Strathmere Lodge

	Manual	{{ manual }}
	Policy Number	{{ policy_id }}
	Original Date	{{ original_date }}
	Revised/Reviewed Date	{{ reviewer_date }}
	Issued By	{{ reviewer_name }}
	Approved By	{{ approver_name }}

Policy Statements

Middlesex County is committed to a high standard of privacy and has implemented policies and procedures to ensure personal health information (PHI) is kept confidential and secure while allowing for the effective delivery of health care.

The Legislative Services Manager/Clerk or delegate for the County of Middlesex is the Privacy Contact for Middlesex County and contact information is clerk@middlesex.ca

Strathmere Lodge under the authority of Middlesex County collects and uses PHI for the purposes of providing or supporting health care and for other purposes that are permitted or required by law. Furthermore, Strathmere Lodge staff may only use PHI within the limits of each staff member's role.

The policies and procedures within this document apply to PHI in all forms as it pertains to Clinical Connect i.e., verbal, written and electronic. Staff who print hard copies of PHI must comply with the limitations on the use and disclosure of PHI as described above.

Strathmere Lodge provides health care under an implied consent model and obtains knowledgeable consent of patients for the collection, use, or disclosure of PHI, as required by law. PHI can be collected, used, or disclosed without the knowledge and consent of patients only where it is permitted or required by law.

This policy is required to be read in conjunction with service area specific Personal Health Information Privacy Policies and Procedures

Strathmere Lodge provides a public friendly version of the Strathmere Lodge Privacy Policy (Privacy Notice).

Table of Contents **Pages**

Glossary of Terms Used in this Document

Term	Meaning

Access Requests Related to Logs	• A patient/SDM have the right to request the following reports for ClinicalConnect/EHR system:
	  ○ Report of who has viewed the individual's PHI in the system
	  ○ Report of the history of consent directives applied and removed in the system
	  ○ Report of all instances of consent directive overrides.

Consent Directive (or lock box)	• A patient's withdrawing consent to collect, use, or disclose their PHI for health care purposes. Also commonly known as a consent directive, withdrawal of consent, patient instruction, lockbox or mask.
Information Privacy Commissioner (IPC)	• The government office in Ontario that is the oversight body for the Personal Health Information Protection Act (PHIPA).
Lock box	• A patient's withdrawing consent to collect, use, or disclose their PHI for healthcare purposes. Also commonly known as a consent directive, withdrawal of consent, patient instruction, block, or mask.
Medical Record Personal Health Information (PHI)	• Recorded personal health information.
Privacy Breach	• Defined term under PHIPA s. 4 and includes all information in Middlesex County's medical records and the PHI viewed in ClinicalConnect/EHR system.
Program Office	• Any event where patient information is collected, used, or disclosed counter to PHIPA, Strathgmere Lodge policies, or obligations defined in agreements binding Strathmere Lodge. Privacy breaches may be real or suspected.

Term	Meaning
Request for Access	• The organization responsible for managing a specific EHR system e.g., Hamilton Health Sciences is the program office for ClinicalConnect
Request for Correction	• The right of a person to request a copy of or to see his or her health information.
Ontario's Electronic	• The right of a person to request a correction to his or her PHI if it is inaccurate or incomplete.
Health Record (EHR) System	• ConnectingOntario – Clinical Data Repository (CDR) • ClinicalConnect Viewer • Ontario Laboratory Information System (OLIS) • Diagnostic Imaging Common Services (DI CS) • Digital Health Drug Repository (DHDR) • May also include other provincial repositories in the future.
Substitute Decision Maker (SDM)	• A person who has the authority to make a decision on an individual's behalf, including making request for access, correction, consent directives, and so forth. The individual may be mentally incapable, or the patient may be deceased, in which case the estate trustee in relation to the individual's PHI is the rightful SDM.
Verify Identity	• The process of confirming that the person is who they say they are, and confirming their authority to act as SDM (if relevant).

Application

Middlesex County is both a custodian under PHIPA and an organization that is an institution under the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*).

Subject to certain exceptions, Strathmere Lodge is governed by PHIPA, not MFIPPA, with respect to Personal Health Information in its custody or under its control. All other records in the custody or under the control of Middlesex County are subject to the requirements of MFIPPA.

This policy sets out Strathmere Lodge privacy-related operating practices for Personal Health Information as governed by PHIPA.

Requests for information in the custody or under the control of Middlesex County made under MFIPPA are subject to the applicable policies of the County of Middlesex.

Privacy Related Operating Practices

I. Request for Access

Key points

A Patient/SDM may ask to see or to be provided with copies of their medical records created by Strathmere Lodge. Requests may be verbal or written. Strathmere Lodge responds to such requests within 30 calendar days or notifies the patient in writing if an extension is required.

Operating Practices

1. When a patient asks staff to see or to be provided with a copy of their medical record held at Strathmere Lodge, staff should show or create a copy of the record if it is easy to do so (e.g., showing the patient your screen or printing the record).
2. If staff cannot show or give a copy of the record to the patient, staff must direct the requestor to contact the Privacy Contact and provide their contact information.
3. The Privacy Contact shall follow these steps:

3.1 Ask the requestor to complete Strathmere Lodge's *Request for Access Form* found in Appendix A, and note on the form the date the completed form was returned.

3.2 Verify the identity of the requestor by asking for photo identification. If a SDM is making the request on behalf of a patient, validate the authority of the SDM by following the steps outlined in the *Confirming Authority to Act as Substitute Decision Maker* section of Appendix B – *Identity Verification Standards*.

3.3 Decide whether to charge or waive a fee to cover the cost of printing the medical record. If applicable, tell the requestor how much they will be charged before preparing a copy of the record and do not change it once the requestor agrees to the fee[1].

3.4 Determine whether any information in the medical record should not be given to the requestor[2]. The reason for not releasing some or all PHI must be consistent with PHIPA ss. 8 or 52.

3.5 When responding to the requestor, the Privacy Contact must do one of the following:

- Give a complete copy of the records requested;
- Give only some of the records requested if a legal exception applies;
- Not give any of records that are requested if a legal exception applies; or
- Notify the patient in writing that Middlesex County requires an additional 30 days to respond.

If the request is refused in whole or part, the Privacy Contact must inform the requestor in writing of their right to make a complaint to the IPC. A *Request for Access Response Template* can be found in Appendix C.

---

[1] The IPC Order HO-009 established what is "a reasonable fee for access requests" i.e., $30 for the first 20 pages and 25 cents for every additional page.

[2] Exceptions include but are not limited to 1) PHI that is expected to result in serious harm to treatment or recovery 2) information that is part of a Quality Assurance Program, 3) raw data from standardized psychological tests or assessments 4) record that is subject to a legal privilege, disclosure is prohibited under MFIPPA etc.

3.6 Retain a copy of the request form and any related correspondence for a period of two years.

4. Access Requests Related to ClinicalConnect/EHR System

4.1 Requests for access to PHI in ClinicalConnect/EHR System, including Access Requests Related to Logs must be directed to the Privacy Contact.

4.2 If the access request relates to PHI that was solely contributed to the ClinicalConnect/EHR by Middlesex County, the Privacy Contact must follow the operating practices above beginning with step No. 3.

4.3 If the request relates to PHI contributed to ClinicalConnect/EHR system by another HIC or multiple organizations, the Privacy Contact will redirect the requestor to the appropriate program office and provide contact information (refer to Appendix F - *eHealth Ontario Contact Matrix*).

II. Request for Correction

Key Points

Patients or their SDMs may ask Strathmere Lodge to correct their medical record if the information is out-of-date, inaccurate, or incomplete. Strathmere Lodge honors correction requests from patients who have previously accessed their medical record. Strathmere Lodge responds to correction requests within 30 calendar days or notifies the requestor in writing if an extension is required.

Operating Practices

1. Refer all correction requests from patient/SDM to the Privacy Contact.

2. The Privacy Contact shall follow these steps:

2.1 Ask the requestor to complete Strathmere Lodge's *Request for Correction Form* found in Appendix D, and record on this form the date that the completed form is returned.

2.2 Verify the identity of the requestor by asking for photo identification. If the SDM is making the request on behalf of a patient, validate the authority of the SDM by following the steps outlined in Appendix B - *Confirming Authority to Act as Substitute Decision Maker*.

2.3 Discuss the correction with the appropriate clinician to determine whether or not to change the information[3]. The reason for not making some or all of the requested changes must be consistent with PHIPA s. 55.

2.4 Respond to the requestor within 30 days of having received the request. A *Request for Correction Response Template* can be found in Appendix E. When responding to the patient, the Privacy Contact must do one of the following:

- Make the correction;
- Notify the requestor that the request has been refused; or
- Notify the requestor in writing that an additional 30 days is required to respond to the request.

2.5 If the correction is granted, the Privacy Contact strikes out the previous information in the medical record (leaving it readable) and records the new information. If asked to do so, inform any other clinics or health care providers to which Strathmere Lodge disclosed the information of the change if it may impact the patient's care.

2.6 If the correction is refused, the Privacy Contact will inform the requestor in writing of their right to make a complaint to the IPC. The Privacy Contact or delegate must also ask the requestor if they would like to attach a note[4] to the medical record explaining that

---

[3] Strathmere Lodge may decide not to make a correction to a medical record if 1) the information represents a clinical opinion that was made in good faith 2) the medical record is not incomplete or inaccurate 3) the correction is frivolous, vexatious or requested in bad faith or 4) the information was created and received from another organization and Strathmere Lodge does not have enough information to know whether it should be corrected.

[4] Under PHIPA, this is called a "Statement of Disagreement" (SOD).

they disagree with the accuracy of the information. If SOD is provided staff will be made aware. If a document has a SOD, the SOD document will accompany the report when sharing with other HICs.

2.7 Retain a copy of the request form and any related correspondence for a 2-year period.

3. Correction Requests Related to PHI in ClinicalConnect/EHR System

3.1 All correction requests involving ClinicalConnect/EHR system must be directed to the Privacy Contact.

3.2 If the request relates to PHI that was solely contributed Strathmere Lodge to the ClinicalConnect/EHR system, the Privacy Contact must follow the operating practices above beginning with step No. 2.

3.3 If the request relates to PHI contributed to ClinicalConnect/EHR system by another HIC or multiple organizations, the Privacy Contact will redirect the requestor to the appropriate program office and provide contact information (refer to Appendix F. *eHealth Ontario Contact Matrix*).

III. Inquiries and Complaints

Key Points

Strathmere Lodge allows patients to ask questions or make a complaint about its PHI handling practices or its compliance with PHIPA. Inquiries may be verbal or in writing.

Strathmere Lodge responds to all inquiries or complaints within 30 calendar days or notifies the patient that additional time to respond to an inquiry or complaint is required.

Operating Practices

1. When a staff member receives a privacy-related question that is easy to answer, they should answer it.

1.1 If the staff member is unable to answer the question, tell the patient that they will give the question to the Privacy Contact and that the Privacy Contact will respond within 30 days.

1.2 Give the inquiry to the Privacy Contact.

2. If a staff member receives a privacy-related complaint:

   2.1 Tell the patient that they will forward the complaint to the Privacy Contact and that the Privacy Contact will respond within 30 days; and

   2.2 Give the complaint to the Privacy Contact.

3. When receiving the question or complaint, the Privacy Contact must:

   3.1 Contact the person as soon as possible and ask for clarification if the question or complaint is unclear.

   3.2 Ask the person to contact the appropriate organization if the question or complaint relates to another organization.

4. When responding to the question or complaint, the Privacy Contact must:

   4.1 Write a response to the question or complaint (*Inquiry or Complaint Response Template* can be found in Appendix G);

   4.2 Circulate the response to other staff members at Strathmere Lodge, if required;

   4.3 Respond to the question or complaint within 30 days or inform the person that an additional 30 days is needed; and,

   4.4 Retain a copy of the written response for a 2-year period.

5. If a question or complaint causes Strathmere Lodge to identify a privacy breach, the Privacy Contact initiates Strathmere Lodge's *Privacy Breach Management* protocol.

6. Inquiries or Complaints Related to ClinicalConnect/EHR System

   6.1 If a person has a question or complaint related to ClinicalConnect/EHR System, the Privacy Contact must:

   - Respond to the question following normal procedures (i.e., starting at step No. 1 of this operating practice) if the answer is known; or
   - Give the patient information within four (4) days on how to contact the appropriate program office (see Appendix F, *eHealth*

Ontario Contact Matrix) if it relates to the ClinicalConnect/EHR system or one or more other health service providers.

6.2 If Strathmere Lodge receives a question or complaint from a program office on behalf of a patient, the Privacy Contact must follow instructions from the program office on whether to:

- Respond to the person directly and follow the above procedures; or
- Give the program office the information needed to respond.

IV. Privacy Breach Management

Key Points

Strathmere Lodge must promptly respond to any real or suspected privacy breaches. All staff members at Strathmere Lodge must support the privacy breach response if required by the Privacy Contact.

Willful privacy breaches or repeated instances of accidental privacy breaches caused by a member of Strathmere Lodge will result in disciplinary action up to including dismissal and reporting to legal or regulatory authorities.

A privacy breach is:

- Any event where patient information is collected, used, or disclosed counter to PHIPA, Strathmere Lodge's policies, or obligations defined in agreements binding Strathmere Lodge.
- Any event where a patient's privacy rights under PHIPA, Strathmere Lodge's policies, or agreements binding Strathmere Lodge are violated whether or not it results from accidental or willful actions.

Operating Practices

1. Responding to a breach:

The person who identifies a suspected or real breach must:

1.1 Take immediate steps to prevent any further harm or risk; and,

1.2 Inform the Privacy Contact of the suspected or real breach within one hour of identifying the breach. The Privacy Contact must confirm whether the suspected breach is real.

1.3 The Privacy Contact must review the steps to ensure that no further harm or risk is anticipated.

1.4 The Privacy Contact has authority to take further action to minimize harm or risk up to and including:

- Removing the person's access to any paper or electronic copies of medical records, including ClinicalConnect/EHR System;
- Retrieving any copies of PHI that were inappropriately collected, used, or disclosed;
- Disconnecting systems from the network or Internet;
- Requiring support from other members of the clinic to effectively contain the privacy breach; and
- Taking any reasonable action to minimize harm or risk to patient(s).

1.5 Once contained, the Privacy Contact must lead a breach investigation which includes:

- Assembling members of Strathmere Lodge as required to understand who was responsible for the breach and how it occurred;
- Whether the breach was willful or accidental;
- Whether other steps could be taken to minimize harm or risk;
- The patient(s) that were impacted by the breach; and
- Recommendations to prevent breaches of similar nature in the future.

1.6 The Privacy Contact must document the breach and investigation using the *Privacy Breach Report Template* (Appendix H)

1.7 The designated manager must review the recommendations and determine which recommendations should be implemented.

1.8 The Privacy Contact must:

- Develop a plan to implement the approved recommendations and provide status updates to the designated manager as often as required; and,
- The Privacy Contact must log the breach and resulting investigation using *Privacy Breach Log* (see Appendix I. *Privacy Breach Log*).

2. Disciplinary Action

2.1 Where the privacy breach was willful or is accidental, the Privacy Contact must make recommendations to the designated manager.

2.2 Disciplinary action may include:

- Remedial training;
- Termination-upon termination, employee has agreed to adhere to the privacy responsibilities as per training.
- Restricted access to medical records;
- Probation;
- Reporting to IPC, the appropriate regulatory college, and/or law enforcement; and/or
- Other disciplinary action as appropriate.

3. Notification to the Impacted patient(s)

3.1 The Privacy Contact must notify impacted patient(s) of the privacy breach as soon as possible if their medical records have been collected, used, or disclosed counter to PHIPA, Strathmere Lodge's policies, or obligations defined in agreements binding Strathmere Lodge.

3.2 The Privacy Contact must notify patient(s) of the privacy breach in a way that is sensitive to the needs of the patient. Potential mechanisms to notify the patient are:

- Writing a letter;
- Telephoning;
- Putting a note in the medical record to speak with the patient on his or her next visit; or
- Public notices if the identity of the impacted patient(s) is not known.

3.3 The Privacy Contact determines the most appropriate way to notify patient(s), but the notice must generally include:

- The name of the person or people who caused the privacy breach if it was a willful act or relevant to the privacy breach;
- The date and time of the privacy breach;
- A description of the nature and scope of the privacy breach;
- A description of the PHI and scope of PHI that was breached;
- What was done to contain the breach;
- Summary of the investigation;
- Steps that the impacted patient(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable
- Contact information for the Privacy Contact; and
- Information about making a complaint to the IPC.

3.4 The Privacy Contact must save a copy of the notice provided to the impacted patients or log that the notice was given using *Privacy Breach Log* (see Appendix I).

4. Breaches Related to PHI in ClinicalConnect/EHR System

a. If the privacy breach relates to PHI from ClinicalConnect/EHR System, the Privacy Contact must notify the responsible program office by the end of the next business day after identifying or

becoming aware of the privacy breach (see Appendix F. *eHealth Ontario Contact Matrix*).

b. If the privacy breach is related to PHI in ClinicalConnect/EHR System, Strathmere Lodge must follow instructions from the program office on managing the privacy breach, understanding that remediation or disciplinary activities must be approved by the applicable oversight body at the program office responsible for ClinicalConnect/EHR System.

V. Consent Management

Key Points

Strathmere Lodge must not collect, use, or disclose PHI for healthcare purposes if the patient or SDM wants it blocked (i.e., consent directives). Written requests for consent directives are preferred.

Strathmere Lodge must try to create a block that most closely matches the patient's wishes. As an example, these may include:

- Block all or some of the medical record from being accessed by anyone or disclosed to another healthcare provider for healthcare purposes;
- Block all or some of the medical record from being accessed by particular people in Strathmere Lodge or from being disclosed to named healthcare providers; or
- Allow all or some members to access an otherwise blocked medical record.

When a staff member accesses PHI that is blocked, Strathmere Lodge must confirm that it was appropriate and tell the patient that blocked information was accessed.

Operating Practices

1. Getting Consent

1.1 Strathmere Lodge provides health care under an implied consent model and obtains knowledgeable consent of patients for the collection, use, or disclosure of PHI, as required by law. PHI can be

collected, used, or disclosed without the knowledge and consent of patients only where it is permitted or required by law.

1.2 If a patient asks a staff member to create or remove a block on their medical record, the staff member must:

- Tell the patient that they will give the request to the Privacy Contact and that the Privacy Contact will contact them; and
- Give the request to the Privacy Contact as soon as possible.
- Patient will be notified of the following:
  - The consent directive only applies to PHI the patient has already provided.
  - Health Care providers may override the directive.
  - Quality of Care may be impacted.

1.3 Before creating or removing the block in the patient's medical record, the Privacy Contact must:

- Document the request using Strathmere Lodge *Lockbox Request Form* (Appendix J), or ask the requestor to complete the form.
- Write in *Consent Directives Log (*see Appendix I) that the request was made;
- Verify the identity of the patient by asking for photo identification.
- Confirm that the person is indeed the SDM for the patient, if applicable, by following the guidelines for *Confirming Authority to Act as SDM (*see Appendix B)
- Discuss with the patient the messages found in Appendix K- *Sample Messaging to Use When Creating/Modifying or Removing a Consent Directive*
- Help the patient choose a block that most meets their needs.

1.4 When creating the block, the Privacy Contact must:

- Identify any location or system where the patient's medical record exists; and
- Create a block on the medical record that most closely reflects the patient's wishes or write a note on the outside of the file folder if it is a paper copy or on the demographic screen if it is an electronic record that does not support consent directives.

1.5 After creating or removing the block, the Privacy Contact must:

- Confirm with the patient that the block was created or removed;
- Discuss with the patient the messages found in *Template of Messages to Discuss with patient when Creating or Removing a Block* if this did not already happen;
- Record that the notice was made in the *Consent Directives Log* (see Appendix I).

1.6 If consent directive is requested, staff will be notified via processes implemented in EMR.

2. Requests for Blocking/Lock-boxing PHI in ClinicalConnect/EHR System

2.1 If a patient/SDM wants to create, remove or modify a block in the ClinicalConnect/EHR system, the Privacy Contact will direct the individual to the appropriate program office (see Appendix F. *eHealth Ontario Contact Matrix*) and provide their contact information.

3. Overriding Blocks/Consent Directives in ClinicalConnect/EHR System (PSSA 14) (PSSA 15)

3.1 With a few exceptions[5], a staff member may only access PHI that a patient has blocked in ClinicalConnect/ EHR system under the following circumstances:

[5] Note that consent directive overrides to eliminate risk of harm are not permitted for OLIS and the DHDR.

- Obtains the express consent of the patient to whom the PHI relates;
- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the patient to whom the PHI relates, and it is not reasonable possible to obtain the consent of the individual in a timely manner; or
- Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons.

3.2 When a staff member overrides a patient's block, the Privacy Contact will:

- Follow-up with the staff member that overrode the block to make sure it was appropriate and also determine whether the staff member printed a copy of the locked-out PHI.
- If there is a printed copy of PHI that was accessed thru an override, the Privacy Contact will either 1) locate and shred the printout or 2) clearly mark the date and purpose on the print out (noting it void).
- If the override was appropriate, the Privacy Officer will notify the patient in writing and retain a copy of the written notice for a 2-year period.[6] (Appendix L - *Sample Notification of Consent Override*)
- If the override was for the purpose of eliminating the risk of significant harm to the patient or other individual, the Privacy Contact must notify the IPC in writing and retain a copy of that notice for a 2-year period. A *Notification of Consent Override to IPC* can be found in Appendix M)

[6] MOHLTC notifies individuals if a consent directive in OLIS or DHDR is overridden.

- If the override is determined to be inappropriate, the Privacy Contact must follow Middlesex County *Privacy Breach Management* protocol.

VI. Privacy and Security Training

Key Points

Strathmere Lodge must train all staff members on their privacy and security obligations before giving them access to PHI. Strathmere Lodge retrains their staff on an annual basis.

Operating Practices

1. Training Staff Members of Their Obligations

1.1 Whoever hires a new staff member must tell the Privacy Contact that a new person has been hired.

1.2 Before giving the person access to PHI and every year after, the Privacy Contact must:

- Train the new staff member regarding their privacy and security obligations or require them to review an eLearning / video module;
- Write in the *Training Log* (Appendix I) that the staff member was trained.
- Have the new staff member sign the Strathmere Lodge *Confidentiality Agreement* (see Appendix N) that:
    - They understand their privacy and security obligations;
    - Their privacy responsibilities continue to apply even after employment with Strathmere Lodge terminates; and,
    - They are aware that not meeting their privacy and security obligations could lead to disciplinary action including dismissal and reporting to legal authorities or professional bodies.

1.3 The Privacy Contact will think of other ways in addition to training to foster and promote a culture of privacy.

1.4 Strathmere Lodge must remove the staff member's access to medical records if they fail to complete the training.

2. Before Accessing New Systems or Information

If a staff member needs access to new information system, the Privacy Contact or their delegate must:

- Determine whether the new system or information repository requires new or different privacy and security messages than was provided during training;
- Train the staff members on the additional privacy and security messages; and
- Write in the *Training Log* (see Appendix I) that the staff member received additional training.

3. Contents of Training Materials

The Privacy Contact must create training materials relevant to the staff member's role. The Privacy Contact will determine how the mandatory privacy and security training required for ClinicalConnect/EHR system is implemented at Strathmere Lodge.

4. Non-Strathmere Lodge Observers

The Privacy Contact needs to approve any individuals from other organizations that wish to attend at Strathmere Lodge to gain knowledge about the health care system and will also decide if that individual is required to sign a *Confidentiality Agreement for Non-Clinical Observers* (Appendix O).

VII. Retention

Key Points

Strathmere Lodge will ensure records containing PHI are protected and disposed of in accordance with Strathmere Lodge Information Security Policies and Procedures.

Operating Practices

1. Strathmere Lodge retains records containing PHI for specified periods of time:
    1.1. Any information collected to respond to access and correction requests, inquiries, complaints, and information pertaining to consent directives must be retained for two years after the request was made.
    1.2. Any information created about a patient's part of an investigation of Privacy Breaches and/or Security Incidents must be retained for two years after the privacy breach/security incident has been closed.
    1.3. Audit and monitoring reports that contain PHI created and maintained for compliance purposes should be retained for the longer of thirty years or when PHI is removed from the EHR.
    1.4. Information used for identity provider registration that contains personal information should be retained for seven years after last use.
    1.5. System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI should be retained for a minimum of two years.
    1.6. Assurance-related documents should be retained for ten years.
    1.7. Where Strathmere Lodge is an Identity Provider:
        - Authentication events for sixty days online or twenty-four months total in archive; and
        - End user credential information permanently.
        - The Privacy Contact at Strathmere Lodge will ensure records are protected and disposed of in accordance with the Strathmere Lodge Information Security Policy.

1.8. Strathmere Lodge will log all instances of record destruction and will retain indefinitely. The “Disposing of Your Electronic Media” document issued by the IPC in March 2018 has been adopted. See appendix.

VIII. Logging and Auditing (ClinicalConnect)

Key Points

The Privacy Contact at Strathmere Lodge must follow the guidance provided by the relevant program office (i.e., ClinicalConnect and eHealth Ontario) for auditing Strathmere Lodge staff members’ access to ClinicalConnect/EHR system.

Operating Practices

Audit reports conducted for compliance purposes will be retained in accordance with Strathmere Lodge Retention Procedures.

If a suspect access is identified as a result of any auditing activities, the Privacy Contact will follow the Strathmere Lodge Privacy Breach Management procedures.

The Privacy Contact must ensure that all other assurance-related activities required for Strathmere Lodge participation in ClinicalConnect/EHR System are satisfied.

IX. Disclosure of PHI

1. Any request for the disclosure of PHI will be directed to and processed by the Privacy Contact.
2. The Privacy Contact decides whether to charge or waive a fee to cover the cost of responding to the request and will ensure the fee is consistent with the rules under PHIPA.
3. In response to a subpoena, summons, warrant, the Privacy Contact must review on a case-by-case basis the scope of each legal document to determine what exact records of PHI must be disclosed. The Privacy Contact will also consult with legal counsel or IPC if needed.

4. Shared records of PHI in which part of the record has a consent directive will not have that part of the record shared and the recipient of the record will be notified.

Clinical Connect Policy 1.01

Appendix A – Request for Access Form

Request for Access

Instructions to person making the request:

- Complete this form with as much information as possible.
- We only accept requests from the patient/client or someone that the patient/client has asked to make the request (i.e., substitute decision maker).
- You will need to provide photo identification, and prove that the patient/client has allowed you to make the request.
- Ontario law (PHIPA) allows a healthcare provider to charge administrative fees to a person who wants a copy of his or her medical records. We may ask you to pay a fee before giving you a copy of your record.

1. Patient/Client Information

First Name: *	Last Name: *
Enter Text.	Enter text.

Contact Information if it is different than the information we have on file: *

Enter Text

2. Person Making the Request (ONLY COMPLETE IF YOU ARE NOT THE Patient/Client)

First Name: *	Last Name: *
Enter text.	Enter text.

Relationship to the Patient/Client:

Enter text.

Contact Information:

Enter text.

3. Information being Requested

Which of the following information do you need (please check all that apply)?

☐ All health information from the last:

☐ 3 months	☐ 3 years
☐ 6 months	☐ 5 years
☐ 12 months	☐ All

☐ Some health information (describe what information you would like):

☐ List of people that have viewed your medical record

- ☐ All of them, or
- ☐ Some of them:

A certain person: _____

People who viewed my medical record in the past:

☐ 3 months	☐ 3 years
☐ 6 months	☐ 5 years
☐ 12 months	☐ All

☐ List of consent instructions that you have provided and changes you made to them

Clinical Connect Policy 1.01

☐ List of times when someone has overridden your consent instructions

☐ All of them, or

☐ Some of them:

Done by a certain person (provide name and where s/he works): _____
Only overrides in the past:

☐ 3 months ☐ 3 years

☐ 6 months ☐ 5 years

☐ 12 months ☐ All

4. Permission to Leave Voice Mail

If we need to confirm information or contact you, we will call you. May we leave a message if you do not answer the phone?

☐ Yes, you may leave a detailed message

☐ No, you may not leave a detailed message

Provide any instructions about leaving a message (e.g., only on electronic voicemail, not with a person if the phone is answered).

5. Signature

Name: _____ *(printed)*

Signature: _____

Date: _____

For Internal Use Only. Do Not Complete.

6. Identify Confirmed

7. Notes

Clinical Connect Policy 1.01

Appendix B – Identify Verification Standards

The Privacy Contact will rely on the following documentation of proof of identity. Individuals must present one of the following:

- Copy of ID issued by a federal, provincial/territorial/state or municipal authority and which bears a photo and signature of the Individual; or
- Copy of a student card bearing a photo and signature of the person, where the person is between 12 and 18 years of age, inclusively.
- Reliance on the parent or legal guardian's assertion of identity where the person is less than 12 years of age and where the parent or legal guardian's identity has been verified; or
- An assertion from eHealth Ontario or another organization trusted by Strathmere Lodge of the person's identity.

The documents may be presented in-person, through mail, or by fax. Photocopies are acceptable.

Confirming Authority to Act as Substitute Decision Maker (SDM)

Note that a privacy contact may rely on a patient providing verbal confirmation that a person is their SDM.

The privacy contact will rely on the following documentation of proof that the Individual making the request is the SDM for the patient. The documents may be presented in-person, through mail, or by fax. Photocopies are acceptable.

Patient is under 12 years of age	• A birth certificate for the patient, signatures from both parents who appear on the birth certificate, and a photocopy of ID issued by a federal, provincial/territorial/state or municipal authority which bears a photo and signature of both parents; • A legal document demonstrating that the Individual has sole custody or guardianship for the patient; or • An assertion from eHealth Ontario or another organization trusted by Strathmere Lodge of the person's identity.
Patient is between 12 and 18 years of age, inclusively	• A signed letter from the patient and photocopy of ID issued by a federal, provincial/territorial/state or municipal authority or student card which bears signature of the patient; • A legal document demonstrating guardianship or Power of Attorney; or • An assertion from eHealth Ontario or another organization trusted by Strathmere Lodge of the person's identity.
Patient is above 18	• A signed letter from the patient and a photocopy of ID issued by a federal, provincial/territorial/state or municipal authority which bears a photo and signature of the patient. • A legal document demonstrating guardianship or Power of Attorney; or • An assertion from eHealth Ontario or another organization trusted by Strathmere Lodge of the person's identity.
Patient is deceased	• A letter signed by the patient prior to his or her death and a photocopy of ID issued by a federal, provincial/territorial/state or municipal authority which bears a photo and signature of the patient • A legal document demonstrating right to have access to the patient's information; or • An assertion from eHealth Ontario or another organization trusted by Strathmere Lodge of the person's identity.

Clinical Connect Policy 1.01

Appendix C – Request for Access Response Template

Instructions

1. Use the appropriate letter template below for communicating with the patient/client about the results of the request to obtain a copy of his or her medical record.
2. Complete the letter template and send it to the patient/client within 30 days of receiving the request.
3. Save a copy of the completed letter or log the response in *Request for Access Log*.
4. The completed letter may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Use this template if you are releasing the entire medical record

Dear <<patient/client>>,

This is a copy of your medical record. You asked for this information on <<date of request>>.

If you want to discuss this or have questions about what the information in your medical record means, please contact me at <<phone number for privacy contact>>.

Sincerely,

<<Name, Title>>

Use this template if you are not releasing all of the medical record

Dear <<patient/client>>,

You asked for a copy of your medical record from our files.

We have decided not to give you a copy of <<any of/part of>> your medical record. This is allowed by Ontario law (Personal Health Information Protection Act, s52 (1) <<insert the number of the relevant clause in s52 (1)>>). We made this decision because <<provide reason that the access request is being denied as long as it does not expose the PHI being withheld>>.

<<If the request is being denied in part, briefly describe the nature of the medical records being withheld (e.g., mental medical records, medical records from a particular encounter, all medical records) if it does not expose the PHI being withheld, and whether some medical records are still being released.>>

If you want to discuss this or need more information, please contact me at <<phone number for privacy contact>>.

You also have a right under Ontario's laws to register a complaint about not getting access to your information. Contact the Information and Privacy Commissioner of Ontario to make a complaint:

Information and Privacy Commissioner of Ontario 2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8

Sincerely,

<<Name, Title>>

Clinical Connect Policy 1.01

Use this template if you need more than 30 days to provide the person with the medical record

Dear <<name of individual>>,

We have received your request for a copy of your medical record. We will be able to provide you with the information however the retrieval of your information will take 30 days due to the following reason:

<<provide reason for the extension; note that the reason must be aligned with PHIPA, s54 (3) where it is a Request for Access or s55 (3) where it is a Request for Correction>>.

If you have any concerns or questions about why we need more time, please contact <<name of privacy contact>> at:

<<name of privacy contact>>
<<organization name>>
<<HIC Address>>
<<HIC Phone>>

Sincerely,

<<Name, Title>>

Clinical Connect Policy 1.01

Appendix D – Request for Correction Form

Request for Correction	
Instructions to person making the request: • Complete this form with as much information as possible. • We only accept requests from the patient/client or someone that the patient/client has asked to make the request (i.e., substitute decision maker). • If we don't know you or are unsure whether the patient/client has asked you to make the request, you will need to provide photo identification, and prove that the patient/client has allowed you to make the request.	
1. Patient/Client Information	
First Name: * Enter Text.	Last Name: * Enter Text.
Contact Information if it is different than the information we have on file: * Enter Text.	
2. Person Making the Request (ONLY COMPLETE IF YOU ARE NOT THE Patient/Client)	
First Name: * Enter Text.	Last Name: * Enter text.
Relationship to the Patient/Client: Enter text.	
Contact Information: Enter text.	
3. Nature of the Change	
Describe the information that you feel is not correct or out-of-date, and the suggested correction. Provide as much detail as possible. Enter text.	
4. Permission to Leave Voice Mail	
If we need to confirm information or contact you, we will call the phone number that you provided above. May we leave a message if you do not answer the phone? ☐ Yes, you may leave a detailed message ☐ No, you may not leave a detailed message Provide any instructions about leaving a message (e.g., only on electronic voicemail, not with a person if the phone is answered). Enter text.	

Clinical Connect Policy 1.01

5. Signature
Name: _____ *(printed)* Signature: _____ Date: _____
For Office Use Only. Do not Complete.
6. Identify Confirmed
Do not include identifiers in this section.
7. Notes

Clinical Connect Policy 1.01

Appendix E – Request for Correction Response Template

Instructions

1. Use the appropriate letter template below for communicating with the patient/client about the results of a Request for Correction.
2. Complete the letter template and send it to the patient/client within 30 days of receiving the request.
3. Save a copy of the completed letter or log the response in Request for Correction Log.
4. The completed letter contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Use this template if you have made the correction

Dear <<patient/client>>,

You asked that the following information about you be changed:

- <<describe PHI that was inaccurate>> We made the following change:
- <<describe the change that was made>>

If you want to discuss this change, please contact me at <<phone number for privacy officer>>.

Sincerely,

<<Name, Title>>

Use this template if you are not making the correction

Dear <<patient/client>>,

You asked that the following information about you be changed:

- <<describe PHI that was inaccurate>>

We decided not to make the changes because <<explain reason for not making the change which must be aligned with PHIPA, s55 (9).>>

If you want to discuss this or want to attach a note to your medical record saying that you do not agree with the information, please contact me at <<phone number for privacy contact>>.

You also have a right under Ontario's laws to register a complaint about our decision. To register your complaint, contact the Information and Privacy Commissioner of Ontario at:

Information and Privacy Commissioner of Ontario 2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8

Sincerely,

<<Name, Title>>

Clinical Connect Policy 1.01

Use this template if you need more than 30 days to make the correction

Dear <<name of individual>>,

You asked us to make a change to your medical record.

We require an additional 30 days to investigate the change.

The additional time is required because <<provide reason for the extension; note that the reason must be aligned with PHIPA, s55 (3)>>.

If you have any concerns about the extra time, please contact <<name of privacy contact>> at:

<<name of privacy contact>>
<<organization name>>
<<HIC Address>>
<<HIC Phone>>

Sincerely,
<<Name, Title>>

Clinical Connect Policy 1.01

Appendix F – eHealth Ontario Contact Matrix

This contact matrix may be used by the Privacy Contact, Agent or delegate in responding to **patient requests** concerning Ontario's Electronic Health Record.

Do not include personal information or personal health information in email.

System	Description of Personal Health Information	Privacy Inquiries or Complaints	Access Request (copy of record for another HIC, multiple HICs or Report of Access to PHI)	Consent Directive and Consent History Report (including consent options available)	
Connecting Ontario	Clinical reports: discharge summaries, emergency department and visits and encounters	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416-586-4397 privacy@ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416- 586-4397 privacy@ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416- 586-4397 privacy@ehealthontario.on.ca	1. All personal health information 2. All personal health information created and contributed by a particular organization or practice 3. All users from a particular organization or practice. 4. A particular user.
ClinicalConnect	Clinical reports in South Western Ontario	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5 Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5 Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5 Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	1. All personal health information 2. All personal health information in a particular repository or system. 3. All personal health information created and contributed by a particular organization or practice. 4. A particular record of personal health information.

Clinical Connect Policy 1.01

System	Description of Personal Health Information	Privacy Inquiries or Complaints	Access Request (copy of record for another HIC, multiple HICs or Report of Access to PHI)	Consent Directive and Consent History Report (including consent options available)	
Diagnostic Imaging Common Services (DI CS)	Diagnostic imaging reports and images (ultrasounds, MRIs, x-rays)	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416- 586-4397 privacy@ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416- 586-4397 privacy@ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 1-866-250-1554 F: 1-866-831-0107 or 416- 586-4397 privacy@ehealthontario.on.ca	1. All personal health information in a particular repository or system. 2. A particular record of personal health information. 3. All users from a particular organization or practice
Ontario Laboratories Information System (OLIS)	Laboratory test orders and results (urine, blood, microbiology)	Service Ontario 1-800-291-1405 TTY: 1-800-387-5559	Freedom of Information and Privacy Coordinator Access and Privacy Office, Ministry of Health and Long-Term Care 99 Adesso Drive, 1st floor, Concord, ON L4K 3C7 416-327-7040 generalapo@ontario.ca	Service Ontario 1-800-291-1405 TTY: 1-800-387-5559	All personal health information in a particular repository or system.
Drug and Pharmacy Services	Dispensed drug history	Service Ontario 1-800-291-1405 TTY: 1-800-387-5559	Service Ontario 1-800-291-1405 TTY: 1-800-387-5559	Service Ontario 1-800-291-1405 TTY: 1-800-387-5559	All personal health information in a particular repository or system.

Information and Privacy Commissioner of Ontario

Privacy-related complaint
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8

Clinical Connect Policy 1.01

Telephone: 416-326-3333 • 1-800-387-0073
Fax: 416-325-9195, TTY: 416-325-7539

This contact matrix may be used by the Privacy Contact or delegate for **privacy-related matters** concerning Ontario's Electronic Health Record.

Do not include unencrypted personal information or personal health information in email.

System	Consent Directive Request (on behalf of Patient)	Requesting a Privacy Audit Report	Notify other Health Information Custodians of a Correction Request	Reporting any real or suspected Privacy Breaches	Submitting a Privacy Breach Report Summary
Connecting Ontario	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416-586- 4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario's Service Desk (ESD) 1-866-250-1554 servicedesk@ ehealthontario.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca
ClinicalConnect	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5 Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5 Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5	ClinicalConnect Privacy Office Hamilton Health Sciences 1200 Main Street West Hamilton, ON L8N 3Z5

System	Consent Directive Request (on behalf of Patient)	Requesting a Privacy Audit Report	Notify other Health Information Custodians of a Correction Request	Reporting any real or suspected Privacy Breaches	Submitting a Privacy Breach Report Summary
	Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca			Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca	Tel: 905-521-2100 ext. 75122 privacy@clinicalconnect.ca
Diagnostic Imaging Common Services (DI CS)	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416-586- 4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca	eHealth Ontario's Service Desk 1-866-250-1554 servicedesk@ ehealthontario.ca	eHealth Ontario Privacy Office P.O. Box 148, Toronto Ontario M5G 2C8 T: 1-888-411-7742 ext. 64767 or 1- 416-946-4767, 1-866-250-1554(ESD) F: 1-866-831-0107 or 416- 586-4397 privacy.operations@ ehealthontario.on.ca
Ontario Laboratories Information System (OLIS)	N/A	eHealth Ontario's Service Desk (ESD) 1-866-250-1554 servicedesk@ehealthontario.ca	N/A	eHealth Ontario's Service Desk 1-866-250-1554 servicedesk@ ehealthontario.ca	N/A
Drug and Pharmacy Services	N/A	eHealth Ontario's Service Desk (ESD) 1-866-250-1554 servicedesk@ehealthontario.ca	N/A	eHealth Ontario's Service Desk 1-866-250-1554 servicedesk@ ehealthontario.ca	N/A

Clinical Connect Policy 1.01

Appendix G – Inquiry or Complaint Response Template

Instructions

1. Use this letter template to respond to a person making an Inquiry or Complaint.
2. The completed letter may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Template:

Dear <<name of individual>>,

We received a (Question/Complaint) from you on <<date of receipt>>. <<Provide response here>>

If you have any other questions or concerns, please contact:

• <<name of privacy contact>>

Ontario
eHealth Ontario

• <<contact information for privacy officer >>

(*Instruction: only include the following if it was a complaint*) You can also contact Ontario's Information and Privacy Commissioner with privacy complaints. If you want to register a complaint, please contact:

Sincerely,
<<Name, title of privacy officer>>

Clinical Connect Policy 1.01

Appendix H – Privacy Breach Report Template

Privacy Breach Report	
Date report last updated: Version number of report: Is this the final version of the report?	
1. Privacy Breach Information (Reporter to complete as much as known)	
Time and date Privacy Breach occurred (if known)**:**	
Time and date Privacy Breach identified:	
Breach Severity (Critical, Severe, Moderate, Minor, Near Miss):	
Person responsible for the Privacy Breach (if relevant and known):	
Does the breach involve a shared system? If so, please identify which one(s).	
Breach Type ☐ Collection ☐ Use ☐ Disclosure ☐ Retention ☐ Destruction ☐ Mishandling ☐ Other, explain:	Was the Breach? * ☐ Unintentional ☐ Intentional
Description of the nature and scope of the Privacy Breach * *Include information such as:* • *What activity or activities occurred? When did they occur?* • *Who was involved?* • *Why is it a Breach?* • *What is supposed to happen? What are the standard operating procedures?* • *How many <<patients/clients>> were affected?*	
What PHI was involved in the Breach? * ☐ Demographic Information ☐ Medical ☐ Other Description of the PHI involved in the Breach:	

Clinical Connect Policy 1.01

2. Privacy Breach Containment

Person responsible for containment *

Description of any containment measures taken *

3. Privacy Breach Escalation

Identify which if any of the following has been notified about the Privacy Breach *

Group *Date of Notification*

- ☐ Program Office (if shared system)
- ☐ Clinic Leadership
- ☐ IPC / Ontario
- ☐ Law enforcement
- ☐ Regulatory College
- ☐ Other, explain

4. Notification to Impacted Individuals

Were the impacted individuals notified? If not, why? *

Describe the manner of the notice *

Include information such as:

- *Who was responsible for the notice?*
- *When was notice provided?*
- *How was notice provided?*

5. Investigation

Breach Investigator (Name) *

Description of investigation activities *

Include information such as:

- *Scope and nature of the investigation*
- *Steps that were followed*

Root cause of the Privacy Breach *

6. Remediation Plan

Identify the remediation activities that have been completed or are recommended to be completed.

Activity	Owner	Status of Completion	Expected Date of Completion

Clinical Connect Policy 1.01

Appendix I – Privacy Logs Workbook

The Privacy Contact is responsible for ensuring the following logs are created and maintained by Strathmere Lodge Staff:

- Training Log
- Privacy Breach Log
- Consent Directives Log

Clinical Connect Policy 1.01

Appendix J – Consent Management / Lockbox Request Form

A correction request or lockbox has been placed by <insert name of patient/client/SDM here> on the use and/or disclosure of the personal health information of <insert name of patient here>.

Lockbox restrictions apply to:

- Entire record
- Portion of the record

Lockboxed information may be released with the consent of the patient or SDM. If the patient or SDM refuses or the patient is incapable and the SDM is not available, lockboxed information may be released only:

- To eliminate or reduce a significant risk or serious bodily harm to a patient or to another person or other group of persons, or
- If the use or disclosure of the information is permitted or required by law, e.g.
  - For the purpose of examining, assessing, observing or detaining the client under the Mental Health Act
  - To respond to the receipt of a Court Order, Search Warrant, or other legally binding Order mandating the release of information, and/or
  - Other uses or disclosures that are permitted or required by law – contact Privacy Office for information on these uses.

The following health care providers have been notified of restrictions placed on this record:

Name _____

Date notified _____ By: _____

Name _____

Date notified _____ By: _____

Name _____

Date notified _____ By: _____

Clinical Connect Policy 1.01

Appendix K – Sample Messaging to Use When Creating/Modifying or Removing a Consent Directive

1. Use These Messages when Creating a Block

When creating a block, talk to or write to the patient/client about:

- The type of block that will be or was placed on the individual's file and how it will meet the patient/client's request;
- The impact of a block on the patient/client's care to be discussed with requestor:
    - The consent directive only applies to PHI patient has already provided, and not to PHI that may be provided in the future.
    - Despite the consent directive, health care providers may override in certain circumstances such as emergencies.
    - The consent directive may result in delays in receiving health care, reduced quality of care due to a health care provider's lacking complete information about the patient, and a health care provider's refusal to offer non-emergency care.
- When a consent directive can be overridden (3 purposes);
- That the patient/client will be notified if the block is overridden;
- That the patient/client can change his or her mind at any time, or create other blocks; and
- How to contact Privacy Contact with any other questions or requests.

2. Use These Messages when Removing or Modifying a Block

When removing a block, talk to or write to the patient/client about:

- Confirming that the block was removed or modified as requested;
- The type of block that was removed or modified and what information will now be made available;
- That the patient/client can change his or her mind at any time, or create other blocks; and
- How to contact Privacy Contact with any other questions or requests.

3. Template of Messages to Discuss with patient/client when an Override Occurs

Instructions

1. Use the template below when discussing overrides with patients/clients.
2. Write in the Consent Directives Override Log when you have had this discussion with the patient/client or, if you are creating a letter based on this template, save a copy of the letter.

Document Storage and Handling Instructions

1. This template is stored in Privacy Contact's office.
2. The completed form if relevant should be stored in Privacy Contact's office.
3. Keep the completed form for 2 years

Clinical Connect Policy 1.01

Appendix L - Notification of Consent Override

Remove title and watermark before sending the letter.

STRATHMERE LODGE
1035 Adelaide St. S
London, ON N6E 1R4

<<MONTH DD, YYYY>>

Attn. :<< Individual's Name >>
<<Street Address>>
<<City, Postal Code>>

Re: Notification of Consent Override in ConnectingOntario

To <<Individual's Name>>:

You have restricted access to your patient records within the ConnectingOntario Electronic Health Record by applying a consent directive.

This letter is to inform you that a consent directive override was performed by a health care provider at<<Organization Name>> for the purpose identified below. The temporary override has since expired and your consent directive has been re-activated.

Date of Override	<<MM, DD, YYYY>>
Time of Override	<<00:00 AM/PM>>
Purpose of Override	<<Select one of: a) Express consent of patient or substitute decision maker; b) To eliminate or reduce a significant risk of bodily harm to the patient; c) To eliminate or reduce a significant risk of bodily harm to persons other than the patient>>
Type of Personal Health Information	<<type of record in ConnectingOntario that was subject to a consent directive>>
Name of individual who performed the override	<<Agent Name >>
Organization Name	Organization Name
Disclosing Organization	<<HIC that contributed the PHI to ConnectingOntario>>

If you believe the consent override was performed for a reason other than this purpose, or should you have any questions about this consent override, please contact <<Organization Name, PHONE NUMBER>>.

If you have any questions about the ConnectingOntario Electronic Health Record, please contact eHealth Ontario at 416-946-4767.

You have a right to make a complaint about <<Organization Name's>> or eHealth Ontario's information practices by contacting:

Information and Privacy Commissioner of Ontario at:

Telephone: (416) 326-3333 or (905) 326-3333
Toll free: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539

Sincerely,

<<Name of Privacy Officer/Lead>>
<<Role, Organization Name>>

Clinical Connect Policy 1.01

Appendix M - Notification of Consent Override to IPC

Remove title and watermark before sending the letter.

<<MONTH DD, YYYY>>

Information and Privacy Commissioner of Ontario
Attn: Commissioner
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Re: Consent Override Notice Pursuant to the *EHR Consent Management Policy*

This letter is to provide you with a notification of a consent override performed by a clinician at <<Organization Name>> for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the personal health information (PHI) relates or to a group of persons.

In accordance with the *Electronic Health Record Consent Management Policy*, please find the relevant consent override information below:

Date and Time of Consent Override	<<DD,MM,YYYY at 00:00 AM/PM>>
HIC that collected PHI	<<HIC Name>>
Agent of HIC that collected PHI	<<Agent Name>>
Disclosing HIC	<<Name of HIC that contributed the PHI>>
Type of PHI	<<type of record in ConnectingOntario>>

Should you have any questions, please contact our privacy office at <<organization contact number>>.

Sincerely,

<<Name>>

<<Role>>

<<Contact Information>>