# OCINet Participant Privacy Manual

Version 2.0

# Document Control

## *Document Version History*

| Version Number | Version Date | Summary of Changes | Changed By |
|---|---|---|---|
| 1.0 | Nov 6, 2025 | Version approved by PAC by email with revisions based on feedback during approval process on July 21, 2025. Board approved on Nov 6, 2025. | Darcelle Hall |
| 2.0 | Jan 30, 2026 | Privacy Assurance policy updated with PAC input from Nov 25, 2025 meeting and email follow-up; Board approved on Jan 30, 2026.<br>Edits to description of SW PACS solution in section 1 for clarity. | Darcelle Hall |
| | | | |
| | | | |
| | | | |

## *Document Owner(s)*

| Name | Position Title | Organization |
|---|---|---|
| Darcelle Hall | Manager, Privacy | OCINet |
| Shafique Shamji | President and CEO | OCINet |

# Contents

# Definitions and Acronyms

**Agent** – As per PHIPA section 17, an agent of a HIC may collect, use, disclose, retain or dispose of personal health information on the custodian's behalf.

**Clinical Imaging Data** -- Electronic images for diagnostic and other clinical purposes, and data associated with such images

**Corporation Service Provider** -- Service providers retained by the Corporation to assist it in providing the DIR or the services, including any subcontractors to such service providers

**DIR** – A shared repository for clinical imaging data.

**HIC** – Health Information Custodian as defined in PHIPA and O Reg 329/04

**HINP** – Health Information Network Provider as defined in PHIPA and O Reg 329/04

**New Participant Service Provider** -- A Participant Service Provider that OCINet has not previously authorized to process PHI for a particular type of service; provided that a like-for-like replacement of a prior Participant Service Provider that is a picture archiving and communication system provider or otherwise required for the Participant to be able to access OCINet's core services will not be considered a New Participant Service Provider.

**OCINet services** – As defined in OCINet Service Level Agreements, Services Agreements addressing OCINet core services, or other agreements executed between OCINet and individual participants for services outside of the core services.

**Originating Party** – As defined in the DSA Schedule B, is a Participant and HIC of PHI transferred to the DIR or to the Corporation (OCINet) for the services.

**Participant** – Has agreements in place with OCINet for OCINet Services and is either a public hospital that is a Member or a Health Provider that is not a Member (referred to in this document as health service providers).

**Participant Service Provider –** is a service provider (other than OCINet) retained by one or more Participant(s) as part of a Participant Service Provider Arrangement.

**PSP Arrangement** -- is a contractual arrangement between a Participant and a Participant Service Provider in connection with certain services, as set out in Section 4.1 of the DSA.

**PI –** Personal Information as defined in FIPPA.

**PHI** – Personal Health Information as defined in PHIPA.

**Receiving Party** – As defined in the DSA Schedule B, is a Participant and a HIC of PHI of which it is not the Originating Party the first time the Participant accesses, views or otherwise collects the PHI through the DIR or the services.

# Introduction

The OCINet Participant Privacy Manual (the Privacy Manual) is intended for the hospitals and health service providers that receive services from OCINet and who are OCINet Participants (Participants). The Manual has three parts:

- Part 1: A **Background** on OCINet services and summary of the material obligations and privacy laws that apply to OCINet and the Participants when collecting, using, disclosing, storing or retaining personal health information (PHI) or personal information (PI) in the custodianship of Participants for purposes associated with OCINet services.
- Part 2: **Shared Policies** that OCINet and the Participants are subject to in accordance with the OCINet Data Sharing Agreement (DSA) including any new or updated privacy requirements identified and approved over time.
- Part 3: **Support Materials** intended for use by OCINet and Participants in relation to the Shared Policies.

# Part 1: Background

Both OCINet and Participants are subject to Ontario's *Personal Health Information Protection Act*, 2004 (PHIPA) and the regulations thereunder along with the privacy and security obligations set out in agreements between OCINet and the Participants, including the *Second Amended and Restated Data Sharing Agreement* (OCINet DSA).

The OCINet DSA states that, in addition to complying with PHIPA and the OCINet DSA, OCINet and each Participant will comply with their respective obligations under policies established by OCINet and approved by OCINet's Board of Directors with respect to the privacy and security of PHI (Schedule B, section 2.2 of the OCINet DSA). These shared privacy policies that both OCINet and the Participants are subject to are set out in Part 2 of this Privacy Manual.

OCINet services are set out in agreements with each Participant. Not all services are consumed by, and/or available to, all OCINet Participants. The core services provided by OCINet include:

- Provision of the Diagnostic Imaging Repository (DIR) and related services that enable the storage and retrieval, transfer and/or viewing of clinical imaging data (i.e., clinical images and reports) for permitted purposes. Currently there are three regional DIRs: the Central East (CE DIR), Northeast (NE DIR) and Southwest (SW DIR).
- Provision of the Emergency Neuro Imaging Transfer System (ENITS), a service that provides timely access to urgent and emergent neurological, vascular, cardiac, and stroke images, as well as pediatric echo studies to specialized healthcare providers utilizing a dedicated repository and viewer.

- Provision of shared Picture Archiving and Communication Systems (PACS) used by OCINet Participants to capture, store, distribute, and display medical images for interpretation or review as part of the provision of health care services to patients.
- Provision of Speech Recognition Reporting Systems (SRRS) that are integrated with PACS to provide a comprehensive reporting solution that combines advanced speech recognition technology and integrated productivity tools for creation of high-quality diagnostic interpretations.

## Purposes for Collection, Use and Disclosure

OCINet provides Participants with a shared clinical imaging repository (DIR) and related or ancillary services for electronic clinical imaging data that enable them to collect PHI for the purposes of providing health care or assisting in the providing of health care and to subsequently use or disclose (or otherwise process) for purposes permitted by PHIPA or other applicable law, including any requirement for consent identified in PHIPA.

Where a Participant collects PHI for the purpose of providing or assisting of the provision of health care, the Participant may only subsequently process (i.e., use or disclose) PHI for purposes permitted by PHIPA or other applicable law.

Each OCINet Participant acknowledges that it has control of, and is responsible under PHIPA as a HIC for, PHI that the Participant transfers to and/or stores in OCINet clinical imaging systems (as an Originating Party), or that a Participant accesses and collects by means of the clinical imaging systems and subsequent processing of the PHI (as a Receiving Party) as it relates to OCINet services.

OCINet provides OCINet services as both a PHIPA Health Information Network Provider (HINP) and Agent and will not access, use, disclose or otherwise process for any purpose other than providing the DIR and other OCINet services, or as permitted or required by applicable law.

Both OCINet and the OCINet Participants commit to limiting the amount of PHI collected or used to that necessary for the applicable purposes. OCINet further commits to limiting the amount of PHI and the persons requiring access to PHI to the least amount required to provide the services, and to protect the PHI using strong safeguards.

*Please note: Part I of the Manual is intended to provide an overview of certain key obligations applicable to OCINet and the Participants set out in the OCINet DSA for informational purposes only. This section is not intended to be construed as legal advice and should not be considered an amendment or waiver of any of OCINet's rights under the OCINet DSA. Participants should review and obtain independent legal advice on how the OCINet DSA applies to their organization. The OCINet DSA, and PHIPA as applicable, set out the permitted purposes of collection, use and disclosure of PHI and the associated obligations of both OCINet and OCINet Participants relating thereto. Part I of the Manual does not introduce any new obligation on OCINet or any Participant. In the event of any conflict between the summary information in Part I of the Manual and PHIPA or the OCINet DSA, PHIPA or the OCINet DSA, as applicable, prevails.*

# OCINet and Participant Privacy Roles

## OCINet Privacy Roles When Providing Services

The DSA identifies OCINet as a Health Information Network Provider (HINP) and Agent under PHIPA and the regulations thereunder. OCINet's Corporate Privacy Policy describes the organization's obligations under PHIPA and its agreements with OCINet Participants for the personal health information (PHI) or personal information (PI) that it uses to provide the OCINet services and how they will be met through the OCINet privacy governance structure and privacy program including its privacy policies and procedures.

OCINet acts as a HINP when providing the technology services that enable disclosure of PHI among two or more HICs. OCINet acts as an Agent of each Participant where it uses PHI in the custody of the Participant, on their behalf, for permitted purposes associated with OCINet services as defined in the Service Level Agreement and Services Agreements including the operational activities associated with establishing and maintaining connectivity between Participant and OCINet systems and various data management activities associated with the clinical imaging data.

OCINet may also provide other services as Agent when directed in writing by a Participant including, but not limited to, use of PHI in order to enable transfer or sharing of clinical imaging data with a data recipient or other third party on behalf of the Participant including but not limited to:

- Transferring imaging data to Ontario Health for Diagnostic Imaging Common Services (DI CS)
- Transferring imaging data to OntarioMD for Health Report Manager
- Transferring imaging data to PocketHealth users upon request and on behalf of Participants who have contracted with PocketHealth for release of information services (only in the CE region)
- Enabling Participants to transfer clinical imaging data to, or receive clinical imaging data from, a contracted radiology reading services provider who is an Agent of the Participant when providing radiology reading services involving collection, use or disclosure of PHI. This PSP arrangement requires connectivity to the system of the provider for this purpose and is only available to users of OCINet SW Agfa EI Shared PACS service.

These other services are subject to separate agreements with OCINet but are still subject to the terms of the DSA.

## OCINet Participant Privacy Roles When Receiving Services

The OCINet Second Amended and Restated Data Sharing Agreement identifies OCINet Participants as Health Information Custodians under PHIPA and the regulations thereunder. Some OCINet Participants are also Institutions under FIPPA. As such, OCINet Participants have obligations that include a requirement to have adequate information practices in place that include privacy and security processes, policies and procedures, training and a privacy contact who is responsible for ensuring these practices are in place.

The Shared Policies in the next section of this document will provide more information on the privacy obligations and expected responsibilities of OCINet and the Participants.

# Part 2: Shared Policies

The Shared Policies are not intended to replace the corporate privacy policies, processes or training activities of OCINet or OCINet Participants where each organization is required to have its own policies, processes or training activities to meet their privacy obligations under PHIPA, other applicable laws, or obligations established through agreements including the OCINet DSA.

The OCINet Shared Policies are intended to:

- Confirm the roles and responsibilities of OCINet and OCINet Participants as it pertains to how they will meet certain privacy obligations, manage privacy risks and demonstrate compliance in relation to OCINet Services.
- Provide guidance on where privacy operations and privacy-related practices should be aligned to support timely communication, collaboration and privacy compliance
- Define expectations for how OCINet Participants as HICs can meet the same obligations and standards for privacy in order to reinforce mutual trust amongst Participants
- Define expectations for how OCINet will support Participants by demonstrating compliance with its obligations and support Participants in meeting their obligations.

## 1. Privacy Assurance Policy

| | |
|---|---|
| **Version:** | 2 |
| **Last Updated/Approved Date:** | January 30, 2026 |
| **Next Review Date:** | November 2028 |

### Purpose

This Shared Privacy Policy describes the mechanisms in place to monitor and reinforce compliance with the privacy obligations established in OCINet agreements and further elaborated in OCINet's Shared Privacy Policies. The policy will enable communication and transparency on OCINet and Participant privacy practices and provide confidence in OCINet and Participant privacy practices as they support both compliance and protection of PHI in OCINet systems.

The Shared Privacy Policies are intended to align with the privacy obligations identified in Ontario's Personal Health Information Act, 2004 (PHIPA) for health information custodians (HICs), agents and persons who provide services to HIC to enable them to collection, use and disclose PHI, and associated Regulations.

## Scope

This policy is applicable to OCINet Participants who have executed an OCINet Data Sharing Agreement and to OCINet as a Health Information Network Provider and Agent of the Participants.

## Roles and Responsibilities

Participant Privacy Policies are developed and updated by the OCINet Privacy Office with input from the OCINet Privacy Advisory Committee (PAC).

PAC approval of the Participant Privacy Policies is a precursor to OCINet Board approval.

## Policy Statements

**Privacy Oversight and Advisory**

- OCINet's Privacy Office Chairs the Privacy Advisory Committee (PAC) which provides a forum for Participants to receive updates and information on privacy matters, to advise OCINet on HIC obligations as they pertain to OCINet services and privacy functions, and to address changes or issues arising from a privacy perspective. The role and function of the PAC including the creation of Working Groups and the issue escalation path is documented in the *Privacy Advisory Committee Terms of Reference*
- OCINet will consult with the PAC for any updates to the Privacy Manual and Shared Policies to address new privacy requirements or changes to OCINet systems or services impacting privacy.
- OCINet will provide the PAC with an annual privacy report at the Fall PAC meeting. The report will also be made available to all participants outside of the PAC.

**Participant Privacy Attestations**

- OCINet will provide new Participants with a privacy attestation to be completed, reviewed and accepted by OCINet before a new Participant can be connected to OCINet systems. The attestation will require Participants to verify their privacy practices, processes and documentation required to comply with the OCINet DSA and Shared Policies including compliance with PHIPA, although the attestation is not intended to evaluate overall compliance with PHIPA obligations where this is the responsibility of each Participant as a HIC.
- OCINet will meet with the new Participant to review any issues or gaps identified in the attestation including the Participant's plan to remediate gaps in a reasonable timeframe. Any substantive gaps identified that cannot be remediated in a reasonable timeframe may delay connecting to OCINet systems.

- OCINet will establish an annual privacy re-attestation and information update process for existing Participants to validate compliance with privacy obligations in agreements and policies the Participant is subject to, and to ensure that participant privacy contact information and Integrated Community Health Service Centre (ICHSC) business information is up to date. OCINet will work with each Participant to review any gaps identified in the attestation including establishing a plan for remediation in a reasonable timeframe.

**Privacy Accountability Mechanisms**

- Participants will provide and keep up to date the contact information for the privacy contact responsible for addressing privacy matters associated with OCINet systems and services and providing any other privacy designate contact information.
- ICHSC Participants will review, verify and/or update business information for their facilities and/or locations as part of the annual re-attestation process; however, information on business or facility changes should be communicated to OCINet no later than 30 days after the date of such change.
- OCINet and the Participants are responsible for their Agents including staff and any third parties that may collect, use, disclose, retain or otherwise process PHI/PI on their behalf. As such, each party should establish an agreement with its Agents that addresses confidentiality and includes acknowledgement of the user's role in following the participant's privacy policies and procedures in compliance with PHIPA as it pertains to systems and services where the hospital authorizes user access to PHI that would be inclusive of OCINet systems and services.

## Related Documents

OCINet Corporate Privacy Policy

OCINet Participant Privacy Manual

OCINet New Participant Privacy Attestation Form

OCINet Participant Privacy Re-Attestation Form

## Related Legislation or Regulatory Requirements

Personal Health Information Protection Act, 2004

Ontario Regulation 329/04

# 2. Access and Corrections Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy defines how individual requests for access to, or correction of, PHI contributed to OCINet systems will be handled when received by OCINet or Participants, and any supports to be provided by OCINet or Participants to facilitate response to an individual's request.

**Access and Correction Requests Received by Participants**

- Where a request relates to PHI in OCINet systems contributed by your organization, process and respond to the request using the privacy access and corrections policies and procedures in place in your organization.
- Where a request relates to PHI contributed by another Participant, direct the individual to contact the contributing Participant where the Participant can be identified. If unknown, direct the person to contact OCINet at privacy@ocinet.ca for follow-up within 72 hours, or three business days.
- If the request involves access or correction requests for imaging contributed by more than one other Participant, the Participant who receives the request should direct the individual to contact each of the Participant organization(s) separately. Where the Participant organization(s) are unknown, a participant may contact OCINet at privacy@ocinet.ca for support in directing the individual to the appropriate Participant(s) within 72 hours, or three business days of receiving the request from the individual.
- Where a participant receives an access request pertaining to Ontario Health's DI CS or Clinical Connect, the Participant should direct the individual to the appropriate information and/or contact at these organizations.

**Access and Correction Requests Received by OCINet**

- Where OCINet receives a written access or correction request from an individual for PHI contributed by a single Participant, OCINet will direct the individual's request to the Participant's Privacy Contact or designate within 72 hours, or three business days.
- Where OCINet receives a request to support redirection of an access or correction request from a Participant, OCINet will provide supporting information related to the contributor(s) of the PHI to the requesting Participant. OCINet will respond to the Participant's request within 72 hours, or three business days.

# 3. Privacy Inquiries and Complaints Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy defines how privacy inquiries or complaints pertaining to PHI in OCINet systems will be handled when received by OCINet or Participants, along with any supports to be provided by OCINet or Participants to facilitate response to an individual's privacy inquiry or complaint.

**Privacy Inquiries or Complaints Received by Participants**

- Where a privacy inquiry or complaint received by a Participant relates to PHI in OCINet systems contributed by your organization, respond using the privacy inquiry and complaint policies and procedures in place in your organization. Where information on OCINet systems or services is required, contact the OCINet Privacy Office for support at privacy@ocinet.ca. OCINet will follow up with your organization within 72 hours, or 3 business days to confirm information to be provided.
- Where an inquiry or complaint relates to PHI contributed by another identifiable Participant, direct the individual to contact the Participant. If the Participant is unknown, direct the person to contact OCINet at privacy@ocinet.ca. OCINet will follow- p with the individual within 72 hours, or 3 business days to support identification of the appropriate Participant(s).
- If the inquiry or complaint involves other OCINet participants and/or OCINet the Participant who receives the inquiry or complaint should submit an *OCINet Privacy Inquiries and Complaints Notification Form* to the OCINet privacy office at privacy@ocinet.ca within 72 hours, or three business days of receipt of the inquiry or complaint, to enable OCINet to distribute to Participants and support coordination of the response. It is anticipated that the recipient of the inquiry or complaint will take the lead in providing the response but this can be confirmed by the Participants involved.
- Where a Participant receives an inquiry or complaint specific to Ontario Health's DI CS or Clinical Connect, the Participant should direct the individual to the appropriate information and/or contact at these organizations.

**Privacy Inquiries and Complaints Received by OCINet**

- Where OCINet receives a privacy inquiry or complaint that is general to how OCINet handles personal health information when providing services, OCINet will respond directly to the individual within 72 hours, or three business days, and complete its response within 30 days.
- Where OCINet receives a privacy inquiry or complaint pertaining to an individual's concern about PHI involving a single Participant, OCINet will direct the individual to the Participant's

Privacy Contact or designate for privacy inquiries or complaints, including forwarding any written request received, within 72 hours, or 3 business days.

- Where OCINet receives a request from an individual or a Participant about an inquiry or complaint involving multiple participant(s), OCINet will document the details and forward a *OCINet Privacy Inquiries and Complaints Notification Form* to the impacted participants within 72 hours, or 3 business days of receipt of the inquiry or complaint.
- Impacted Participants and OCINet will work together to investigate and respond to the inquiry or complaint, and to identify the Lead Organization responsible for responding to the individual. The lead organization will ensure that the inquiry or complaint is addressed within 30 days, and in a manner that meets each organization's PHIPA obligations. OCINet and Impacted Participants will support this effort in a timely fashion. Where additional time is required to address the inquiry or complaint an extension of 30 days may be used, as permitted by PHIPA.

# 4. Privacy Breach Management Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

Defines how suspected or actual privacy breaches involving PHI that is lost, stolen or subject to unauthorized collection, use, disclosure, retention or destruction in OCINet systems will be handled where identified by OCINet or Participant(s), including any supports to be provided by OCINet and/or Participants to enable identification, reporting, containment, notification, investigation and remediation of privacy breaches in a timely fashion.

Where OCINet or a Participant suspects, or is aware of, an incident that may result in a privacy breach originating from their organization involving PHI in OCINet systems, they should follow their own privacy breach management policies and procedures and this policy that outlines roles and responsibilities of OCINet and the Participants for how they will work together where required.

**Privacy Incident or Breach Identification**

- Participants may require support from OCINet to identify an actual or suspected privacy breach originating from their organization. Participants should contact privacy@ocinet.ca to request any immediate support, ensuring that their privacy office is engaged at the same time.
- Where participants suspect a security incident or breach, they should contact their regional OCINet helpdesk as soon as possible using the following contact information:

  NE: 1-866-804-4623, helpdesk@neodin.ca

  SW: 1-519-685-8500 x 44357, Toll Free 1-877-465-7167, helpdesk@lhsc.on.ca

  CE: 1-800-387-9525, hdirs-servicedesk@shn.ca

- OCINet or the Participant from whom the suspected or actual breach originated may require support from other Participants to identify the full scope of a privacy breach involving PHI in OCINet systems. The *OCINet Privacy Incident Notification Form* should be completed and submitted to OCINet privacy@ocinet.ca along with a request for support with identification, containment, investigation or remediation.

**Management and Reporting of a Multi-HIC Privacy Breach**

- Where a Participant suspects or identifies a suspected or actual privacy breach impacting more than one Participant, the *OCINet Privacy Incident Notification Form* should be completed and sent to OCINet as soon as is reasonably possible, or within 48 hours of receipt.
- For a suspected or actual privacy breach impacting one or more OCINet Participants, OCINet will send the completed *OCINet Privacy Incident Notification Form* to the Privacy Contact or designate for impacted Participants as soon as reasonably possible or within 48 hours or two business days of receipt of the form from a participant, or on its own behalf where required.
- The Participant who caused the breach will become the Lead Organization for managing the breach; however, all impacted Participants and OCINet are expected to assist and be engaged in the breach management process including IPC and patient notification.
- The Lead Organization (either a Participant or OCINet) will be responsible for:
    - Leading the breach management process
    - Providing updates on the progress of investigation, containment and remediation activities including upon request
    - Coordinating with impacted Participants on the plan for, and content of notification of the IPC and individual(s) to whom the PHI relates. This may include notification of the IPC by either the Impacted Participants or OCINet as determined by the Participants.
    - Completing and submitting an *OCINet Privacy Breach Report Form* to be circulated by OCINet to impacted participants
    - Notifying any other regional or provincial systems where required (e.g., Ontario Health for DI CS, Clinical Connect.
    - Where OCINet is the Lead Organization they will follow contractual obligations, the OCINet privacy breach management procedure, and this policy regarding notification of Participants and collaboration on breach management.

**Containment**

- Where OCINet or Impacted Participants are able to undertake activities to prevent any further collection, use or disclosure of PHI resulting from a privacy breach they should be directed to do so as soon as is reasonably possible by the Lead Organization in collaboration with OCINet, and report the result back when complete, including providing any supporting documentation to inform the privacy breach report.

**Investigation and Remediation**

- OCINet and the Participants should follow their own breach management policy and procedures for privacy breach investigation and remediation for breaches originating from their organization.
- OCINet or Participants impacted in a Multi-HIC Privacy Breach should support the Lead Organization with any privacy investigation and remediation activities as required and appropriate including providing any supporting documentation to inform notification and the privacy breach report.

- The Lead Organization should confirm the breach-related contact at each organization and establish a mutually agreed-upon schedule for updates during the investigation and remediation phase up until the final Breach Report is issued.

**Individual Notification**

- The Lead Organization for a multi-HIC Privacy Breach should consult with OCINet and the impacted participants on responsibility for patient notification, the contents of the notification communication to individual(s) whose PHI was breached, and the timing for sending the notification.

# 5. Consent and Support for Consent Management Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy clarifies that Participants may only contribute PHI to OCINet systems where they have consent for the permitted purposes as defined in the OCINet DSA.

This policy also defines how Participants can support individuals to withdraw or reinstate their consent for the collection, use or disclosure of PHI contributed to OCINet systems where this is supported, and the options available in OCINet systems to override consent directives as permitted by PHIPA.

*Please note:* OCINet system consent directive functionality is under review and may be updated. Where this occurs, the policy will be updated.

**General Statements**

- Participants should follow their own consent directive policies and procedures for receiving and responding to a consent directive request involving OCINet systems including informing individuals of the options and risks associated with withdrawing consent for collection, use or disclosure of PHI in OCINet systems where this functionality is available. OCINet will provide Participants with supporting information on this functionality.
- OCINet systems have limited functionality to support application of a “lock-box” to patient records or support for “override” of a lockbox as it pertains to patient withdrawal of consent for collection, use or disclosure of PHI. See table in Appendix A for more details.
- Available support for consent management in OCINet systems is described below. Participants can contact the OCINet privacy office for more information on consent management functionality and any related support materials including forms where applicable.
- Where a Participant receives a consent withdrawal request from an individual for PHI they did not contribute to OCINet systems, they should direct the individual to the appropriate Participant if known. Where unknown, the Participant should forward the individual’s request to the OCINet privacy office for redirection to the appropriate Participant by OCINet within 72 hours, or three business days.
- Where OCINet receives a consent withdrawal request directly from an individual, the Privacy Office will redirect the individual to the privacy office of the Participant(s) who contributed the PHI within 72 hours, or three business days.
- Where OCINet transfers diagnostic imaging data or links to imaging data in OCINet repositories to Ontario Health for DI CS as directed by participants who hold a Provincial EHR Contributor Agreement with Ontario Health, Ontario Health expects to receive all imaging data inclusive of imaging data subject to a consent directive. If an individual wishes to withdraw consent for

collection, use or disclosure of their imaging data available through the Provincial EHR, they can submit a request directly through Ontario Health.

- Participants are responsible for advising individuals on the consent withdrawal processes involving their imaging data in Ontario Health's DI CS system and Provincial EHR.

**Adding or Modifying a Consent Directive in OCINet Diagnostic Imaging Repositories**

*Central East Diagnostic Imaging Repository (CE DIR)*

The Privacy Contact or designate can submit a request to OCINet to add or remove a consent directive on individual patient studies in the using the *OCINet Consent Directive Request Form*, also available from the OCINet privacy office (i.e., for a specific study accession number inclusive of study images and radiology report).

The Privacy Contact or designate can contact privacy@ocinet.ca to receive a link to a secure folder that can be used to upload the form or send to OCINet using other approved secure means.

OCINet will process the request and notify the participant when the addition or removal is complete within 72 hours, or three business days.

*Southwest Diagnostic Imaging Repository (SW DIR)*

The Privacy Contact or designate can submit a request to OCINet to add or remove a consent directive on individual patient studies in the using the *OCINet Consent Directive Request Form*, also available from the OCINet privacy office (i.e., for a specific study accession number inclusive of study images and radiology report).

The Privacy Contact or designate can contact privacy@ocinet.ca to receive a link to a secure folder that can be used to upload the form or send to OCINet using other approved secure means.

OCINet will process the request and notify the participant when the addition or removal is complete within 72 hours, or three business days.

*Northeast Diagnostic Imaging Repository (NE DIR)*

There is no method available to apply a consent directive to patient studies in the NE DIR.

**Adding or Modifying a Consent Directive in an OCINet PACS System**

*Southwest Agfa EI (SW Agfa EI Shared PACS)*

Authorized users of the PACS Desktop Application can activate "VIP Status" for a patient to block access to all patient imaging data. The block is applied at the patient level and removes access to all patient study information. Authorized users of the PACS Desktop Application can activate "Emergency Override" to access VIP patient imaging data during their active session.

The Privacy Contact or designate can contact privacy@ocinet.ca to request a report of consent directives overrides and related privacy audit of access to PHI. See detail in the Privacy Audit Policy.

Contact OCINet for an Information Sheet with more detailed information on consent directive functionality in this system and how its use will be managed between contributing and receiving HICs.

### Adding or Modifying a Consent Directive in the OCINet ENITS System

Where a participant that contributes studies to ENITS directly from imaging modalities wants to prevent a study from being available to users of ENITS they will need to work with their medical imaging team to manually intervene in the image sending process in advance of the imaging being conducted for a specified patient receiving imaging. Alternatively, the participant can contact the SW helpdesk at helpdesk@lhsc.on.ca to request that a patient's imaging be removed for consent-related purposes.

### Appendix A: OCINet System Consent Management Capabilities

| | |
|---|---|
| **Diagnostic Imaging Repositories** | **CE DIR**<br>• The current CE DIR supports placement of consent blocks at the individual study level only. Access to specified study data including patient demographics, images and the radiology report is blocked in the CE Xero Viewer and withheld from disclosure via OCINet's FEM service. There is no indication that studies have been suppressed and no option for override of the consent block.<br>• Blocked studies remain available to the contributing participant via their local PACS and CE DIR administrator tools.<br>• Where OCINet sends a copy of an Ontario Health Contributor's study reports and study imaging links to Ontario Health for DI CS, copies of all studies including those with consent blocks in place will be sent and will be available via the Provincial EHR; however, the image links will not be active. Patients must submit a request directly to Ontario Health to have consent directives applied to their studies available through the provincial EHR.<br><br>**SW DIR**<br>• The current SW DIR supports placement of consent blocks at the study level with no option for override through the solution. A notification message specific to each blocked study provides the name and contact information for the contributing participant to enable a clinician to follow up for access. Such access would be handled by the participant in accordance with their policies and would not involve the DIR.<br>• Studies cannot be identified or accessed via GE OneView or retrieved via Foreign Exam Management in participant PACS systems.<br>• Where OCINet sends a copy of an Ontario Health Contributor's study reports and study imaging links to Ontario Health for DI CS and a copy of study imaging |

| | |
|---|---|
| | links to Clinical Connect, copies of all studies including those with consent blocks in place will be sent and will be available via the Provincial EHR; however, the image links will not be active. Patients must submit a request directly to Ontario Health to have consent directives applied to their studies available through the provincial EHR.<br>• Technical limitations of participant PACS systems may prevent modification or removal of consent blocks placed on studies in the SW DIR.<br><br>**NE DIR**<br>• The current NE DIR currently has no support for placement of a consent block or override. |
| **PACS Services** | • OCINet's Agfa EI PACS supports placement of consent blocks at the patient level with option for user override for authorized reasons. More specific information on this functionality, how it is managed, and related reporting is available from the OCINet Privacy Office.<br>• OCINet's Optum PACS supports placement of consent blocks at the study level with an option for the user to override. The system logs the override action.<br>• For both OCINet PACS systems, consent blocks involve a global setting and will apply to all participant users in the shared system. |
| **ENITS** | • The ENITS viewer has no support for consent management. Study data is retained in ENITS for up to 14 days to support emergency consults with remote specialists.<br>• Participants can elect not to send study data to the ENITS system by preventing the study from transferring out from the modality automatically. The processes for doing this are unique to each Participant and their medical imaging department.<br>• Where imaging has been transferred to ENITS and it is identified that the information is subject to consent withdrawal after the fact, the participant can request that the study data be deleted by submitting a request to the ENITS helpdesk who will engage OCINet privacy in handling the request. |

# 6. Privacy Auditing Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy defines how OCINet will support Participants by providing them with privacy audits that address both access to PHI and transfer of PHI as required or requested, and how Participants will support each other with privacy auditing of their clinical systems used to collect PHI from OCINet systems.

**General Statements**

- OCINet will provide electronic records of access to, or transfers of, PHI for systems and equipment it controls as requested by participants, or as scheduled, using OCINet's privacy auditing procedures.
- Participants can use the *OCINet Privacy Audit Request Form* to request a privacy audit of access to PHI or transfer of PHI for systems where OCINet controls the logs and auditing capability.
- OCINet systems subject to requested or scheduled privacy auditing are those that enable participant users to contribute, access, retrieve or disclose PHI. Other OCINet systems used to store and process PHI in relation to OCINet services that *do not* directly facilitate participant users to contribute, retrieve or disclose PHI will be audited by OCINet as required or requested, along with other privacy auditing of OCINet staff access to PHI in any system. See system list in appendix for more information.
- OCINet will work with the Privacy Advisory Committee (PAC) to develop and implement a schedule of privacy audits to be provided by OCINet to each participant to enable them to monitor for, or detect, unauthorized viewing of electronic records, theft, loss, unauthorized copying, modification, or disposal of information that can be reasonably supported by its technology systems.
- Scheduled audits will be distributed by OCINet to each participant. Each participant is responsible for reviewing the audit reports and following up on any actual or suspected unauthorized collection, use, disclosure, or disposal of PHI including viewing of electronic records, theft, loss, unauthorized copying, or modification of information.
- In some instances involving unauthorized collection, use, disclosure, or disposal of PHI including unauthorized viewing of electronic records, theft, loss, unauthorized copying, or modification of information, participants may require privacy auditing support of other participants whose participant systems were used to retrieve and/or store PHI of the originating party. Participants will support these requests in a timely fashion as part of the privacy breach management process. The lead organization for the privacy breach investigation will request these audits with support from OCINet where required.

**Participant Requests for Privacy Audits**

- Participants will use the *OCINet Privacy Audit Request Form* to submit requests for audit to the OCINet privacy office using secure means. Participants should indicate the priority level for requests, for example, where required to validate a suspected privacy breach.
- OCINet will acknowledge receipt and request any clarifications within 48 hours of receipt of the request and deliver the requested audit report within 48 hours after acknowledgement or clarification. Where a priority audit is required OCINet will return the report as early as is reasonably possible.
- Participants who use the SW Agfa EI Shared PACS system may submit requests pertaining to override of consent blocks in place and any associated Privacy Audit of access to PHI associated with access to PHI during the override period. These requests can be submitted using the *OCINet Privacy Audit Request Form* using secure means.

**OCINet Distribution of Scheduled Audits**

- *This process will be defined in future.*

**Appendix: OCINet System Auditing Details**

*Indicates most commonly requested systems for privacy audits, including access to PHI or transfer audits that enable the highest volume of access to PHI by participant users.

| OCINet Systems | Participant Users | OCINet Users | Notes |
|---|---|---|---|
| DIR Clinical Viewers* | X | X | NE/SW DIRs: GE OneView Viewers<br>CE DIr: Agfa Xero Viewer |
| Other DIR Applications | X<br>(CE Admin Console only) | X | OCINet DIR Admin Consoles<br>Interlinx and other brokers used to support the OCINet FEM Service (transfers only)*<br>OCINet Interface Engines |
| ENITS | X | X | |
| SW Agfa EI Shared PACS * | X | X | |
| CE Shared PACS (Optum) | N/A | N/A | Audits through system or on request from vendor |
| SRRS – Speech Recognition | X | X | |
| CE PocketHealth* | N/A | N/A | Transfer audits only |
| OCINet M365 Suite | N/A | X | |
| OCINet HelpDesk Systems | N/A | X | |

# 7. Privacy Training Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy defines expectations for the scope of privacy training content, the delivery of training and the tracking of training delivery by OCINet and the Participants.

**Expectations for Training Content**

Where OCINet and OCINet Participants are responsible for providing privacy training to their agents that is applicable to the use of OCINet clinical imaging systems, the privacy training or related privacy awareness materials should have content that address the following privacy expectations:

| | |
|---|---|
| **Appropriate Limiting of Collection, Use and Disclosure of PHI with OCINet Systems or accessed via OCINet Services** | • Agents of the Participant are subject to their own organization's privacy policies and procedures when using OCINet systems for permitted purposes<br>• Agents should only access PHI for the permitted purposes and only as much PHI as is reasonable required for the purpose<br>• Agents should ensure they have the required authority to collect, use or disclose PHI using OCINet systems |

OCINet will provide Participants with privacy awareness content for OCINet systems that can be used in conjunction with Participant training, targeted for users of OCINet systems where it is understood that Participant privacy training does not address the unique requirements of provincial or regional systems specifically.

The privacy awareness content will also address approved methods for Secure Sharing of PHI with OCINet and OCINet Participants, along with other guidelines to be provided by OCINet.

**Expectations for Training Delivery**

Where OCINet and OCINet Participants are responsible for delivering privacy training to their agents, agents should receive privacy training in advance of gaining access to OCINet systems and annually thereafter as a refresh to their privacy training.

OCINet and OCINet Participants should log and maintain records of when their agents received privacy training and be able to produce such logs were they to be subject to audit of compliance with the OCINet DSA.

# 8. Privacy Considerations for Access Management Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy defines how OCINet and the Participants will work together to ensure that reviews of active Participant users, including their assigned user role(s), are regularly conducted and the results acted upon, including each Participant's responsibility to contact OCINet to suspend or de-activate user accounts when required.

**Participant Review of User Accounts Provisioned by OCINet**

Where a Participant identifies an authorized user whose access has been suspended or terminated by their organization, they will notify their OCINet helpdesk as soon as is reasonably possible to ensure the user can be deprovisioned in a timely manner. Where suspension or termination is related to a security or privacy incident or breach, OCINet should be made aware of this circumstance.

Where OCINet provisions Participant authorized users with accounts for OCINet systems, OCINet will provide each Participant with a list of provisioned users to review and confirm on an annual basis. The list will identify the role(s) held by each user. Each Participant should notify OCINet of any required modifications to user roles or deprovisioning of user accounts as soon as is reasonably possible.

**Participant Review of User Accounts Provisioned by Participants**

Where a Participant provisions OCINet system accounts for authorized users in their organization, the Participant is responsible for regularly reviewing the status of active user accounts to identify accounts that should be modified or deprovisioned.

Participants are responsible for suspending or deprovisioning authorized user accounts in OCINet systems as required where a user's accounts have been suspended or terminated in other Participant systems.

# 9. Privacy Considerations for Information Handling Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Scope and Purpose**

This policy establishes expectations for secure handling of PHI for privacy-related communications with OCINet or among Participants and addresses retention periods for key data types associated with privacy compliance.

**Electronic Means for Sharing PHI**

OCINet and OCINet Participants will limit sharing PHI by email to only the agreed-upon identifiers required to support an operational issue. Otherwise, OCINet and the OCINet Participants should not email or message PHI.

OCINet and OCINet Participants will use the OCINet-approved means for secure sharing of electronic files containing PHI. Where a Participant has technical limitations that prevent use of such means, Participants may share documents using a mutually agreed-upon method of file encryption. See the Guideline for Secure Sharing of PHI in Appendix B.

**Retention and Disposal**

OCINet has a corporate retention policy and schedule that pertains to the PHI or PI of OCINet Participants. Where OCINet and OCINet Participants have their own retention policies and schedules, the following retention expectations apply to PHI and other information associated with OCINet services:

| Record Type | Minimum Retention Period |
|---|---|
| Logs required to conduct Access to PHI audits for Participant systems connected to the OCINet DIR that enable authorized user access to imaging data (e.g., PACS). | As directed by PHIPA, or as technically possible by participant system. |
| Information collected by an organization to respond to individual related to their:<br>• Access or Correction requests under PHIPA<br>• Requests to make, modify or withdraw a Consent Directive under PHIPA<br>• Inquiries or Complaints under PHIPA | 2 years after the Access or Correction or Consent Directive Request has been closed<br>2 years after a Complaint has been closed by the participant, OCINet, and/or the IPC |

| | |
|---|---|
| Information created about an individual as part of an investigation of a Privacy Breach and/or Security Incident. | 2 years after the Privacy Breach or Security Incident has been Closed by the participant, OCINet, and/or the IPC |
| End user credential information where the Participant is an identity provider | Permanent |
| Information collected for provider identification or registration that contains PI | 7 years after last use |
| Assurance-related documents | 10 years |

# 10. Privacy Risk Management Policy

| | |
|---|---|
| **Version:** | 1.0 |
| **Last Updated/Approved Date:** | November 6, 2026 |
| **Next Review Date:** | November 2028 |

**Purpose and Scope**

This policy describes how OCINet will share information on its privacy risk management to ensure compliance with its privacy obligations under PHIPA and applicable agreements, and to inform Participants about identified risks that may impact them. The policy will also identify opportunities for Participants to engage with OCINet on the outcomes of privacy assessments and associated risk response and remediation activities.

**General Statements**

- OCINet has corporate policies and procedures that identify the triggers for conduct of privacy reviews and assessments and related privacy risk management activities including tracking risks in a privacy risk register and associated risk management processes and activities. OCINet will provide a copy of privacy and security risk assessment results to participants upon request.
- Where OCINet and the Participants involved in privacy breach management identify risks to be remediated by OCINet, these privacy risks will be added to the OCINet privacy risk register and will be subject to OCINet's enterprise risk management policies and procedures.
- Where Privacy Working Groups are established for OCINet system or service implementation projects the results of privacy assessments will be reviewed with the group along with proposed risk remediation activities. More information on the formation of Working Groups is identified in the PAC Terms of Reference.
- Where Participants have concerns about potential or actual privacy risks associated with OCINet systems or services, these issues can be raised and escalated through the Privacy Advisory Committee to the OCINet CEO and Board Committees. More information on this escalation path is identified in the PAC Terms of Reference.
- OCINet has corporate policies and procedures pertaining to its corporate service providers that include identification of privacy terms to be included in agreements and processes for monitoring compliance with privacy obligations in agreements.
- OCINet will provide guidance to Participants for due diligence review and monitoring of New Participant Service Provider (PSP) Arrangements and establish agreements where required with Participant Service Providers to manage risk to OCINet associated with PSP connectivity.

# Part 3: Privacy Support Materials

**Appendix A: Privacy Advisory Committee Terms of Reference APPROVED (April 26-25)**

**Appendix B: Guideline for Secure Sharing of PHI**

**Appendix C: OCINet Privacy Forms**

- OCINet New Participant Privacy Attestation Form
- OCINet Participant Privacy Re-Attestation Form
- OCINet Privacy Audit Request Form
- OCINet Privacy Inquiries and Complaints Notification Form
- OCINet Consent Directive Request Form
- OCINet Privacy Incident Notification Form
- OCINet Privacy Breach Report Form