Strathmere Lodge

Strathmere Lodge Caring for seniors in Middlesex	Manual	{{ manual }}
	Policy Number	{{ policy_id }}
	Original Date	{{ original_date }}
	Revised/Reviewed Date	{{ reviewer_date }}
	Issued By	{{ reviewer_name }}
	Approved By	{{ approver_name }}

Strathmere Lodge is committed to a high standard of security 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.

Table of Contents **Pages**

1. Purpose

The *Personal Health Information Protection Act, 2004* (PHIPA), which governs the collection, use and disclosure of personal health information (PHI) in Ontario, requires that health information custodians (HICs) take adequate steps to safeguard PHI they collect, use or disclose. The purpose of this policy is to define behavioral controls intended to protect the confidentiality, integrity, and availability of PHI, while limiting the risks of compromised applications/systems, devices, or networks, and legal/regulatory issues to Strathmere Lodge.

This policy is mandatory and by accessing any PHI or any applications/systems, devices, or networks in the custody of, owned, or leased by Strathmere Lodge, users are agreeing to abide by the terms of this policy.

This policy is required to be read in conjunction with the Strathmere Lodge Policy manual and any other applicable policies, procedures or standard operating procedures.

2. Audience

This policy applies to all agents and electronic service providers associated with/acting on behalf of Strathmere Lodge utilizing Clinical Connect.

3. Scope

This document applies to all uses of Clinical Connect associated with:

- PHI in the custody of Strathmere Lodge.
- Applications/systems (e.g., Electronic Medical Records (EMR)) or devices owned or leased by Strathmere Lodge.
- Personal devices used to conduct business on behalf of Strathmere Lodge.
- Networks (Wi-Fi, LAN, WAN, etc.) owned or leased by Strathmere Lodge.

4. Definitions

Agent: Anyone who performs services on behalf of a health information custodian, whether they are paid or unpaid. For the purposes of this policy, it includes all employees (full-time, part-time, permanent and temporary), volunteers, contractors, and consultants.

Device: Includes all workstation computers/desktops, laptops, tablets, pagers, mobile phones, printers, fax machines, and scanners/photocopiers.

Credentials: An object that is verified during an authentication transaction to ensure that the bearer is in fact who they claim to be. For the purposes of this policy, it refers to any username and password used to access a device, applications/system, or network.

Electronic Service Provider: A person that provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

Health Information Custodian (HIC): Any person or organization who is responsible for collecting, using and disclosing personal health information for a patient. HICs include health care practitioners (e.g., facility or private practice), hospitals, psychiatric facilities, pharmacies, laboratories, nursing homes and long-term care facilities, homes for the aged and homes for special care, community care access corporations, ambulance services, boards of health, the Minister of Health and Long-Term Care, and the Canadian Blood Services, and in this policy, specifically refers to Strathmere Lodge.

Information Technology: Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Mobile Computing Device: Any reasonably portable electronic device used for purposes capable of storing or transmitting data, including the following: smart phones (including Blackberry's and iPhone's), Laptops (including Net books), Personal digital assistants, USB memory sticks, Portable hard disk or solid state data storage devices, Numeric, alpha-numeric and 2 way pagers, Medical or other electronic devices that contain hard disk or solid state data memory and which can be plugged into a USB port, CD / DVD disks or CD/DVD 'burners'.

Personal Health Information: Any data that a HIC collects, uses, or discloses that can be used to identify a client or patient. This includes demographic information, provider name, payment information, substitute decision maker information, OHIP information, visit number, medical history, test and lab results, etc.

The EHR Solution and supporting systems (e.g. the EHR Solution, OLIS and the Acute Care CDR) store and make available specified electronic PHI from the electronic health information systems of HICs that may not be available in planned provincial or regional repositories so as to act as a single repository of such information to reduce the load on source systems. This does not include any participating HIC's information systems or information technologies.

5. Principles

5.1 Awareness and Training - An information security-positive culture will be fostered, which may be achieved by implementing awareness and training to help all agents and electronic service providers with access to PHI to understand their information security-related obligations.

5.2 Access Control – Appropriate logical access controls must be implemented to manage access to PHI. These controls must ensure that only:

5.2.1 Authorized agents and Electronic Service Providers are granted access to PHI and that personal accountability is assured.

5.2.2 Authorized devices are granted access to applications/systems and networks.

5.2.3 The least possible number of privileges are provided to authorized agents and electronic service providers in applications/systems and devices to perform their duties.

5.3 Application/Systems, Devices, and Networks – Controls must be implemented to secure applications/systems, devices, and networks, and establish procedures to secure their ongoing management and operation including updating patches and anti-virus software.

5.4 Assurance – Privacy and security risks and areas of non-compliance must be identified and mitigated. Auditing and monitoring activities on agents and Electronic Service Providers who have access to PHI must be performed to ensure compliance.

5.5 Electronic Service Providers – Controls must be in place to govern Electronic Service Providers who have access to PHI in order to protect and maintain confidentiality, integrity and availability of PHI.

5.6 Information Security Incident Management - An information security incident management process must be implemented to identify and resolve incidents quickly and effectively, while minimizing their impact and reducing the risk of similar incidents from occurring.

5.7 Protection of PHI – Tools or procedures must be implemented to ensure that appropriate methods exist to communicate PHI securely (e.g., through the use of encrypted email).

6. Information Security and Procedures

6.1 General

6.1.1 Only use your assigned user ID and password (“credentials”) when accessing any application/system (including shared systems), device, or network resource.

6.1.2 Never allow another person to use your credentials. You are accountable for any actions performed using your credentials.

6.1.3 Never disable, override or willfully bypass any security control on any application/system (including shared systems), device, or network resource.

6.1.4 Never attempt to exploit any suspected security weakness on any system, device, or network–even to explore that such a weakness may exist—unless it is part of your assigned job duties or responsibilities and you are explicitly authorized to do so.

6.1.5 Never knowingly perform an act that will interfere with the normal operations of any shared system, or try to disrupt that system, either by intentionally making the system unavailable, or by affecting the integrity of the data being stored in or processed by that system.

6.2 Personal Use

6.2.1 Incidental personal use of email and the Internet is permitted, as long as it does not interfere with the normal performance of those devices or the network and does not interfere with your job-related duties and responsibilities.

6.3 Protecting PHI

6.3.1 Only access PHI if you are required to do so and it is necessary to do so (e.g., to provide or assist in the provision of healthcare).

6.3.2 When accessing shared systems that provide access to PHI, abide by their terms and conditions.

6.3.3 Use only devices, processes, and tools approved by Strathmere Lodge to view, access, collect, or dispose of PHI, either locally or from a remote location.

6.3.4 Only store PHI on approved devices or storage networks, and only store the minimal amount of PHI necessary on any encrypted portable storage media (e.g., an encrypted USB stick, laptop or tablet).

6.3.5 Never take a picture of PHI (e.g., with a camera or cellphone).

6.3.6 Never discuss PHI with any person that does not have a need-to-know or is not authorized to know the information. Prior to disclosing PHI, if you are uncertain about the person’s identity, ask them to provide you with information that can be used to verify their identity.

6.3.7 Never discuss PHI in public areas, including elevators, as it may be easily overheard by those who do not have a need-to-know. Even in the office, be mindful of eavesdropping.

6.3.8 Lock up PHI in any form (e.g., locking paper or portable storage media containing PHI in a cabinet) when left unattended in an unsecured area, especially when the office or area is vacated.

6.3.9 Lock your screen (e.g., by pressing ctrl + alt + delete and selecting “Lock this computer” on a Windows workstation) when leaving your computer unattended.

6.3.10 Never use PHI obtained using the EHR Solution for research purposes.

6.3.11 Always ensure that paper documents containing PHI are shredded or placed in a secure shredding receptacle when they are no longer needed.

6.4 Email

6.4.1 Use caution when opening email attachments received from unknown senders, as these may contain malware.

6.4.2 Only use the email account provided to you when sending/receiving PHI to/from patients, health information custodians, or other relevant parties. Never use external email accounts (e.g., Hotmail, or Gmail).

6.4.3 Either encrypt emails that contain PHI, use a secure file transfer solution, or use a secure email system approved by Strathmere Lodge.

6.4.4 Sensitive information in emails must only be sent when necessary and acceptable for the purpose of providing or assisting health care.

6.5 Printing, Faxing, and Photocopying

6.5.1 Retrieve paper that contains PHI from the printer immediately.

6.5.2 Confirm the phone number prior to faxing a document that contains PHI and verify that it was dialed correctly.

6.5.3 Ensure that you do not leave original materials in photocopiers or fax machines.

6.6 Social Media

6.6.1 Consider everything that you post online as public, even if privacy controls have been added to restrict access to your social media account.

6.6.2 Always be professional. Never post anything that could damage the reputation of Strathmere Lodge or any of your colleagues.

6.6.3 Never, either expressly or implicitly, attribute personal statements, opinions or beliefs to Strathmere Lodge when posting online.

6.6.4 Never post any type of PHI (even if you do not include personal identifiers, such as a patient's name).

6.6.5 Refrain from "friending" or "following" patients unless a prior personal relationship pre-dates your employment at Strathmere Lodge or the patient's treatment by Strathmere Lodge.

6.6.6 Do not post content considered to be discriminatory, disparaging, defamatory, harassing, or that can create a hostile work environment. An agent's after-hours use of social media may lead to disciplinary action or termination if such use is found to tarnish the image of Strathmere Lodge or the image of its agents or electronic service providers.

6.7 Creating and Protecting Passwords

Passwords are the first line of defense in protecting access to electronic PHI and other sensitive electronic information. However, they are only effective if they are too difficult to guess by another person and kept a secret.

6.7.1 Always create passwords that are at least eight characters long and include at least three of the following:

- One number
- One uppercase letter
- One lowercase letter, or
- One special character.

6.7.2 Never create passwords that include:

- All or part of your ID.
- Easily obtained personal information about yourself (e.g., names of family members, pets, birthdays, anniversaries, or hobbies).
- Three consecutive characters *(e.g., 'AAA').

6.7.3 Use phrases (e.g., "IL0v3It@ly)", where possible, when creating passwords.

6.7.4 Choose passwords that are easy to remember but difficult to guess by someone else.

6.7.5 Never change passwords in an easily recognized pattern (e.g., changing the number at the end of a password, such as changing "IL0v3It@ly1" to "IL0v3It@ly2").

6.7.6 Ensure that your passwords are different from password(s) used for personal accounts (e.g., personal email or personal banking, etc.).

6.7.7 Commit your passwords to memory. Avoid keeping a record of your passwords (e.g., on paper, or stored on in a file), unless it:

- Can be stored securely, and
- Does not indicate the associated ID or the system for which it is used.

6.7.8 Keep your passwords a secret. Never tell anyone your password.

6.7.9 Immediately change your password if you suspect that someone else may know your password and notify the Privacy and Security Officer.

6.7.10 Do not include your credentials ID in any automated sign-on process (e.g., saving it in a browser).

6.7.11 Always change any password that is provided to you at initial login.

6.8 Working Remotely

6.8.1 Follow the proper procedures to disconnect from any application or system (including shared systems) that provides access to PHI (e.g., use the disconnect/logout option rather than simply closing the application).

6.8.2 Never access any application or system (including shared systems) to provide access to PHI in an area where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).

6.8.3 Never leave your mobile device that has the ability to access PHI, unattended in a public place.

6.8.4 When required to leave your mobile device in a vehicle, lock it in the trunk or place it out of view before getting to your destination. If you get to the destination before securing the device you should take it with you instead.

6.8.5 Ensure that if personal health or personal information is downloaded onto your mobile device, the location where the data is stored is encrypted or the device utilizes full disk encryption.

6.8.6 For remote (VPN) access ensure the following:
Maintain security through firewalls, and other means, using industry best practices (e.g., encryption). Any personal health information that must be transmitted outside the organization must be encrypted using industry standard methods.

6.9 Reporting Privacy Breaches and Security Incidents

6.9.1 Examples of privacy breaches and security incidents include, but are not limited to:

- Unauthorized disclosure of PHI
- Theft or loss of information technology that contains PHI, even if it is encrypted
- Virus or malware infection
- Attempts (either failed or successful) to gain unauthorized access to any form of PHI (paper or electronic)
- Compromised password (i.e., another individual knows your password)

6.9.2 Immediately report suspected or confirmed privacy breaches or security incidents to the Information and Security Officer. The Information and Security Officer shall contact the organizations Privacy Contact.

6.9.3 Provide your full cooperation with any information security incident investigation.

6.10 Cryptography

6.10.1 Only use the EHR Solution-approved cryptographic algorithms for connections established with the EHR Solution. A list of approved cryptographic algorithms can be found in Appendix A: Approved Cryptographic Algorithms.

6.10.2 Ensure that each cryptographic key or key component has the fewest number of key custodians necessary.

6.10.3 All persons must ensure that if PHI resides on a mobile device, it must be encrypted, or the device itself must utilize full disk encryption.

6.11 Electronic Service Provider

6.11.1 Middlesex County has identified their Electronic Service Providers in Appendix B: ESP List and have categorized their ESP(s) according to supplier type (e.g., application service provider, network service provider, storage service provider, etc.) and criticality of the services provided.

6.11.2 The ESP agrees to use the information shared with it only as needed to fulfill the contract and to put effective administration, technological and physical safeguards in place to prevent theft, loss or unauthorized access, copying, modification, use, disclosure or disposal of information.

6.11.3 The ESP agrees to follow all applicable privacy laws, including PHIPA.

6.11.4 Middlesex County has formally documented the:

- Technological and organization relationship covering ESP roles and responsibilities under the Personal Health Information Protection Act and its regulations (PHIPA) and under Middlesex County information security policies and procedures - refer to Appendix C.
- Roles and responsibilities for implementing, maintaining and supporting the information systems or services that ESP is required to fulfill.
- Service goals.
- Expected deliverables.
- Representatives of ESP.

6.11.5 Formal documentation may include contracts, agreements and service levels.

6.11.6 Middlesex County has assessed the potential information security and privacy risks posed by all new Electronic Service Providers to the EHR Solution prior to engaging in a contractual relationship with that Electronic Service Provider.

6.11.7 Middlesex County has defined and documented all information systems and services to be provided by ESP, or on renewal of Service Agreements. Service agreements should specify:

- Roles and responsibilities under PHIPA and under the information security policies and procedures implemented in respect to the EHR Solution.
- Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided.
- The level of criticality of the service.
- The dates and times when the service is required.
- The capacity requirements of systems and networks.
- Maximum permissible down-time and service level objectives.
- Service level reports and frequency.
- Critical timescales (e.g., the timescale beyond which a loss of service would be unacceptable to Middlesex County.
- The penalties to be imposed in the event ESP fails to deliver the pre-agreed level of service or fails to fulfill its roles and responsibilities.
- Minimum information security and privacy controls.

6.11.8 Middlesex County requires their ESP(s) and any new Electronic Service Providers to implement applicable information security and privacy controls prior to the Electronic Service Provider being granted access to the EHR Solution.

6.11.9 Middlesex County has established a consistent method for handling the termination of relationships with their ESPs, which may include:

- Designating agents responsible for managing the termination.
- Revocation of physical and logical access rights to the organization's information.
- Secure return, transfer or destruction of all assets (e.g., back-up media storage, documentation, hardware, and authentication devices).

6.12 Information and Asset Management

6.12.1 Middlesex County will ensure that all PHI that is transmitted to the EHR Solution eHealth Program Office and Clinical Connect Program Office through the ONE Mail system.

6.13 Information Security Incident Management

6.13.1 Middlesex County has the ability to implement a security incident ("incident") management process to deal with incidents related to the EHR Solution.

- Identification/Triage
- Response
- Recovery, and
- Follow-up

(See Appendix D: Information Security Incident Management Process diagram).

6.13.2 If at any point in the incident management process Middlesex County realizes that the incident has resulted in a privacy breach, then the incident will be handled in accordance with the Middlesex County Personal Health Information and Privacy Policies and Procedures.

6.13.3 With Respect to Identification/Triage, the Information and Security Officer is the point of contact to which actual or suspected incidents related to the EHR Solution are reported. The Information and Security Officer will notify the Privacy Contact.

6.13.4 The Information and Security Officer has or will ensure that agents and ESPs are aware of their responsibility to immediately report actual or suspected incidents.

6.13.5 The Information and Security Officer will generate an incident ticket or log for all reported incidents related to the EHR Solution. At a minimum, the incident ticket will contain the following elements:

- The time and date of the reported incident.
- The name and contact information of the agent or Electronic Service Provider that reported the incident.
- Details about the reported incident, (e.g., type and how it was detected).
- Any impacts of the reported incident.
- Any actions undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident or the point of contact.

6.13.6 The Information and Security Officer is responsible for initiating the triage, response, recovery and follow-up activities for incidents related to EHR Solution. This includes verifying whether or not an incident has occurred.

6.13.7 The Information and Security Officer will classify all actual incidents related to the EHR Solution according to severity (See Appendix E: Incident Severity and Priority Ratings for severity ratings).

6.13.8 The Information and Security Officer will initiate an incident report related to the EHR Solution (See Appendix F: Incident Report Details).

6.13.9 The Information and Security Officer on behalf of Middlesex County will notify the EHR Solution eHealth Program Office and the Clinical Connect Program Office by ONE Mail or telephone and any affected HICs by the end of the next business day of confirmed incidents that are classified as Severity 1 or Severity 2 according to Appendix E: Incident Severity and Priority Ratings.

6.13.10 At a minimum, the notification will contain the following elements:

- The time and date of the reported incident
- The name and contact information of the agent or Electronic Service Provider that reported the incident
- Details about the reported incident (e.g., type and how it was detected)
- Any known or suspected impacts of the reported incident, and
- Any actions undertaken to contain the incident either by the agent or Electronic Service Provider that reported the incident, the point of contact, or the incident response lead or team.

6.13.11 If an incident that originates at Middlesex County affects multiple HICs or EHR Solution, the EHR Solution Health Program Office may assume leadership of the incident management activities.

6.13.12 The individual or team that leads the incident management activities must notify the Applicable Oversight Body. Note: Middlesex County is a viewing organization, so the lead agency will be the EHR Solution eHealth Program Office. Middlesex County may be asked to participate in the notification process.

- Within 72 hours of notification for any incident related to the EHR Solution and classified as a Severity 1 or
- Within one week of notification for any incident related to the EHR Solution and classified as a Severity 2.

6.13.13 Middlesex County will prioritize incidents related to the EHR Solution.

6.13.14 The Information and Security Officer will take steps to limit the scope and magnitude of an incident. Mitigation or containment activities may include:

- Backing up the information system
- Discontinuing operations
- Changing passwords or modifying access control lists on the compromised information system, or
- Restricting connectivity.

6.13.15 NOTE: Depending on the severity of an incident it may be necessary to activate Middlesex County business continuity plans.

6.13.16 Middlesex County will remediate affected information systems so that they return to full and normal operations. Remediation activities may include:

- Eradicating the cause of the incident (e.g., removing malware)
- Restoring and validating the information system
- Deciding when to restore operations, and
- Monitoring information systems to verify normal operations without further information system or data compromise.

6.13.17 Middlesex County will investigate incidents related to the EHR Solution to identify the cause of the incident (e.g., by performing a root causes analysis.)

6.13.18 Once an incident related to the EHR Solution has been resolved (e.g., all remediation activities have been implemented and affected information systems and information technology have returned to full and normal operations), the Information and Security Officer will complete the incident report. During longer investigations led by Middlesex County, the EHR Solution eHealth Program Office may request status updates on the incident investigation in the interim.

6.13.19 Middlesex County will archive its incident reports related to the EHR Solution for a minimum of 24 months.

6.13.20 Middlesex County will provide the EHR Solution eHealth Program Office with an incident report related to the EHR Solution within 72 hours of the incident report being requested.

6.13.21 The final incident reports should be reviewed by the Connecting Security Committee and if necessary, the Applicable Oversight Body.

6.13.22 Middlesex County will implement a mechanism to review its incidents related to the EHR Solution at a minimum, monthly to identify trends and to determine whether any preventative actions can be taken to reduce the likelihood of similar incidents from occurring in the future.

6.13.23 Middlesex County will develop procedures for collecting evidence for the purposes of disciplinarily or legal action against agents or The ESP. These procedures should require:

- Forensics work to be performed on copies of the evidential material
- The creation of copies be witnessed
- Details of the creation be logged, including:
    - ✓ When and where the copying process was executed
    - ✓ Who performed the copying activities, and
    - ✓ Which tools or programs were utilized for the copying process
    - ✓ The integrity of all evidential material is protected.

6.14 **Local Registration Authority**

6.14.1 Middlesex County uses ClinicalConnect as its Identity Provider and follows the procedures established by ClinicalConnect.

6.14.2 The LRA has been trained to use ClinicalConnect policies and practices.

6.14.3 ClinicalConnect has provided for the assignment of eHealth Ontario Assurance Levels in the ClinicalConnect Access Governance system.

6.14.4 The following policy statements address eHealth Ontario LRA practice requirements and will be maintained by the LRA when provisioning users with access to ClinicalConnect where provincial EMR data sets (i.e., DHDR, DI-CS, AC-CDR, PC-CDR) are available for viewing.

6.14.5 Middlesex County has identified the Strathmere Lodge Administrator as the legally responsible person (LRP) for Strathmere Lodge. Strathmere Lodge has identified the Strathmere Lodge Administrator as the LRA to manage the enrollment of its agents and Electronic Services Providers (specifically the ESP) who require access to the EHR Solution.

6.14.6 The LRA will ensure that:

- They have the time and resources required to perform the duties.
- They are stable in their current position (not subject to reassignment).
- They meet Level 2 assurance qualifications according to the Federation Identity Provider Standard.
- They understand the importance of policy adherence, especially privacy and information security.

6.14.7 The LRA is registered at Assurance Level 2 (AL2) or higher to register End Users. The LRA will not register an End User at a Level of Assurance higher than his own Level of Assurance.

6.14.8 Modifications to the status of the LRA and LRP will be based on a request from the LRA or LRP, as the case may be, or if it is suspected or discovered that LRA or LRP is non-compliant with relevant policies, procedures or agreements.

6.14.9 If the status of the LRP is revoked or suspended, as LRP he must submit a request to lift the suspension before the status may be reinstated.

6.14.10 With respect to enrolling an Agent or Electronic Service Provider with access to the EHR Solution, the LRA will verify the identity of each Agent or Electronic Service Provider requesting access to the EHR Solution and ensure that each End User registered is 16 years of age or older. An individual shall be assigned a defined Level of Assurance at the time of Registration. Assurance Level 1 (AL1) and Assurance Level 2 (AL2) are relevant to ClinicalConnect.

6.14.10.1 Assurance Level 1 (AL1) is appropriate for information that has a sensitivity level of “unclassified” and is normally used for public information and internal communications such as internal documents and unclassified communications, normally intended for communication between staff. AL1 is insufficient when Personal Health Information or Personal Information will be accessed.

6.14.10.2 For ClinicalConnect access (access to PHI), AL1 is not acceptable. When access to the ClinicalConnect Access Governance System ONLY is required for the LRP, Information and Security Officer and the LRA, the LRP will automatically be set to AL1. If access to ClinicalConnect itself (PHI viewer) is required, the Assurance Level will be changed to AL2 as appropriate.

6.14.10.3 Assurance Level 2 (AL2) is appropriate for information that has a high sensitivity level within Middlesex County or the health sector environment, and that is intended for use by specific and Authorized individuals only. If compromised, this information could reasonably be expected to cause serious injury or financial losses to one or more of the parties involved or would require legal action for correction. For access to PHI in ClinicalConnect, AL2 is required. Privacy Auditors must also be assigned an AL2.

6.14.10.4 To be registered at AL2, applicants will present one document from the list of Primary Identity documents. Applicants will also present one document from either the Primary or Secondary Identity Document lists. These lists are available at https://accessonehealth.ca/

6.14.10.5 Agents or Electronic Service Providers whose identities have already been verified by Middlesex County in accordance with the EHR Solution’s Level 2 assurance requirements do not need to have their identities revalidated. The LRA will still ensure that the individual that requested access is the one who was authorized. For example, if the on-boarding process for Middlesex County requires an agent to present at least two identity documents with one of the documents being from the primary identity document list (see Appendix G: Acceptable Identity Documents) and the other from either the primary identity document list or secondary identity document list (see Appendix G: Acceptable Identity Documents), and Middlesex County has a record of these document (e.g., in an agent’s file) then Middlesex County does not need to revalidate identity of agents associated with Middlesex County. All requests for access to the EHR Solution must be approved by the Sponsor (the LRA).

6.14.11 The Sponsor will retain a copy of his approval when enrolling an agent or Electronic Service Provider with access to t EHR Solution.

6.14.12 Once access to the EHR Solution has been revoked, agents or Electronic Service Providers will re-enroll in order to have their access to the EHR Solution reinstated.

6.14.13 The Sponsor will suspend an End User account if information is discovered suggesting that:

- A registration was misleading, false, or fraudulent
- An End User failed to comply with policy, standards, agreements, or terms and conditions

- The End User’s suspension is requested by a Sponsor or Registration Authority.

6.14.14 An account that has been suspended due to misleading, false, or fraudulent information will not be used or reactivated unless the relevant information, documentation, or other material facts are true, accurate, and complete.

6.14.15 The Sponsor will document and retain a reason for a suspension and any resulting actions taken, including any investigation.

6.14.16 The Sponsor will revoke the account of an End User if:

- The individual no longer needs to account (e.g., deceased, resigned, retired)
- It is determined the account is a duplicate
- It is determined that the information, documentation, or any other matter provided for registration was misleading, false, or fraudulent
- The identity has been compromised (e.g., identity theft)
- Requested by the end user

6.14.17 The Sponsor will document and retain a reason for a revocation and any resulting actions taken, including any investigation.

6.14.18 The LRA will identify a named person(s), group(s), or role(s) that has the authority to act as a sponsor in the LRA’s place.

6.14.19 The Sponsor will only provide access to the EHR Solution clinical components to Agents whose purpose of access is to collect PHI for providing or assisting in the provision of healthcare.

6.14.20 The Sponsor will only provide access to the EHR Solution administration components to Agents and Electronic Service Providers whose purpose of access is to:

- Provide support for defined and permitted functionality within the administration roles of the EHR Solution (e.g., Privacy Officers, System Administrators). Such access will not be granted to functionality intended for those providing health care or assisting in the provision of health care (e.g., Pharmacists). For example, privacy officers may require access to privacy reports to generate audit reports. These individuals will not be granted access to functionality intended for those providing healthcare or assisting in the provision of health care (e.g., Pharmacists).

6.14.21 Sponsors will not provide access to the EHR Solution if access is requested for purposes other than providing or assisting in the provision of healthcare, e.g., providing access for the purposes of:

- Program planning, evaluation, or monitoring
- Risk or error management
- Improving the quality of care, programs, and services
- Education and training (unless the individual is a student or resident who requires access to provide care)
- For processing payments. Sponsors must not provide access to the EHR Solution if access is requested for the purpose of research.

6.14.22 If an agent or ESP has multiple roles (e.g., is both a pharmacist and a risk manager), the Sponsor may assign that person with access to the EHR Solution for the purposes of collecting PHI for providing or assisting in the provision of health care and must ensure that the end user understands their permissions and obligations.

6.15 Network and Operations

6.15.1 The ESP on behalf of Middlesex County will implement network zones and manage these network zones in a manner that observes the separation of different computing environments. The segregation of networks may be based on criteria, such as:

- The classification of information transmitted on the network.
- The level of assurance required.

6.15.2 The ESP on behalf of Middlesex County will control traffic between networks zones by using a security gateway at the zones' perimeter.

6.15.3 The ESP on behalf of Middlesex County will implement a process to review security gateway configurations at least annually. The process should ensure the:

- Review of the rule sets on their security gateways
- Removal of expired or unnecessary rules
- Resolution of conflicting rules, and
- Removal of unused or duplicate objects (e.g., network or computer systems)

6.15.4 Malware detection and repair software or equivalent solution should be implemented on tools and workstations approved by

Middlesex County, to protect from malicious code. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writeable capabilities. Questions regarding the appropriateness of alternative solutions should be directed to the Information Security Officer for the EHR Solution which can be put forward to the Connecting Security Committee.

6.15.5 Middlesex County will keep its malware detection and repair software up-to-date.

6.15.6 Middlesex County may request executive summaries (results) of TRAs that are completed on the EHR Solution.

6.15.7 Where Middlesex County receives a TRA from the EHR Solution eHealth Program Office, Middlesex County will restrict access to that TRA and any supporting documentation and ensure that the TRA is handled in a secure manner.

7. Roles and Responsibilities

7.1 All agents and electronic service providers must read and comply with the section 6 ("Policy Requirements") of this policy.

7.2 The Information and Security Officer for Middlesex County will ensure compliance with this policy and any other information security policies, standards, and supporting documents.

7.3 The Information and Security Officer will:

- Develop, implement and maintain the policies and procedures embedded within this document to ensure compliance.
- Ensure that the ESP and all agents are appropriately informed of their information security responsibilities.
- Ensure that the ESP and all agents who have access to PHI, agree to an end user agreement that includes confidentiality provisions, before being provided with access to PHI.
- Hold The ESP and all individual agents accountable for unauthorized or inappropriate access, collection, use, disclosure, disposal, destruction, modification, or interference of PHI, or any application/system (including shared systems), device, or network that is used to collect, access, or store PHI

8. Actions

Any exceptions to this Policy must be approved by the LRP, who will authorize exceptions only where there is clear justification to do so and only to the minimum extent necessary to meet the justified need.

9. Enforcement

9.1 Strathmere Lodge may monitor applications/systems, devices, and network traffic at any time to ensure compliance with this policy. All instances of non-compliance will be reviewed by the Information and Security Officer and the EHR Solution eHealth Program Office.

9.2 Strathmere Lodge has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Appendix A – Approved Cryptographic Algorithms

Algorithm	Minimum Key Length	Appropriate Usage	
Symmetric Key Algorithms			
AES	128-bits	Data encryption: • Session • Storage ○ Backup ○ Archival	Key encryption: • Session • Storage ○ Backup ○ Archival
Skipjack	80-bits, with 32 iterations	Data encryption: • Session • Storage ○ Backup ○ Archival, < 5 years	
Triple DES	112-bits	Data encryption: • Session • Storage ○ Backup ○ Archival	Key encryption: • Session • Storage ○ Backup ○ Archival
Asymmetric Key Algorithms			
Elliptic Curve	160-bits		
RSA	2048-bits		
MACs and Hashes			
AES MAC	128-bits	Message authentication.	
MD5[3]	128-bits, with 16 iterations	Message authentication and message digest.	
SHA-1[4]	Not applicable.	Message authentication and message digest.	
SHA-2	Not applicable.	Message authentication and message digest.	

Algorithm	Minimum Key Length	Appropriate Usage
TDES (Triple DES) MAC	112-bits	Message authentication.
DSA (Digital Signature Algorithm)	1024-bits	Digital Signature.
Elliptic Curve DSA	160-bits	Digital Signature.
RSA DSA	2048-bits	Digital Signature.
Digital Certificates		
X.509 v3 compliant	N/A	Binds a public key with a specific identity.
Key Transport/Agreement Algorithms		
Diffie-Hellman	1024-bits	Digital Session key establishment
Elliptic Curve Diffie-Hellman	160-bits	Digital Session key establishment
Cryptographic Protocols		
TLS 1.1 and higher	N/A	Protocol to authenticate and encrypt communication between authenticated

[3] All *new* implementations of MACs and hashes must not be based on MD5.

[4] All *new* implementations of MACs and hashes must not be based on SHA-1.

Appendix B – Form to Record Electronic Service Providers

Instructions:

Use this form to document the Electronic Service Providers (ESPs) your organization has service relationships with, as well as updating those that become obsolete or retired. Complete one form for each ESP relationship. ***This form must not contain any personal health information.***

Retention:

Once the form is completed, it should be retained for as long as your organization has electronic service provider relationships in place or as required by your organization's record keeping policies.

Yearly Updates:

It is suggested that every year, you review your organization's list of electronic service providers and reflect any changes in this template. Enter new electronic service provider relationships into the form when their service begins.

Store completed document in:

<Enter a secure location on your organizations' network, with access controls limited to those who require the information.>

Electronic Service Provider (ESP) Relationship Agreement Form

The ESP agrees to use the information shared with it only as needed to fulfill the contract and to put effective administration, technological and physical safeguards in place to prevent theft, loss or unauthorized access, copying, modification, use, disclosure or disposal of information. The ESP agrees to follow all applicable privacy laws, including the Personal Health Information Protection Act (PHIPA) and adhere to its roles and responsibilities under the Act.

Electronic Service Provider Relationship Information	
Name of ESP	
Contact Information for ESP Representative	
Will Middlesex County grant the ESP access to PHI in the EHR Solution? If yes – ensure the ESP reviews and signs off on the full Middlesex County Information Security Policies and Procedures	

Supplier Type (i.e., application service provider, network service provider, storage service provider, IT service provider)	
Criticality Priority 1 – Critical Priority 2 – High Priority 3 – Medium Priority 4 – Low	
Roles, Responsibilities, Service Goals, and Expected Deliverables List information systems or services that the ESP is providing or maintaining and the role the ESP is expected to perform.	
Service Details (Service Details (please indicate n/a if field is not applicable to supplier type or service being performed)	
Dates that service is required	
Capacity requirements of systems and networks	
Maximum permissible down-time and service level objectives	
Service Level reports and frequency	
Critical timescales e.g., the timescale beyond which a loss of service would be unacceptable to Middlesex County	
Penalties to be imposed if the ESP fails to deliver the pre-agreed level of service or fails to fulfill its roles and responsibilities	
Minimum information security and privacy controls. (i.e., any additional controls that need to be in place on a project-by-project basis when work is considered highly sensitive)	

Appendix C - ESP Roles and Responsibilities Under Legislation

- *Personal Health Information Protection Act (PHIPA)*

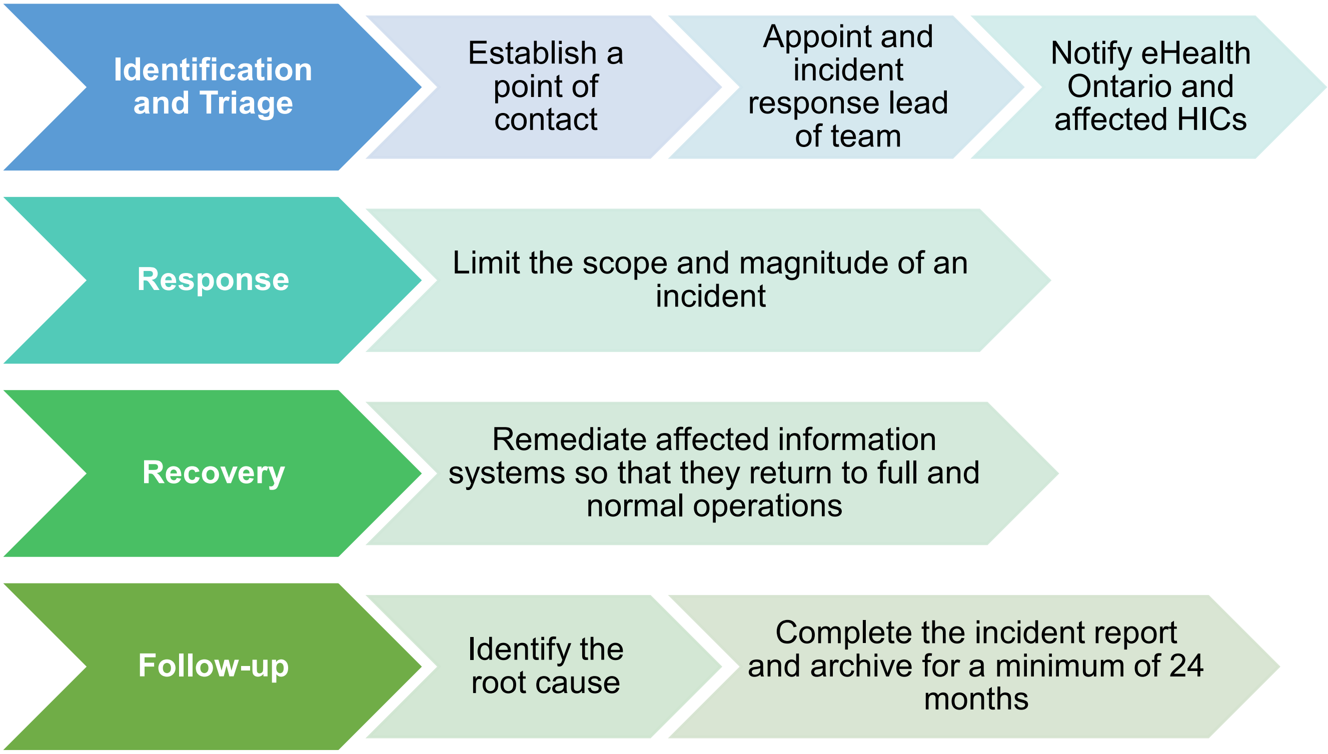
  Under s. 10(4) - A person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.

- *Ontario Regulation 329/04*

  Under s. 6.(1) - Except as otherwise required by law, the following are prescribed as requirements for the purposes of subsection 10 (4) of the Act with respect to a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, and who is not an agent of the custodian:

  1. *The person shall not use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services.*
  2. *The person shall not disclose any personal health information to which it has access in the course of providing the services for the health information custodian.*
  3. *The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection.*

Appendix D – Information Security Incident Management Process



Identification and Triage

- Establish a point of contact
- Appoint and incident response lead of team
- Notify eHealth Ontario and affected HICs

Response

- Limit the scope and magnitude of an incident

Recovery

- Remediate affected information systems so that they return to full and normal operations

Follow-up

- Identify the root cause
- Complete the incident report and archive for a minimum of 24 months

Appendix E – Incident Severity and Priority Ratings

Severity Ratings

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
1	**Critical** • Critical or multiple sites down • Loss of service poses substantial risk to participating HICs • Posing a public health safety, privacy or security risk • Causing significant adverse impact affecting a large number of internal and/or external systems, e.g., large scale malware outbreak Immediate response and restore – "all hands on deck".	30min	6hrs	72hrs
2	**High** • Single, critical site down • Loss of non- mission-critical service • Help desk unavailable. • Remedy Failure • Service degradation affecting HICs Response/restore as quickly as possible - within one business day	2hrs	12hrs	24hrs
3	**Medium** • Application or physical component slowdowns • Minor technical or function problems • Application or component failure affecting single client Restore within the next few business days	4hrs	36hrs	48hrs
4	**Low** • Minimal impact, not time- critical, or work-around exists. Restore within a week	24hrs	36hrs	15 days

Priority Ratings

Incident Type	**Priority Rating**	
	P2	**P1**
Access Control: Reserved for security incidents related to a potential compromise of access control.		
Privilege account compromised E.g., a Privileged ID (such as system administrators, database administrators, and firewall administrators) demonstrates unusual activities/behaviors (e.g., unexplained log-ins, unexplained file accesses).	X	
Phishing attack detected – targeting privileged users E.g., numerous suspicious emails targeting users with privileged access.	X	
Asset security: For incidents that involve lost or stolen assets and attacks to an asset causing disruption of service.		
Loss of unencrypted storage media E.g., loss of an unencrypted USB drive containing sensitive data is lost.	X	
Denial of Service (DOS) attack against a critical asset detected E.g., a DOS attack has been initiated against a server hosting business critical applications	X	
Data security: For incidents that threaten the confidentiality of data.		
Unusually high volume of data access on server(s) hosting sensitive data/applications that process or store sensitive data E.g., a system alarm is triggered that there is a high volume of data transfer during non- business hours (not caused by data back-up)	X	
Malware / Virus infection detected– high impact E.g., an alarm is triggered that a virus outbreak was detected	X	
Data and System Integrity: Incidents related to a potential compromise of integrity of data and systems		
Major data breach that has attracted media attention: E.g., a major data breach that has attracted media attention		X
Tape back-up failed on over period of time E.g., A tape back-up failed for the past five sessions	X	

Appendix F – Incident Report Details

The following details are required in an information security incident report:

1. Contact Information of the agent or Electronic Service Provider that reported the incident, AND the incident response lead or team
   - Name
   - Unit (e.g., department, division, team) (if applicable)
   - Email address
   - Phone number
   - Location (e.g., mailing address, building and room number)
2. Incident Details
   - Date/time when the incident was discovered
   - Estimated date/time when the incident started
   - Incident ticket number
   - Type of incident (e.g., denial of service, malicious code, unauthorized access, inappropriate usage)
   - Physical location of the incident (e.g., city)
   - Current status of the incident (e.g., ongoing attack)
   - Source/cause of the incident (if known), including hostnames and IP addresses
   - Description of the incident (e.g., how it was detected, what occurred)
   - Description of affected resources (e.g., networks, hosts, applications, data), including information systems' hostnames, IP addresses, and function
   - Operating system, version, and patch level
   - Antivirus software installed, enabled, and up-to-date (yes/no)
   - Mitigating factors
   - Estimated technical impact of the incident (e.g., data deleted, system crashed, application unavailable)
   - Actions performed by the agent or Electronic Service Provider who reported the incident (e.g., shut off host, disconnected host from network)
   - Other organizations contacted (e.g., software vendor)
   - Type of information compromised (if applicable)
3. General Comments (recommended but not required)
4. Summary of the Incident
5. Contact information for all involved parties
6. Log of containment/mitigation actions taken by incident response lead/team
7. List of evidence gathered
8. Cause of the Incident (e.g., misconfigured application, unpatched host)
9. List of recommended and implemented remediation activities
10. Current Status of the Incident Response

Appendix G – Acceptable Identify Documents

Social Insurance cards and provincial health cards are NOT acceptable forms of identification.

Under the Photo and Expiry Dates columns, “Unknown” means that the document may or may not contain a photo or expiry date depending on the origin or version of the document.

Primary Identity Documents

Government Document Type	Photo?	Expiry Date?
Driver’s License (including graduated driver’s license)	Yes	Yes
Canadian Passport	Yes	Yes
Certificate of Canadian Citizenship (paper document or plastic card but excludes commemorative issue)	Yes	No
Birth Certificate issued by a Canadian Province or Territory	No	No
Canadian Certificate of Birth Abroad	No	No
Canadian Certificate of Indian or Metis Status	Yes	No
Canadian Permanent Resident Card	Yes	Yes
Statement of Live Birth from Canadian Province (Certified Copy)	No	No
Certification of Naturalization (paper document or plastic card but excludes commemorative issue)	No	No
Citizenship Identification Card issued by a foreign jurisdiction where these exist (e.g., Mexico, Europe)	Unknown	Unknown
Confirmation of Permanent Resident (IMM 5292)	No	Yes
CANPASS (A Remote Area Border Crossing permit allowing the bearer to cross into Canada at certain remote areas without reporting to a port of entry as long as imported goods are declared)	Yes	Yes
Nexus (A cross-border express pass available to low-risk individuals who have passed a stringent Canadian and American security check including a fingerprint biometric, photograph and personal interview with immigration officials. In order to maintain this pass, the individual must reapply every two years.)	Yes	Yes
Firearm Registration License	Yes	Yes
A valid Passport issued by a foreign jurisdiction.	Yes	Yes
Immigration Canada - Refugee Claimant ID Document	Yes	Yes
Ontario Photo Card	Yes	Yes

Secondary Identify Documents

Document Type	Expiry Date?
Old Age Security Card	No
Certificate issued by a government ministry or agency, e.g., Marriage, Divorce, Adoption	No
Canadian Convention Refugee Determination Division Letter	No
Canadian Employment Authorization	Yes
Canadian Minister’s Permit	Yes
Canadian Immigrant Visa Card	Yes
Canadian Student Authorization	Yes
Record of Landing (IMM 1000)	Yes
Document showing the registration of a legal change of name accompanied by evidence of use or prior name for the preceding 12 months	No
Current Registration Document from the College of a Health Profession under the Regulated Health Professions Act, 1991. Audiology and Speech Language Pathology Chiropody Chiropractic Dental Hygiene Dental Technology Dentistry Denturism Dietetics Massage Therapy Medical Laboratory Technology Medical Radiation Technology Medicine Midwife Nursing Therapy Occupational Therapy Optician Optometry Physiotherapy Psychology Respiratory	Unknown
Federal, Provincial, or Municipal Employee Card	Unknown
Current Employee Card from a Sponsoring Organization	Unknown
Union Card	Unknown
Other Federal ID Card, including Military	Unknown
Ontario Ministry of Natural Resources Outdoors Card	Unknown
Judicial ID Card	Unknown
Student Identification Card	Unknown
BYID Card (Formerly Age of Majority Card)	Unknown

Document Type	**Expiry Date?**
CNIB (Canadian National Institute for the Blind) Photo Registration Card	Unknown
Canadian Police Force Identification Card	Unknown
Blind Persons Right Act ID Card	Unknown
Current Professional Association License/Membership Card (for any Regulated Health Profession including the following: Association of Ontario Midwives Denturist Association of Ontario Nurse Practitioner Association of Ontario Ontario Association of Medical Radiation Technologists Ontario Association of Naturopathic Doctors Ontario Association of Orthodontists Ontario Association of Speech Language Pathologists and Audiologists Ontario Chiropractic Association Ontario Dental Association Ontario Medical Association Ontario Nurses' Association Ontario Opticians' Association Ontario Pharmacists' Association Ontario Physiotherapy Association Ontario Podiatric Medical Association Ontario Society of Chiropodists Ontario Society of Medical Technologists Registered Nurses' Association of Ontario Registered Practical Nurses' Association of Ontario Respiratory Therapy Society of Ontario	Unknown

Appendix H – Contact List

Contact	At:	For:
Middlesex County: Privacy Officer	clerk@middlesex.ca	All incidents/inquiries related to Middlesex County
The EHR Solution Program Office: eHealth Ontario's Service Desk	1-866-250-1554 servicedesk@ehealthontario.on.ca	To report any real or suspected Security Incidents related to the EHR Solution
ClinicalConnect Solution Provider: HITS Helpdesk	(905) 521-2100 ext. 43000 helpd@hhsc.ca	Technical Support when using ClinicalConnect

Appendix I – References

Legislative – PHIPA s. 12, 13 and Part V.1, and Ontario Regulation 329/04, s. 6