the first priority - and determines if the incident involves other participants/HICs. • If the incident involves other HICs, HIC Privacy Officer follows HINP Incident Management Procedures (Ref 2.4) • If the incident does not involve other HICs then the Privacy Officer follows own internal incident management process (Ref 2.10)	HIC	Incident Management Form
2.4	HIC Privacy Officer documents the incident and sends the Incident Management Report Form to the HINP Privacy Officer within 3 days	HIC	Incident Management Reporting Form
2.5	HINP Privacy Officer creates an incident in the Incident Registry, initiates cooperative investigation with most responsible HIC and assists with containment if necessary	HINP & HIC	Incident Registry Log
2.6	HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HIC	
2.7	HIC Privacy Officer executes internal processes to document and handle reported/detected incident	HIC	Incident Management Reporting Form

Ref No	Task/Step	Owner	Artefacts**
2.8	HIC privacy officer updates the Incident Management Reporting Form with incident resolution and sends to the HINP Privacy Officer	HIC	Incident Management Reporting Form
2.9	HINP Privacy Officer updates Incident Registry with details of incident resolution	HINP	Incident Registry Log
2.10	HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HIC	
2.11*	Resident/patient receives notification from HINP HIC regarding the privacy breach of their medical record.	HIC	Patient Notice

*Note: in a situation where multiple HICs are investigating an incident that may affect the same resident/patient, the HINP Privacy Officer is to coordinate the notification of the resident/patient, in order to avoid the resident/patient receiving multiple notifications from different HICs. The HINP will facilitate among the various HICs involved in order to develop the best notification approach for the resident/patient. This could be in the form of a joint letter.

Figure 3: Scenario 3 – Incident Reported by 3rd Party to ESP Management Process 3.0

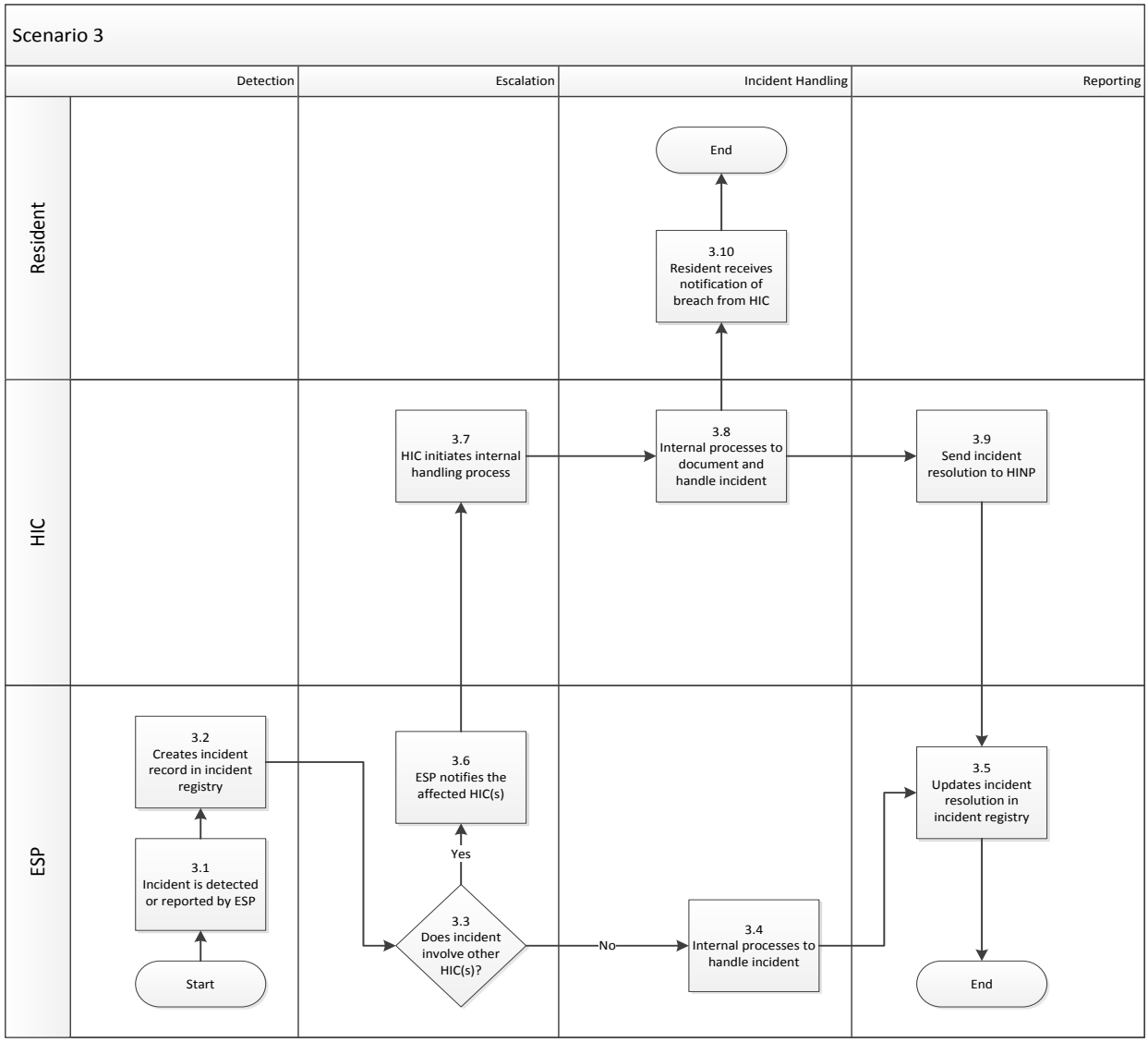

Table 3: Scenario 3 - Incident reported by 3rd party to ESP

Ref. No.	Task/Step	Owner	Artefacts**
Scenario 3 – Incident reported by 3rd party to ESP Examples could include: • The document shredding service provider reports to ESP that documents collected from shredding bins are lost on way to the depot before shredding • ESP reports possible intrusions from unknown source into network, data may have been subject to unauthorized access			
3.1	3rd party reports incident to ESP	3rd party	Telephone call or face to face meeting
3.2	ESP Privacy Officer creates incident record in Incident Registry Log	ESP	Incident Registry Log
3.3	HIC Privacy Officer triages the reported/detected incident - containment is the first priority - and determines if the incident involves other participants/HICs. • If the incident involves other HICs, HIC Privacy Officer follows HINP Incident Management Procedures (Ref 3.6) • If the incident does not involve other HICs then the Privacy Officer follows own internal incident management process (Ref 3.4)	HIC	Incident Management Form
3.4	ESP Privacy Officer initiates internal process to handle the reported incident	ESP	
3.5	ESP Privacy Officer updates the incident management reporting form with incident resolution detail	ESP	Incident Management Reporting Form
3.6	ESP Privacy Officer creates an incident in the Incident Registry, initiates cooperative investigation with most responsible HIC and assists with containment if necessary	ESP & HIC	Incident Registry Log
3.7	HIC Privacy Officer executes investigation and internal processes to handle reported/detected incident	HIC	

Ref No	Task/Step	Owner	Artefacts**
3.8	HIC privacy officer updates the Incident Management Reporting Form with incident resolution and sends to the HINP Privacy Officer	HIC	Incident Management Reporting Form
3.9	HIC Privacy Officer documents the incident and sends the Incident Management Report Form to the HINP Privacy Officer within 3 days	HIC	Incident Registry Log
3.10*	Resident/patient receives notification from HINP HIC regarding the privacy reach of their medical record.	HIC	Patient Notice

*Note: in a situation where multiple HICs are investigating an incident that may affect the same resident/patient, the HINP Privacy Officer is to coordinate the notification of the resident/patient, in order to avoid the resident/patient receiving multiple notifications from different HICs. The HINP will facilitate among the various HICs involved in order to develop the best notification approach for the resident/patient. This could be in the form of a joint letter.

12. Auditing Requirements

PHIPA requires that access to health information be on a need-to-know basis. To meet this requirement, HICs and participants are required to have controls in place that regulate access and log activity as well as procedures to regularly review the logs and user access activity. Access logs play an important role in the access review process and during incident investigations.

The eReferral Service Provider shall run routine system audit logs to ensure system integrity and to cooperate with HINP Privacy Officer should an incident investigation be initiated and be able to respond to the incident inquiry within 3 days of the date of receipt. The eReferral Service Provider shall be able to supply the following:

- Name of patient referred, from whom, to whom and on what date
- Name of PHI records transferred via the eReferral System
- Date the PHI was removed/deleted from the eReferral System

Participating organizations who have an electronic medical record (EMR) are also required to perform routine system audit logs to ensure system integrity and be able to participate fully in an incident investigation which may include providing a log of who accessed specific information on a particular date and time.

Internal electronic medical records should be audited to ensure access to PHI is on a need-to-know basis and is being accessed by appropriate individuals. Internal EMR should be reviewed for access to self, family member or colleague, access to patient not being provided direct patient care by individual, any inappropriate printing or copying of records.

Each participating organization with an electronic medical record shall at a minimum perform monthly routine system and access audits to ensure the integrity of their system and access to PHI is appropriate for the individual's role. These audits are to be stored electronically in such a way that they can be made available to the HINP Privacy Office within 3 days from the date of request should an incident occur in accordance to the Incident Management Policy.

In the case of an incident investigation each participating organization involved in the incident will cooperate fully with the audit investigation and should be able to supply the HINP Privacy Officer with ad hoc audits on specific individuals having access to the EMR and specific patients whose PHI is stored within the EMR within 3 days from the date of request.

Participating organizations who use paper charts to store PHI are expected to maintain the files in a secure environment in alignment with PHIPA regulations and IPC best practice guidelines as identified in the Personal Health Information Protection Procedure Guide Section 9 Safeguarding PHI & Disposal.

All participating organizations who are using the eReferral System must be familiar with how to run an internal audit of their eReferrals and must be able to supply the HINP Privacy Officer with a copy of such audits upon request within 3 days of the date of request.

13. Role of Authorized Individual

PHIPA stipulates that individuals should only be provided access to the PHI required in the performance of their 'role' or 'duties' and that participating organizations who have PHI in their custody or control will provide sufficient awareness to individuals who have access to PHI.

The following serves as a guideline based on common Privacy Policies created by the Information Privacy Commissioner of Ontario, eHealth Ontario and Connecting Privacy Committee. It is suggested that these expectations be presented to the Authorized User during orientation and be reviewed annually thereafter

a. Ensure authorized individuals are in compliance with their Privacy Responsibilities as outlined in Agreement:
    i. Authorized individuals are using computers built in security features such as password protections and adhere to password changes every 90 days. Passwords are not to be shared and must be kept private and secure at all times.
    ii. Authorized individuals are not to install any unauthorized software or connect any unauthorized devices to their computers or use computers for unauthorized purposes.
    iii. Authorized individuals may not copy or transmit any information from their computers unless authorized. This includes using email or instant messaging unless using the software provided for that intended purpose.
    iv. Authorized individuals are to take reasonable measures to avoid accidental exposure of PHI like "reading over the shoulder" or discussing PHI at a loud volume in an area where it may be overheard by unauthorized individuals.

v. Authorized individuals will maintain a 'clean desk policy' by ensuring to close down access/log off computer when not at work station and file PHI safely away.
vi. Authorized individuals should not discuss PHI over cell phone or portable devices. If a recorder has been used, appropriate measures must be taken to ensure it is kept in a safe environment when not in use and all dictations are fully erased when complete.
vii. Authorized individuals are to take appropriate reasonable measures to protect PHI in its collection, distribution and disposal in all forms (verbal, paper & electronic). All hard copy records are to be shredded in approved shredding boxes and all electronic devices containing PHI are to be returned to IT department for appropriate disposal.
viii. Authorized individuals are not to access PHI of anyone they know personally (eg. relative, neighbor, friend). If this information is accidentally accessed or if it is accessed as a direct request of PHI Custodian, notification must be given to Privacy Officer indicating date, PHI accessed and reason.
ix. Authorized users are to report privacy breeches or suspicion of privacy breeches to Privacy Officer.
x. If there is a need for Authorized individuals to remove PHI from building, either electronic or hard copy, reasonable means of securing information until it has reached its final destination is required and appropriate disposal of it when no longer required
xi. Authorized individuals who have remote access to PHI must have appropriate security systems in place and have signed the appropriate Confidentiality Agreement. They must ensure at all times that PHI is being protected from unauthorized individuals.
xii. Authorized users are required to attend Privacy Training Sessions as mandated.
xiii. Authorized individuals must continue to uphold the guidelines stipulated in the Privacy Agreement even after employment/affiliation terminates. Failure to do so may result in legal action.

14. Assurance Practices

- We will conduct PIA & TRAs as requested to fulfill legislative requirements
- We will comply with the completion of eHealth Ontario privacy & security operational self-assessments annually
- Auditing & monitoring activities related to the ConnectingOntario Solution will occur in accordance with PHIPA and eHealth Ontario practices and procedures implemented in respect of solution(s)
- Annual privacy and security training will be provided to all staff and agents who have been given access to the EHR

Appendix A: Consent Management Protocol

All Parties are expected to obtain knowledgeable, express consent from Clients/Patients to collect and disclose PHI for the purpose of making a referral. The Health Information Network requires that Authorized Users confirm that they have obtained such consent by documenting such in the electronic referral process prior to transmitting PHI. If an Authorized User indicates that they have not obtained consent, they should not proceed with a referral.

Each Party must have in place a Privacy Statement and a Privacy Policy that documents what PHI they collect, for what purposes, and under what circumstances PHI will be disclosed to other parties. The Privacy Statement and Privacy Policy must be made available to Clients/Patients and must be eHealth Ontario compliant.

Clients/Patients have the right to withdraw their consent to share PHI at any time. Each Party must have a policy that describes how they manage consent, including the withdrawal of consent by Clients/Patients.

If a Client/Patient has withdrawn consent to share PHI with the Receiving Party after a referral has been made the Originating Party shall:

a) in the case that the Receiving Party has not yet downloaded the PHI, unbook the appointment, which will have the effect of removing the PHI from the Health Information Network and making it unavailable to the Receiving Party;
b) in the case that the Receiving Party has downloaded the PHI, contact the Receiving Party's Privacy Officer and inform her that the Client/Patient has withdrawn consent and request that she destroy the PHI and related documentation immediately, per the Party's Consent Management Policy

Appendix B: Completing the eHealth Ontario Privacy & Security Assessments

Purpose:

While not mandatory to participate in the SCA Program, the purpose of completing the eHealth Ontario viewer assessments will provide the HIC & participant with the awareness required to ensure appropriate deployment of the tool and that they have met their privacy requirements as per PHIPA.

Privacy Legislation
In Ontario, the Personal Health Information Protection Act (PHIPA) is in place to govern the protection of personal health information (PHI); this includes rules regarding the collection, use, and disclosure of PHI by Health Information Custodians (HIC).

Those who may have access to a patient's PHI are those who are providing direct patient care, considered to be in the 'circle of care' or those assisting with the provision of care.

Privacy Obligations

Health Information Custodians have a duty to ensure compliance with PHIPA and to ensure anyone accessing PHI in their control has sufficient privacy legislation awareness. In order to comply successfully the Canadian Standard Association (CSA) Model Code for the Protection of Personal Information can be followed. The Model Code is informed by the following 10 Principals*: Accountability, Accuracy, Identifying Purposes, Safeguards, Consent, Openness, Limiting Collection, Access, Limiting Use, Disclosure and Retention, Challenging Compliance*.

Benefits of Privacy Compliance

Working through the eHealth Privacy and Security Viewer Assessments and using the resources available will allow applicants to meet PHIPA requirements, fulfill the CSA Model Code and meet the requirements to access eHealth Initiatives. Breaches of confidentiality have severe consequences as well as a negative impact on careers and the care patients receive. Having the compliance measures in place allows piece of mind that legislative requirements are being met for your organization. It also helps to build a culture of patient safety, privacy, and confidentiality. When patients feel secure that their PHI is being handled confidentially, they are more open with their health care team and happier with the care they receive.

Please note that if you have chosen to adopt the privacy policies and supporting documents provided you do not need to complete the assessments at this time.

If you have your own policies and processes established and would prefer to use your own processes, please forward a copy of your existing policies to the Privacy Coordinator at your Regional Delivery Partner.

A gap analysis will be conducted for you by the Privacy Coordinator. Should any deficiencies be identified a report with suggested compliances will be provided.

Appendix C: Disclosure Tables

Disclosure Tables

The issue of disclosure is complex. The following tables provide examples of some of the most common disclosures to help you determine when disclosure must or can be made.

Mandatory Disclosure

The Act specifically permits the disclosure of personal health information for a number of purposes as required by other statutes. Consent is not required for these specific purposes. For example, you are required to provide the following information:

To whom disclosure must be made	What information must be disclosed	Authority
Aviation Medical Advisor	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	*Aeronautics Act*
Chief Medical Officer of Health or Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain communicable diseases	*Health Protection and Promotion Act* *Personal Health Information Protection Act*
Chief Medical Officer of Health or Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain SARS	*Public Hospitals Act*
Children's Aid Society	Information about a child in need of protection (e.g., abuse or neglect)	*Child and Family Services Act*
College of a regulated health care professional	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 also include your name as the individual filing the report.	*Regulated Health Professions Act*

To whom disclosure must be made	What information must be disclosed	Authority
College of a regulated health care professional	A written report, within 30 days, regarding revocation, suspension, termination or dissolution of a health care professionals' privileges, employment or practice for reasons of professional misconduct, incapacity or incompetence	*Regulated Health Professions Act*
College of Physicians and Surgeons of Ontario	Information about the care or treatment of a patient by the physician under investigation	*Public Hospitals Act* Notice must be given to the Chief of Staff and the administrator of the hospital
Coroner or designated Police Officer	Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice) Information about a patient who died while in the hospital after being transferred from a listed facility, institution or home Information requested for the purpose of an investigation	*Coroners Act*
Minister of Health and Long-Term Care	Information for data collection, organization and analysis	*Public Hospitals Act*
Ontario Health Insurance Plan	Information about the funding of patient services	*Public Hospitals Act*
Order, warrant, writ, summons or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.	*Personal Health Information Protection Act*
Physician assessor appointed by the Ministry of Health and Long-Term Care	Information to evaluate applications to the Underserviced Area Program	*Public Hospitals Act*
Registrar General	Births and deaths	*Vital Statistics Act*
Registrar of Motor Vehicles	Name, address and condition of a person who has a condition that may make it unsafe for them to drive	*Highway Traffic Act*
Subpoena issued by an Ontario court	Information outlined in the subpoena	*Personal Health Information Protection Act*

To whom disclosure must be made	What information must be disclosed	Authority
Trillium Gift of Life Network	For tissue donations or transplants purposes, notice of the fact that a patient died or is expected to die imminently (not in force yet)	*Trillium Gift of Life Network Act* *Consent must be decided jointly with the Network to determine the need to contact the patient or substitute decision-maker*
Workplace Safety and Insurance Board	Information the Board requires about a patient receiving benefits under the *Workplace Safety and Insurance Act*	*Workplace Safety and Insurance Act*

The following tables outline examples of where personal health information may be disclosed.

Disclosure for Health Related Programs and Legislation

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Ambulance services operator or delivery agent or the Minister	Administration/enforcement of the *Ambulance Act*	No	*Ambulance Act*
Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences or Pediatric Oncology Group of Ontario	To analyze or compile statistical information	No	*Personal Health Information Protection Act regulations*[†]
Chief Medical Officer of Health, Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	To report communicable diseases	No	*Health Protection and Promotion Act*
College of Pharmacists Investigator	Administration/enforcement of the Drug Interchangeability and Dispensing Fee Act	No	*Drug Interchangeability and Dispensing Fee Act*

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
College under the RHPA, or Social Work and Social Services Act, or Board of Regents under the Drugless Practitioners Act	Administration/enforcement of the relevant statutes	No	*Personal Health Information Protection Act*
Deputy Minister of Veteran's Affairs or person with express direction	To review the information about the care received by a member of the Canadian Armed Forces	No	*Public Hospitals Act*
Individual assessing patient capacity, who is not providing care to the patient	To assess capacity under the Substitute Decisions Act, Health Care Consent Act, or Personal Health Information Protection Act	No	*Substitute Decisions Act; Health Care Consent Act; Personal Health Information Protection Act*
Minister Inspector	Administration/enforcement of the *Public Hospitals Act*	No	*Public Hospitals Act*
Minister Inspector	Enforcement of the Drugs and Pharmacy Regulation Act	No	*Drugs and Pharmacy Regulation Act*
Public Guardian and Trustee	To investigate an allegation that a patient is unable to manage their property	No	*Public Hospitals Act; Personal Health Information Protection Act*
Public Guardian and Trustee, Children's Lawyer, Residential Placement Advisory Committee, Registrar of Adoption of Information, Childrens' Aid Societies	To carry out their duties and, for the PGT, to investigate serious adverse harm resulting from alleged incapacity	No	*Personal Health Information Protection Act*

Disclosure to Lawyers, Insurance Companies, Adjusters, Investigators

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Lawyers, Insurance Companies, Adjusters on behalf of a patient	To assist a patient with a claim or proceeding	Yes	*Express consent*
Lawyers, Insurance Companies, Adjusters, Investigators on behalf of a third party, if the third party is an agent or former agent of the physician	To assist the third party with a proceeding	No	*Personal Health Information Protection Act*

Disclosure to Legal Authorities and Law Enforcement

Person requesting health record or patient information	Purpose	Consent Needed	Authority to release information
Head of penal or custodial institution or an officer in charge of a psychiatric facility where the patient is being lawfully detained	To assist with health care or placement decisions	No	*Personal Health Information Protection Act*
Investigator or Inspector	To conduct an investigation or inspection authorized by a warrant or law	No	*Personal Health Information Protection Act*
Police without a warrant	Legal authorities and law enforcement	Yes	*Express consent*
Police without a warrant	Where there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm	No	*Personal Health Information Protection Act*
Probation and Parole Services	Legal authorities and law enforcement	Yes	*Express consent*

Appendix D: Guidelines for Refusal of Access (Legal Exception)

In each of the following situations, you should provide access to the part of the record that is not impacted by the reason for refusal and that can reasonably be severed from the record.

Reason for refusal of access	**Follow-Up Notification to Requestor**	
	State you are refusing the request (in whole or in part) and the reason for refusal	State you are refusing to confirm or deny the existence of any record
The record contains quality of care information	✕	
The record contains information collected/created to comply with the requirements of a quality assurance program under the *Health Professions Procedural Code* that is Schedule 2 to the *Regulated Health Professions Act*	✕	
The record contains raw data from standardized psychological tests or assessments	✕	
The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requestor	✕	
The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded		✕
The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded		✕
Granting access could reasonably be expected to result in a risk of serious harm to the patient or to others (Where this is suspected you may consult a physician or psychologist before deciding to refuse access)		✕
Granting access could lead to the identification of a person who was required by law to provide the information in the record		✕
Granting access could lead to the identification of a person who provided the information in the record in confidence (either explicitly or implicitly) and it is considered appropriate to keep the name of this person confidential		✕

Reason for refusal of access	Follow-Up Notification to Requestor	
	State you are refusing the request (in whole or in part) and the reason for refusal	State you are refusing to confirm or deny the existence of any record
The request for access is frivolous, vexatious or made in bad faith	✕	
The identity or authority of the requestor cannot be proven by the requestor	✕	

Appendix E: Retention Periods for Health Records

Retention Periods for Health Records for Physicians (Private Office Records)

Patient Care Records

Adults: 10 years after the last entry date, or until the physician stops practicing, or for risk management purposes.

Minors: 10 years after the day the patient turns or would have turned 18 or until the physician stops practicing, or for risk management purposes.

Special Notes

Family medicine and primary care physicians should refer to the CPSO's special transfer and disposition rules if they plan to stop practicing.

Dispensing physicians should refer to Supplementary Tables A and B for retention rules relating to dispensing medications.

Investigations

If a notice for an investigation or inspection under the *Regulated Health Professions Act*, *Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed.

Patient Access Requests

A personal health record cannot be disposed of if the patient the record relates to seeks access to those records and has not yet exhausted all avenues allowing for access.

Lawsuits

Where a claim of negligence may arise:

Adults: A minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred

Minors: A minimum period of 15 years from the date the patient turned 18

In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer.

The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case.

For specific retention periods regarding individual cases, consult your lawyer.

Retention Periods for OHIP Records for Physicians

The *Health Insurance Act* requires that records be maintained to demonstrate that:

- an insured service was provided
- the physician provided these services
- the service was medically and therapeutically necessary

Records should be kept a minimum of 10 years, in line with statutory retention periods for clinical records, to assist in proving billing was necessary.

Retention Periods for Research Records for Physicians

General Principle

Identifying data should be retained only as long as necessary to fulfill the research purpose; however,

- in a case where a claim of negligence may arise, records should be kept longer
- due to the complexity of the discoverability rules in relation to claims of negligence, for record retention periods for specific research projects, consult your lawyer
- If research is conducted without patient consent, the researcher receiving the information must follow any return restrictions imposed by the originating health information custodian

Personal Health Information Standardized Incident Reporting Form

When completing this report please provide as much detail as possible:

INCIDENT INFORMATION

1. Date and time the incident occurred

2. Person(s) responsible for incident

3. How was the incident identified? (e.g. investigation of same last name report, complaint from patient or staff member, identified by outside agency/HIC?)

4. Provide the sequence of events

5. Description of the PHI that was involved in the incident breach (e.g. dates the PHI was viewed, type of PHI viewed)

6. Description of the Security incident (e.g. location, type of equipment)

INCIDENT CONTAINMENT/REMEDIATION

1. Describe measures taken to contain the incident (e.g. access to system(s) revoked on (date))

2. Describe any remediation measures taken (e.g. retraining scheduled (date), internal reminder sent to staff)

3. Describe any remediation measures that will be taken (e.g. attend departmental meeting)

4. What are the timelines and person(s) responsible for implementing remediation measures

INCIDENT REPORTING

1. Has the IPC/Ontario been notified? If yes, please explain and provide date of notification, if no, please explain

2. Has the affected individual(s) been notified? If yes provide date of notification & details of notification

3. Have any other regulatory bodies been notified (e.g. regulatory college, other, law enforcement)? If yes, please explain and provide date of notification

4. Provide sequence of events for notification

Incident Investigated by: _____

Date Incident Investigation Completed: _____

Date incident reported to HINP Privacy Lead: _____

Resident/Patient Incident Reporting Form

1. Complainant Information to be completed by Resident/Patient		
First Name	Last Name	Initial
Date of Birth (dd/mm/yyyy)	Email	
Phone No.	Alternate Phone No.	
Street Address (street, city, province, postal code)		
2. Complainant Description In your own words, provide the details of your complaint, the names of individuals or healthcare organizations involved if you know them, and the date when it happened. Attach additional pages if more space is needed.		
Date of Occurrence (dd/mm/yyyy)		
3. Purpose of Use		
I understand that my personal information will be used for the purpose of resolving my complaint.		
Signature	Date (dd/mm/yyyy)	

Incident Management – Patient Notice

The patient notice could be complex such as a Standard Form with headings that provide areas (boxes) that can be filled in with specific details or as simple as a letter addressed to the patient.

My suggestion is to generate a personalized letter. This will provide the resident/patient with the assurance that their issue has been dealt with in a confidential personal fashion by an individual concerned about them and their situation rather than providing them with the coldness of a pre-generated 'fill in the blank' form or notice.

The following explains what the letter must contain:

Notice will be incorporated into patient's medical record. Patient notification should contain the following information:

- The date and time of the incident;
- A description of the nature and scope of the incident;
- A description of the PHI which was subject to the incident;
- The name of the individual(s) that caused or contributed to the incident, where the name is determined to be relevant (e.g., intentional unauthorized collection, use or disclosure of PHI by an individual);
- The measures implemented to contain the incident;
- The name of the investigator;
- A summary of the measures that have been implemented or will be implemented to prevent similar incidents in the future;
- The steps that the patient can take to protect their privacy or minimize the impact of the incident, if applicable; and
- Information on how to make a complaint to the Information Privacy Commissioner of Ontario.

Authorization to Disclose Personal Health Information Consent Form

I, _____, hereby authorize [*Your company/organization's name*] to disclose the following personal health information:

_____

_____

(Description of personal health information to be disclosed)

to

_____

_____

_____

_____
(Name and Address of person/agency to receive personal health information)

From the records of _____
(Name of Patient – Please Print in Block Letters)

Date of Birth: _____ Health Card Number: _____

I hereby waive any and all claims against the Physicians and Staff at [*Your company/organization's name*] in connection with the disclosure of this personal health information.

Request to Access Personal Health Record

Information and Instructions:

We will provide you with access to your personal health record, unless a legal exception applies. We will review all health record access requests, and will make every effort to respond to your request within 30 days.

PART A: REQUESTOR INFORMATION:

Patient Contact Information:

Last Name	First Name
Mailing Address	
Telephone Number	Date of Birth

If you are a substitute decision maker, your contact information:

Last Name	First Name
Mailing Address	
Telephone Number	Date of Birth

Note: Include copies of documents that prove your authority as a substitute decision maker.

PART B: ACCESS REQUEST

1. Please describe what you need and include details that will help us locate the record (ie: dates, name of healthcare provider, etc.)

2. How would you prefer to access this information? Please check off:

☐ Receive hard copies of originals

☐ Receive electronic copies of originals (please provide storage medium ie: CD, USB, etc.)

☐ Examine originals in office

I hereby waive any and all claims against the Physicians and Staff at (insert your office name) in connection with the release of this personal health information.

Signature: _____

(Patient or Substitute Decision Maker) (Relationship to Patient)

Relationship to Patient: _____ Date: _____

Witness: _____ Date: _____

PART C: RESPONSE TO ACCESS REQUEST (For internal use only)

1. Date request was received: _____
2. Response:

☐ Access request granted

☐ Access request not granted

☐ Access request granted in part

3. Reason access request was not granted: _____
4. Extension Request
    a. Date of Extension: _____
    b. Reason for Extension: _____
    c. Date patient notified: _____
5. Date Personal Health Information was accessed: _____
6. Physician Authorization:_____ Date: _____

Patient Personal Health Information Release Letter

(Date)

(Add Recipients Name)

(Add Recipients Address)

To whom it may concern:

RE: (Add Patients Name and DOB)

As authorized, please find enclosed medical records for the above noted patient.

As a courtesy to you, we would like to bring to your attention that:

- □ This is a complete file.
- □ This is an incomplete file. Some information has been withheld due to a Medical Consent Directive requested by patient.

Should you require further information or assistance kindly contact us directly.

On behalf of:

(Insert privacy officer's name or physician name & address)

Express Consent to the Collection, Use and Disclosure of Personal Health Information

I, _____, have reviewed written statement concerning the collection, use and disclosure of personal health information.

I understand that {insert office name} is seeking my express consent for it to collect, use and/or disclose my personal health information from me or from the person acting on my behalf (Substitute Decision Maker) to:

_____

_____

(Insert reason for Express Consent)

I understand that {Insert Name} only collect, use and disclose my personal health information with my consent, unless a particular collection, use or disclosure is permitted or required by law without my consent.

I also understand that I can refuse to sign this consent form and/or withdraw my consent at any time by completing the Withdrawal of Consent form available from {Insert Name} Privacy Officer.

I hereby authorize {Insert Name} to collect, use and disclose my personal health information for the purposes that I have indicated above.

Patient Name: _____

Patient Signature: _____

Witness: _____

Date: _____

Withdrawal of Consent

I, _____, wish to withdraw my consent to any further use or disclosure by (insert office name) of my personal health information to **OR** I wish to put the noted conditions on any further use or disclosure of my personal health information:

_____

_____

_____

_____

It is understood that the consent directive applies only to the PHI which has already provided and not to PHI which might be provided in future:

- *Personal Health Information Protection Act* (PHIPA) permits certain collections, uses, and disclosures of the PHI, despite the consent directive;
- health care providers may override the consent directive in certain emergency circumstances, for the purpose of mitigating significant risk of harm to an individual or group of persons. All overrides will be documented in the patient's medical record
- the consent directive may result in delays in receiving health care, reduced quality of care due to the health care providers lacking complete information about the student, and the health care provider's refusal to offer non-emergency care.
- Health information custodians are required by law to notify recipients when they share a record of PHI that there is PHI subject to a consent directive

Patient Name: _____

(Please Print in Block Letters)

Request to Correct Personal Health Record

Information and Instructions:

We will correct health record information if it is demonstrated, to our satisfaction, that the record is not correct or complete for the purpose for which we collect, use or disclose the information. We will review all health record correction requests, and will make every effort to respond to your request within 30 days.

PART A: REQUESTOR INFORMATION

Patient Contact Information:

Last Name	First Name
Mailing Address	
Telephone Number	Date of Birth

If you are a substitute decision maker, your contact information:

Last Name	First Name
Mailing Address	
Telephone Number	Date of Birth

Note: Include copies of documents to prove your authority as a substitute decision maker.

PART B: CORRECTION REQUEST

3. List or attach the correction requested, with reasons for the correction.

4. How do you wish to receive notification of the correction? Please check off:

☐ In writing

☐ By telephone

I hereby waive any and all claims against the Physicians and Staff at (insert your organization name) in connection with the correction of this personal health information.

Signature: _____
(Patient or Substitute Decision Maker) (Relationship to Patient)

Relationship to Patient: _____ Date: _____

Witness: _____ Date: _____

PART C: CORRECTION REQUEST RESPONSE (For internal use only)

1. Date request was received: _____
2. Response:

☐ Correction Made

☐ Correction Not Made

☐ Refusal letter (with reason) Date sent:_____

☐ Statement of Disagreement attached to PHI record

3. Reason correction request was not granted: _____
4. List names, contact information and comments of any individuals consulted regarding this request: _____
5. Extension Request
    a. Date of Extension: _____
    b. Reason for Extension: _____
    c. Date patient notified: _____
6. Date Personal Health Information was corrected: _____

Sample Correction Request Extension

(Date)

(Name)

(Address)

(Postal Code)

Dear: [Requestor's Name]

RE: Request for Correction to Personal Health Information for [Patient's Name and/or Health Record #]

An extension of _____ days is required to address your request to correct the personal health information of the individual named above. This extension is required for the following reasons:

[Reason for Extension].

If you have any concerns or questions please contact me at [your phone number].

If I am unable to resolve your concerns, you may file a complaint with the Information and Privacy Commissioner/Ontario, who may be contacted at 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8 (1-800-387-0073).

Sincerely,

[Your name]

Privacy Officer,

[Your company name/organization]

Sample Correction Request Refusal

Date

Name

Address

Postal Code

Dear: [Requestor's Name]

RE: Request for Correction to Personal Health Information for [Patient's Name and/or Health Record #]

Your request for a correction to the personal health information of the individual named above has been declined for the following reason:

[Reason for Declining Request].

If you have any concerns or questions please contact me at [your phone number].

If I am unable to resolve your concerns, you may file a complaint with the Information and Privacy Commissioner/Ontario, who may be contacted at 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8 (1-800-387-0073).

Sincerely,

[Your name]

Privacy Officer,

[Your company/organization]

(insert organization name)
Staff/Agent CONFIDENTIALITY AGREEMENT

Name: _____
(Please print)

Definition of Personal Information

Personal Information includes any factual or subjective information, recorded or not, and in any form, about an identifiable individual, but does not include the name, title or business address or telephone number of any employee of an organization. Personal Health Information is included in Personal Information, and is comprised of information related to an individual, whether living or deceased, including: (**i**) information concerning the physical or mental health of the individual; (**ii**) information concerning any health service provided to the individual; (**iii**) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (**iv**) information that is collected in the course of providing health services to the individual; (**v**) information that is collected incidentally to the provision of health services to the individual.

Definition of Confidential Information

Confidential Information includes information, in any format, created or received by (insert organization name) in the course of its business, including patient information, human resources information, financial or legal information.

1. During my association with (insert organization name), I will have access to personal information and material relating to patients, employees, and other individuals which is of a private and confidential nature.

2. At all times, I shall respect the privacy and dignity of patients, employees and all associated individuals.

3. I shall treat all administrative, financial, patient, employee and other records as confidential information, and I will protect them from improper disclosure. I shall not collect, use or disclose any confidential information without authorization nor will I discuss, divulge, or disclose confidential information to others, unless it is necessary to fulfill my duties and responsibilities. If I am unsure if I have the authorization to access, use or disclose confidential information, I agree to seek clarification on this issue from (insert privacy officer name).

4. I shall ensure that confidential information is not inappropriately accessed, used or disclosed either directly by me, or by virtue of my signature, password or security access to premises or systems. I have read and understand the Responsibilities of Authorized Individuals materials Appendix A.

5. Violations of this policy include, but are not limited to: **(i)** accessing confidential information that I do not require for the purposes of fulfilling my duties and responsibilities; **(ii)** misusing, disclosing without proper authorization, or altering patient or personnel information, and disclosing to another person my user name and/or password or failing to adequately protect my password.

6. I shall only access, process, and transmit confidential information using authorized hardware and software, or other authorized equipment, as required by the duties of my role.

7. I am aware that (insert organization name) has policies and procedures regarding privacy, confidentiality and security of Personal Information and I understand that it is my responsibility to be familiar with these policies and procedures and to comply with their provisions.

8. If I have been given access to EMR from my home computer. I am aware that (insert organization name) has policies and procedures regarding privacy, confidentiality and security of Personal Information and I understand that it is my responsibility to be familiar with these policies and procedures and to comply with their provisions. I will only access EMR from my home computer and will not share my access ID with any other individuals. I am aware that my usage will be monitored, and that home access will be revoked if any irregularities are noted.

9. I am aware that photographs are often taken during social, educational, and patient-centred situations. I give consent for my image and/or name to be used:

Web-site applications YES _____ NO _____

Poster presentations YES _____ NO _____

Power Point Presentations YES _____ NO _____

Newsletters YES _____ NO _____

Office displays YES _____ NO _____

I also release and forever discharge (insert organization name), its agents, officers and employees from any and all claims and demands arising out of or in connection with the use of said photographs/images, including but not limited to, any claims for invasion of privacy or defamation.

_____ _____ _____

Name (Please Print) **Signature** **Date**

_____ _____ _____

Name of Witness (Please Print) **Signature** **Date**

Privacy Statement

The Physicians and Staff at (insert organization name) are bound by law and ethics to safeguard your privacy and the confidentiality of your personal information.

We collect, use and disclose your personal health information to:

- treat and care for you;
- get payment for your treatment and care (from OHIP, WSIB, your private insurer or others);
- plan, administer and manage our internal operations;
- conduct risk management and quality improvement activities;
- teach;
- conduct research;
- compile statistics;
- comply with legal and regulatory requirements and
- fulfill other purposes permitted or required by law.

Your request for care implies consent for our collection, use and disclosure of your personal health information for purposes related to your care as noted above. All other purposes would require your express consent.

We may share your health information with other healthcare providers to continue to care for you. This includes healthcare providers at other organizations who can view your information through shared electronic systems/databases to continue to care for you.

You have the right at any time to withhold or withdraw your consent to disclose personal health information. You will be required to sign the appropriate form which will be forwarded to the Privacy Officer.

For a complete review of our Privacy Policy, or to raise a concern, please speak with (insert privacy officer name & phone number)

The Information and Privacy Commissioner of Ontario is responsible for making sure that privacy law is followed. For more information about your privacy rights, or if you are not able to resolve a problem directly with our facility and wish to make a complaint, contact: Information and Privacy Commissioner of Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8; Toll Free: 1-800-387-0073; www.ipc.on.ca.