Managing Participant Service Providers: A Guide for OCINet Participants

Purpose

OCINet participants rely on their own Participant Service Providers (PSPs) to support diagnostic imaging and other clinical and operational workflows, including systems that connect to OCINet systems, as part of their own operations.

Participants are Health Information Custodians (HICs) under the *Personal Health Information Protection Act*, 2004 (PHIPA) and remain fully responsible and liable for personal health information (PHI) in their custodianship at all times, including where PHI is collected, used, disclosed, stored, transmitted or otherwise processed by a PSP or any other third party acting on their behalf. The use of PSPs in relation to OCINet services does not reduce, limit or displace a participant's obligations or liability under PHIPA, the OCINet Data Sharing Agreement (DSA), or applicable laws.

This guide is provided to support participants in understanding and applying certain existing obligations under the DSA and the Shared Policies in the OCINet Participant Privacy Manual as they relate to managing PSP relationships where PSPs connect with OCINet systems. This guide does not alter or replace a participant's legal or contractual obligations under the DSA, Participant Privacy Manual or any Board-approved OCINet policies or procedures. Participants remain solely responsible for determining and implementing the due diligence, contractual controls, and ongoing oversight necessary to meet their own obligations, including in relation to the selection, use and monitoring of PSPs retained by the participant.

No OCINet guidance, review, or connectivity decision by OCINet should be relied upon as satisfying those obligations or as transferring responsibility for a PSP arrangement to OCINet. This guide does not constitute legal advice and is not intended to establish a best practice standard for third party risk management.

How This Relates to OCINet Services

Under the DSA:

- Participants are Health Information Custodians (HICs) and are responsible and liable for PHI processed by their PSPs, including the PSPs that connect with OCINet systems.
- Participants are required to conduct appropriate due diligence before entering into or permitting a PSP arrangement that involves connections with OCINet systems.
- Where a participant enters into a PSP arrangement, the participant must have a written agreement in place with the PSP that supports the participant's ability to comply with PHIPA and the OCINet DSA.
- Participants may only permit their PSPs access PHI through connections with OCINet systems while the applicable agreement between the participant and PSP is in effect. Participants are expected to notify OCINet when they terminate their agreement with the PSP.

- OCINet may request confirmation of due diligence or information about the agreement between the participant and PSP, including a copy of the agreement where needed to assess risks to OCINet systems or services.
- In no circumstance will OCINet's decision to connect a PSP to its systems constitute a waiver of any of OCINet's rights under the OCINet DSA or transfer any responsibility or accountability for a PSP from a participant to OCINet.

OCINet:

- Provides shared technology services and operates as a Health Information Network Provider (HINP) and, in some contexts, as an agent of participants when providing OCINet services. In this role, OCINet applies privacy and security standards to its own systems and service providers that are consistent with its obligations under PHIPA, the DSA and applicable policies.
- Reviews New Participant Service Providers as defined in the OCINet DSA.[1] New Participant Service Providers require OCINet Board approval before OCINet will connect the PSP with OCINet systems. OCINet Board approval applies to the approved type of PSP service; material changes to that service may require re-approval.
- May review new PSP connectivity for the purpose of assessing risks to OCINet systems and services and to determine whether OCINet has reason to believe that a participant may not be able to satisfy its obligations under the DSA in connection with a PSP arrangement. OCINet may, in its sole discretion, refuse, suspend or terminate PSP connectivity to protect OCINet systems and services, including the privacy and security of PHI.
- Does not select, manage, or oversee participant PSPs. Any review, authorization, or decision by OCINet in relation to PSP connectivity or integration does not transfer responsibility for a PSP from a participant to OCINet and does not replace or diminish a participant's independent obligations under PHIPA or the DSA.
- May require that PSPs enter into terms of access directly with OCINet prior to being connected to OCINet systems.

Before You Engage a PSP: Conducting Due Diligence

Participants are responsible for determining and carrying out due diligence measures sufficient to enable them to meet their obligations under PHIPA, the DSA, and applicable Shared Policies when engaging PSPs will connect with OCINet systems. The nature and depth of due diligence should be proportionate to the role the PSP will play and the sensitivity and volume of PHI involved.

Before permitting connectivity or integration, participants should satisfy themselves that the PSP can comply with the restrictions and conditions necessary for the participant to meet its obligations. Considerations may include whether the PSP:

[1] "**New Participant Service Provider**" means a Participant Service Provider that the Corporation 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 the Services will not be considered a New Participant Service Provider.

- ☐ Is willing to enter into a written agreement that includes privacy and security restrictions and obligations required by the participant
- ☐ Understands that it is acting on the participant's behalf when handling PHI
- ☐ Understands the sensitivity of PHI accessed in connection with OCINet services
- ☐ Has experience supporting healthcare or clinical environments
- ☐ Maintains privacy and security policies and procedures and safeguards appropriate to the services provided and the nature of PHI access
- ☐ Has defined processes for identifying and reporting privacy incidents or breaches in a timely manner
- ☐ Can provide compliance evidence where appropriate (e.g., attestations or assessment report findings)
- ☐ Has appropriate insurance coverage for privacy and security incidents (participants may consult with their insurance brokers for guidance on insurance coverage appropriate for their circumstances)
- ☐ Has no history of material privacy or security incidents, or can demonstrate appropriate remediation

Good practice: Participants should retain records demonstrating that due diligence was completed, including the factors considered and the basis for the decisions made in engaging the PSP.

Contracting with PSPs Connected to OCINet Systems

Because participants remain fully accountable for PHI processed by PSPs, participant–PSP agreements should support compliance with PHIPA and the DSA in their specific operational context. While not an exhaustive list, agreements should address the following, as applicable:

Use and Processing of PHI

- ☐ PHI may only be used to provide the agreed-upon services and in accordance with the participant's instructions;
- ☐ No secondary use or disclosure of PHI without authorization and legal authority (e.g., sale of data to third parties, use to develop to test machine learning models, de-identification for other purposes);
- ☐ Access limited to authorized individuals acting on the participant's behalf; and
- ☐ Access to PHI terminates at the end of the agreed upon service term.

Safeguards and Accountability

- ☐ Requirement to protect PHI using appropriate administrative, technical and physical safeguards;
- ☐ Confidentiality agreements and privacy training for staff in place and evidence logged;

- Permitting reasonable audits or reviews by the participant to verify compliance with applicable privacy and security obligations, subject to reasonable notice, frequency, and confidentiality requirements; and
- Providing relevant, recently completed privacy or security assessments relating to the services and cooperating reasonably with the participant to support participant-led risk assessments, subject to confidentiality constraints.

Privacy and Security Incidents or Breaches

- Prompt notification of suspected or confirmed privacy incidents or breaches or confirmed security breaches; and
- Cooperation with containment, investigation, and mitigation activities necessary to support the participant's obligations under PHIPA.

Subcontracting

- Restrictions on subcontracting processing of PHI without prior written authorization; and
- Requirement that any permitted subcontractor be bound by equivalent privacy and security obligations through a written agreement, and that the PSP remain responsible for the acts and omissions of its subcontractors.

End of Services

- Secure return or destruction of PHI with verifiable proof of deletion; and
- Survival of confidentiality and security obligations.

Ongoing Oversight of PSPs

Participants remain solely accountable for PHI processed by PSPs they retain and are expected to maintain oversight for as long as the PSP processes that PHI on their behalf. Oversight should be proportionate to risk.

Oversight activities might include:

- periodically confirming that safeguards remain in place;
- obtaining updated compliance attestations or risk assessments where appropriate;
- reassessing risks if integrations or services change; and
- ensuring access to PHI is removed when no longer required.

OCINet's monitoring activities are limited to OCINet-controlled systems and services and do not extend to participant-managed PSP relationships. OCINet has no obligation to monitor, audit, or verify participant compliance with respect to PSPs, and any monitoring OCINet may conduct does not relieve participants of their independent compliance obligations.

Key Takeaway

PSPs that connect to OCINet systems may introduce privacy and security risks, even where access to PHI is indirect. Participants are solely responsible for identifying, managing, and mitigating these risks in a manner that enables compliance with PHIPA and the OCINet DSA.

Participants should consult with their legal or privacy advisors for advice on complying with their obligations under PHIPA, the OCINet DSA and managing their service provider relationships, including PSPs that connect with OCINet systems.

Participants may also find helpful guidance in the following resource:

Privacy Management Handbook for Small Health Care Organizations (May 8, 2025) available at www.ipc.on.ca.