Privacy Officer Role and Responsibilities: Ontario Electronic Health Record

The Privacy Officer at an organization using the Ontario Electronic Health Record (EHR) through either clinical viewer (ClinicalConnect or ConnectingOntario ClinicalViewer) is responsible for managing the organization's Privacy Program. In turn, the Privacy Program has the following responsibilities:

1. Compliance review and reporting
2. Managing patient consent
3. Responding to patient requests: record access and correction, inquiries and complaints
4. Managing responses to privacy breaches

The EHR Program Office supports certain tasks for both clinical viewers:

Clinical Viewer	Contact	
ClinicalConnect	ClinicalConnect Program Office	905 870 8270 ext. 9 privacy@clinicalconnect.ca
ConnectingOntario ClinicalViewer	Ontario Health, Digital Services Privacy Office	1 866 250 1554 OH-DS_privacyoperations@ontariohealth.ca

Four Components of a Privacy Program

The following items must be in place for the organization's Privacy Program prior to going live with use of the EHR:

1. **Privacy Contacts** • **Privacy Officer:** the lead for Privacy at the organization, responsible for compliance with the EHR Privacy Policies • Ontario Health identifies this individual from the Client Information Form signed by the Authorized Representative at the organization • To notify Ontario Health of a replacement Privacy Officer, send a written update to OH DS_agreements@ontariohealth.ca • **Privacy Officer Delegates:** individual(s) authorized to request and/or receive reports containing Personal Health Information (PHI). Identify this person(s) by sending written confirmation to OH-DS_privacyoperations@ontariohealth.ca	2. **Internal Privacy Policy and Procedures** • Enable the organization to address privacy requests and activities required by the EHR Privacy Policies. See the EHR Health Care Provider Guide
3. **Secure Method of Transmitting PHI to Ontario Health** • All email containing PHI sent to Ontario Health must be encrypted. Ontario Health always encrypts PHI files when circulated internally/externally • Alternatively, encryption and password protection (i.e., WinZip) is required for forms or reports being sent to Ontario Health	4. **Document Retention** • The organization must retain documents related to the EHR in accordance with the EHR Retention Policy

Privacy Program Responsibilities

1. Compliance Review and Reporting

• Ensure the organization, staff and electronic service providers (ESPs) are compliant with the EHR policies and procedures. This enables trust amongst participating organizations by confirming that each has implemented a comparable level of personal health information protection[3]

Reporting

- Prior to going live with the clinical viewer, ensure the organization complies with all of the EHR policies, procedures and standards detailed in *EHR Health Care Provider Guide*

Privacy Role-Based Training

- Ensure the organization's staff and ESPs complete appropriate training prior to Go Live and annually thereafter
- Ensure only authorized users are granted access to the EHR
  Notes:
    - If the organization performs research, include a check in the approvals process that Ontario's EHR systems may NOT be used for this purpose
    - Users accessing the EHR must accept the End User Agreement when logging in for the first time and annually thereafter

Reference: *EHR Health Care Provider Guide*, page 18

Auditing and Monitoring Access to Personal Health Information (PHI)

- Logging, auditing and monitoring all accesses to electronic records of PHI is important to ensure the privacy of patients and the confidentiality of their personal health information
- Audits are required on a quarterly basis at minimum to ensure the organization is proactive in preventing privacy breaches
- Auditing and monitoring is also expected if there is a <u>suspected</u> privacy breach

Reference: *EHR Health Care Provider Guide*, pages 18 to 19

2. **Managing Patient Consent**
- The organization may collect, use and disclose personal health information in the EHR for health care purposes with the patient's consent, which may be express or implied, according to the organization's practices
- The Privacy Officer must:
    - Ensure patients are knowledgeable by providing notices, brochures, updates on website and any other communication channels used (see the [Ontario Health website](#) for downloadable notices and brochures)
    - As referenced in the *Privacy and Security Training for Health Care Providers Using the Provincial Electronic Health Record* course, be prepared to discuss access concerns, implications of applying a consent directive, circumstances in which the record may be temporarily accessed, and process for modifying or removing a consent block
    - Conduct the activities required at the organization when informed of a consent override performed in the organization

Reference: *EHR Health Care Provider Guide*, pages 11 to 13

3. **Responding to Access and Correction Requests; Inquiries and Complaints**

Access Requests	Correction Requests
• As mentioned in the *Privacy and Security Training for Health Care Providers Using the Provincial Electronic Health Record* course, a patient may request the following: • Copies of their individual PHI available in the EHR • Report of who has viewed their PHI • Report of history of consent directives applied and removed • Report of consent directive overrides	• The organization may grant or refuse a correction request, in accordance with Section 55 of PHIPA • If the organization contributes to provincial or regional systems, corrections in the organization's information system are automatically uploaded into the provincial or regional systems • **Note:** If assistance is required in identifying organizations that collected the PHI, contact the EHR Program Office

Ontario Health

Access Requests	Correction Requests
• The nature of the PHI requested, and the Health Information Custodian responsible for that information, determine whom the patient must contact. Refer to the table below for details	• The scope of the request determines the organization that the patient must contact. Refer to the table below for details

Source	Contact
• PHI contributed only by the organization • **Note:** You may charge fees to fulfill access requests associated with EHR systems where your organization is required to provide a copy of the record	Privacy Officer
• PHI contributed by another organization • Audit report for ConnectingOntario or Diagnostic Imaging	Ontario Health Privacy Office 1 866 250 1554; OH-DS_privacyoperations@ontariohealth.ca
• PHI available in OLIS • Access report for OLIS	Ministry of Health, Freedom Of Information & Privacy Coordinator Access and Privacy Office 416 327 7040 generalapo@ontario.ca
• PHI or all reports for DHDR • Consent management-related reports for OLIS	Service Ontario 1 800 291 1405
• PHI in ClinicalConnect • All reports for ClinicalConnect	ClinicalConnect 905 870 8270, ext. 9; Privacy@clinicalconnect.ca

Reference: *EHR Health Care Provider Guide*, pages 15 to 16

Inquiries	Complaints
A privacy-related inquiry is a question raised in respect of: • When, how and the purposes for which PHI in the EHR is collected, used, disclosed, viewed, handled or otherwise dealt with • The administrative, technical and physical safeguards and practices maintained in respect of PHI in the EHR • The policies, procedures and practices implemented in respect of the EHR, and • Compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect of the EHR **Examples** • What is the EHR? • How is my information protected? • Who has access to the EHR and when can it be accessed? • What are my rights as a patient? The scope of the inquiry determines the organization that the patient must contact. Refer to the table below for details	• A privacy-related complaint is a concern raised in respect to compliance with PHIPA, applicable agreements and the policies, procedures and practices implemented in respect to the EHR **Examples** • Someone has accessed my record inappropriately • I was refused access to my PHI • I have not received a written consent directive confirmation • I do not believe my PHI is adequately protected The scope of the complaint determines the organization that the patient must contact. Refer to the table below for details

Ontario Health

Source	Contact
• The patient wants to know more about the organization's privacy and information practices, or • The patient wants to raise a concern about the organization's privacy and information practices	Privacy Officer
• The patient wants to know more about Ontario Health's privacy and/or information practices, or • The patient has questions related to ConnectingOntario or Diagnostic Imaging, or • The patient wants to raise a concern about Ontario Health's privacy or information practices	Ontario Health Privacy Office 1 866 250 1554; OH-DS_privacyoperations@ontariohealth.ca
• The patient wants to know more about OLIS, or • The patient wants to raise a concern about OLIS	Ministry of Health, Freedom Of Information & Privacy Coordinator Access and Privacy Office 416 327 7040; generalapo@ontario.ca
• The patient wants to know more about DHDR, or • The patient wants to raise a concern about DHDR	Service Ontario 1 800 291 1405
• The patient wants to know more about ClinicalConnect, or • The patient wants to raise a concern about ClinicalConnect	ClinicalConnect 905 870 8270, ext. 9; Privacy@clinicalconnect.ca

Reference: *EHR Health Care Provider Guide*, page 16

4. **Managing Privacy Breaches**
   - Prior to Go Live, identify the following for the organization:
     - Point of contact for reporting actual or suspected privacy breaches
       - The *Privacy and Security Training for Health Care Providers Using the Provincial Electronic Health Record* course references the organization's Privacy Officer as the point of contact. However, a delegate can be identified
     - Disciplinary procedures for staff responsible for a breach

Handling Real or Suspected Privacy Breaches
   - The specific steps to follow depend upon the organization that contributed the PHI subject to the breach:

PHI Contributed Only by Your Organization	PHI Contributed by Other Organizations
1. Report to the EHR Program Office 2. Contain, investigate, notify and remediate 3. Summarize	1. Report to the EHR Program Office 2. Contain 3. Notify 4. Investigate and identify remediation steps 5. Summarize 6. Remediate

Reference: *EHR Health Care Provider Guide*, pages 19 to 20

Ontario Health