Category:	Privacy	Policy Number:	EO-ADMIN-PY-001
Subject:	Privacy of Personal Information Policy	Date:	April 1, 2025
Issued By:	Privacy and Applications Manager	Revision Date:	
Approved By:	Chief Digital Officer	Page:	Page 1 of 17

NOTE: A printed copy of this document may not reflect the current, electronic version on EO intranet. Any copies appearing in paper form should always be checked against the electronic version prior to use.

PURPOSE

This policy outlines what ENHANCE Ontario (EO) and its agents must comply with under the Personal Health Information Protection Act (PHIPA).

POLICY STATEMENT

As a Health Information Network Provider (HINP), EO is committed to providing services to member hospitals that facilitate the secure electronic sharing of PHI between health information custodians and also support patients and families with a positive patient experience. PHIPA sets out rules that health information custodians (HIC) – (Member hospitals must follow when collecting, using, disclosing, retaining and disposing personal health information (PHI), and rules that Health Information Network Providers (ENHANCE ONTARIO) must follow when providing services to HICs operating within the province of Ontario, and to individuals and organizations that receive PHI from health information custodians.

EO recognizes that PHI is one of the most sensitive types of information for an individual and, as such, takes the protection of such information seriously by implementing safeguards to ensure the risk of inappropriate access or disclosure is reduced significantly. EO respects privacy as a fundamental patient right and recognizes that PHI belongs to the patient and that the hospitals are its custodian. We are committed to protecting the PHI that our member hospitals create or obtain about our patients. This policy applies to every person who works with PHI, including, but not limited to, directors, employees, volunteers, students, affiliates, privileged staff (physicians, dentists, midwives), researchers, contractors, sub-contractors and other agents. From here on, these individuals are referred to as “EO staff”.

DEFINITIONS

Agent: A person whom EO (HINP) authorizes to maintain and manage systems that include PHIs (Electronic health records).

Health Information Custodian (HIC): Persons or organizations described in PHIPA who have custody or control of PHI as a result of their work. For example, Scarborough Health Network is a health information custodian.

Health Information Network Provider (HINP): PHIPA describes a HINP as someone that provides services to two or more Health Information Custodians where the services are provided primarily to enable the Custodians to use electronic means to disclose Personal Health Information (PHI) to one another. For example, Enhance Ontario (EO) is a HINP. Reference: *s.10(4) of the Personal Health Information Protection Act (PHIPA) and ss.6(3) of Regulation 329/04*

Identifying information: Information that identifies an individual, alone or with other information.

Member Hospitals: The hospitals that are Members of ENHANCE Ontario: Campbellford Memorial Hospital, Haliburton Highlands Health Services, Lakeridge Health, Northumberland Hills Hospital, Peterborough Regional Health Centre, Ross Memorial Hospital, Scarborough Health Network. The Member Hospitals all utilize a single instance of Epic as the main electronic health record together with other regional digital assets

Personal Health Information (PHI): Identifying information about an individual (living or deceased) in oral or recorded form as it relates to, but is not limited to:

- Physical or mental health
- Provision of health care
- Plan of service
- Payment or eligibility for health care
- Donation of body parts or bodily substances
- Health card number or medical record number
- Substitute decision maker

Personal Health Information Protection Act (PHIPA): An Ontario health privacy law that establishes rules for the management of PHI and protection of the confidentiality of that information while facilitating the effective delivery of healthcare services.

Personal Information: Recorded information about an identifiable individual, including

information relating to the name, address, telephone number, age, race, national or ethnic origin, colour, religion, sex, sexual orientation, and marital or family status of the individual. This policy does not apply to personal information (PI) unrelated to a person's health. **Policy Breach**: Includes any non-compliance with this policy, other privacy-related policies, procedures and protocols, or with PHIPA.

Privacy Breach: A privacy breach occurs whenever a person has contravened a provision of PHIPA or its regulations. A breach occurs when information is stolen, lost or inappropriately accessed, used or disclosed without patient consent.

PROCEDURE

1.0 Accountability

EO is a Health Information Network Provider (HINP) that supports and maintains the health information systems where member hospitals collect, use, and disclose PHI's in its custody and control. As a HINP its responsibilities include:

- Managing changes in roles and responsibilities as they pertain to PHIPA and establishing appropriate agreements
- Assessing the privacy and security of the information system to help ensure that it protects personal health information
- Appointing one or more individuals who will be responsible for the privacy and security of the personal health information in the shared system
- Establishing logging, auditing and monitoring policies and procedures, including the communication of these controls to the participants
- Providing incident and breach management support to the participants by informing the parties in the event of a Privacy Breach or unauthorized access
- Making plain language safeguards available to both the public and participating organizations
- Completing a Privacy Impact Assessment (PIA) and Threat/Risk Assessment (TRA)

EO has designated a Chief Privacy Officer (CPO) as the contact person accountable for EO's compliance with this Policy along with the Privacy Officers from each member

hospital.

1.1 **Accountability:** Even though accountability for EO's compliance with this policy and with PHIPA rests with the CPO, other individuals within EO may be responsible for the day-to-day protection of personal information/personal health information. Every agent acting for, on behalf of, or for the benefit of EO must comply with this Policy.

1.2 **Responsibilities:** The Privacy Officer is an agent of EO and is authorized on behalf of the organization to work with the privacy contact of each of the member hospitals to:

a) facilitate the organization's compliance with this policy and with PHIPA generally;
b) ensure that all agents of the organization are appropriately informed of
c) their duties under this policy and with PHIPA generally;
d) respond to inquiries from the public about the EO's information and privacy practices;
e) respond to requests of an individual for access to or correction of a record of PHI about the individual that is in custody or under the control of the hospital; and
f) receive and respond to complaints from the public about the organization's alleged contravention of this policy and with PHIPA generally or its regulations.

1.3 **Public Record of Contact Person:** The identity of the CPO and the individual(s) designated by EO to oversee compliance with this policy and with PHIPA generally will be made known as a matter of public record in a written statement as detailed below. The CPO can be contacted via email at privacy@EO.ca, or by writing to ENHANCE Ontario, Attention Privacy Officer, 1371 Neilson Rd Suite 400B, Scarborough, ON M1B 4Z8.

1.4 **Openness:** ENHANCE Ontario will be open about their information practices concerning the management of PHI. Individuals can acquire information about the organization's policies and procedures without unreasonable effort. This information

will be made available in a generally understandable form.

1.5 Description of Information Practices: ENHANCE Ontario will provide a written statement to the public that will:

a. provide a description of the services and any directives, guidelines and policies of Service Provider that apply to the Services to the extent that the directives, guidelines and policies do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information, and a general description of the safeguards implemented by Service Provider to protect PHI and keep it confidential; and

b. describe how to contact the Privacy Officer
c. the Service Description
d. describes how to make a complaint to EO and the Information Privacy Commissioner.

1.6 Third Party Confidentiality Contracts: EO is responsible to ensure that any third party it retains to assist it in providing the Services agrees to comply (and require the compliance of its personnel) with the privacy and security obligations, restrictions and conditions necessary for Service Provider to comply with the Privacy Requirements.

2.0 Limiting Use, Disclosure, and Retention of Personal Health Information

Personal Health Information will not be used or disclosed by agents of EO Use or disclosure of PHIs will be limited to that reasonably necessary to meet the administrative purposes required by the agents of EO to perform their duties.

2.1 Need-to-know access: Individual access to PHI by agents of EO will be granted based on administrative duties assigned to this individual. Accessing patient information for any other purpose, including research, will be deemed a disclosure and requires approval in accordance with the policy on Access to and Disclosure of PHI.

2.2 Disclosures for Shared Electronic Health Record Systems: EO participates in

provincially approved shared **electronic health records (EHR)** and may securely share patients' PHI with other health care providers involved in their care through an EHR. Patients have the right to know what PHI has been sent to an EHR and which care providers may have accessed this information. Patients may withdraw their consent for provider access to EHR information at any time. In this case, patients would request from one of the member hospitals and EO would support the technical requirements to process the request.

3.0 Ensuring Accuracy of Personal Health Information

4.0 EO is to maintain Personal Health Information within the electronic health systems collected and used by member hospitals as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Ensuring Safeguards for Personal Health Information

Personal Health Information will be protected by reasonable security safeguards appropriate to the nature and format of the information being stored.

4.1 Scope of security: The security safeguards will protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification or disposal. EO will protect personal health information documented and stored within the electronic health systems it supports.

4.2 Appropriate Measures: The nature of the security safeguards will vary depending on the amount of information, distribution method, format, and method of information storage employed. Information will be safeguarded using measures appropriate to the personal health information involved.

4.3 Measures: The methods of protection will include:

a) Organizational measures: for example, limiting access to personal health information on a "need-to-know" basis;

b) Technological measures: for example, the use of passwords, system access controls and encryption where appropriate.

c) Regular audits of system access and use, including appropriate disciplinary action for non- compliance with legal or hospital requirements governing access to information.

4.4 Education and Awareness: EO will provide programs to educate and inform EO staff of the importance of maintaining the confidentiality of PHI and their respective responsibilities. Prior to the start of employment, the granting of hospital privileges or entering into any direct affiliation with the hospital, and on an annual basis thereafter, EO staff are required to:

a) Review EO's privacy policy and procedures.
b) Sign the Statement of Confidentiality (Appendix A)
c) Participate in mandatory privacy training
d) On a regular basis, EO Management will be provided with a list of staff who are non-compliant with privacy requirements (policy review, statement of confidentiality, sign-off and privacy training) for follow-up.

4.5 Handling, Disposal and Anonymization: EO would support record retention and disposal policies established in accordance with the Regulation enacted under the Ontario Public Hospitals Act (Reg. 965, s.20) and are reflected in the policy on Retention/Destruction of Records of member hospitals.

5.0 Privacy Incident Management:

It is prohibited and against the law to access patient data unless such access is required to perform duties assigned or sanctioned by EO. Anyone found accessing patient data outside these parameters has committed a serious breach of privacy and will be subject to disciplinary action. EO staff are also required to follow the correct procedure for accessing their record by completing an access request through the Health Information Management department in the relevant member hospital or accessing MyChart.

EO will ensure compliance with privacy policies and procedures through targeted and random audits of EO information practices and internal systems. The EO Privacy Office will reference legislation and privacy auditing best practices to conduct regular audits of our systems.

EO promotes transparency and encourages staff to report privacy and data protection

concerns, including suspected breaches of PHI and privacy policies and procedures, to the Privacy Office, in confidence, and assures that measures will be taken to ensure reporting personnel suffer no reprisals when suspected breaches are reported in good faith.

All suspected privacy incidents will be managed per EO's privacy breach management protocol.

6.0 Disciplinary Action

Any person who breaches this policy is subject to disciplinary actions, including suspension/deactivation of access to PHI and internal systems, termination of employment, contract termination and a report to their respective regulatory college, if applicable.

7.0 Challenging Compliance with EO's Privacy Policies and Practices

An individual will be able to address a challenge or complaint concerning compliance with the above principles to the Chief Privacy Officer.

1.7 The CPO is the initial point of contact for complaints and inquiries related to compliance with PHIPA at EO. If any individual has a question, concern or complaint about EO's compliance with privacy obligations under PHIPA, they can contact the EO's Privacy Office by email at privacy@EO.ca, or by mail at: **Attention: Privacy Office ENHANCE Ontario,** 1371 Neilson Rd Suite 400B, Scarborough, ON M1B 4Z8.

Inquiries and complaints may also be made to the Information and Privacy Commissioner of Ontario. The Commissioner is located at

2 Bloor Street East, Suite
1400, Toronto ON M4W
1A8.
Telephone: (416) 326-3333 or toll-free at 1 800
387-0073. Website: www.ipc.on.ca.

http://www.shn.ca/wp-content/uploads/SHN-Privacy-Brochure.pdfhttps://www.shn.ca/about-us/privacy/REFERENCES

Canadian Standards Association, (1994). *10 Fair Information Principles of the Canadian Standards Association Model Code for the Protection of Personal Information.*

Information and Privacy Commissioner of Ontario, (2004). *A Guide to the Personal Health Information Protection Act*

Information and Privacy Commissioner of Ontario, (2015). *Circle of Care Sharing Personal Health Information for Health-Care Purposes*

Ontario Statutes, (1996). *Health Care Consent Act (HCCA).*

Ontario Hospital Association, (2004). *Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act.*

Ontario Statutes, (2004). *Personal Health Information Protection Act.*

Adopted by the Sunnybrook Health Sciences Privacy and Security of Personal Health Information Policy

REVIEWED BY

APPROVED BY

_____ _____

Signature Date (dd/mm/yyyy)