Data sharing 'role' decision framework

[tool 4 complementing the data-sharing agreement template developed by BLG]

This document helps OHT members assess organizational readiness and evaluate key factors before agreeing to serve as an agent to other health information custodians or as a Health Information Network Provider (HINP) under PHIPA. It is not a list of mandatory requirements, but a tool designed to help guide and inform your thinking.

Instructions: Click on a link below to the section that best matches your need, or scroll through the entire document to see all three roles and the key decision points. Notes about this artefact from BLG and RISE, as well as a proposed citation, can be found in a box at the end of the document.

The document includes four sections:

1. Agent role

An agent performs services or functions on behalf of a health information custodian involving the collection, use, disclosure, or disposal of personal health information. The agent takes on statutory duties, and the custodian is legally accountable for the agent's actions.

Organizational capacity assessment

- Service definition clarity: Can we precisely define the services we would provide and the PHI we would need to access? Are the boundaries clear and manageable?
- Security infrastructure: Do we have appropriate physical security, IT security controls, and confidentiality protocols to protect PHI to the same standard as custodians?
- IT security expertise: Do we have IT security expertise available to establish and answer questions pertaining to IT security controls?
- Staff training capacity: Can we provide comprehensive PHIPA training to all relevant staff? Do we have resources to maintain ongoing awareness and compliance?
- Privacy expertise: Do we have access to privacy expertise for day-to-day questions, policy development, and incident response?
- Operational controls: Do we have processes for access control, audit logging, secure disposal, and breach management that meet PHIPA requirements?
- Quality assurance: Do we have quality control mechanisms to ensure we perform services accurately and reliably without compromising data integrity?

Relationship and agreement considerations

- Custodian expectations: Have we clearly discussed with the custodian(s) what they expect from us? Are those expectations realistic and within our capabilities? Will be set up to succeed?
- Agreement terms: Are we comfortable with the proposed agent agreement terms, including scope, liability allocation, audit rights, termination provisions, and indemnification?
- Multiple custodians: If serving as agent to multiple custodians, is it clear who we will take direction from? Is there a potential for conflicts, and how will they be resolved?
- Oversight and reporting: Are we prepared to undergo audits by custodians? Can we provide the reporting and transparency they require?

Business and strategic considerations

- Value proposition: Does taking on this agent role create value for our organization and the Ontario Health Team? Will it advance patient care or operational efficiency?
- Resource allocation: Do we have the staff time and resources to take on these responsibilities without compromising our core functions?
- Long-term viability: Is this a one-time project or an ongoing relationship? Do we want to be in this business long-term?

Risk and liability assessment

- Breach exposure: What happens to our reputation and relationships if there's a privacy breach involving PHI we handle as agent?
- Liability limits: Does the agent agreement appropriately limit our liability? Do we have insurance that covers our agent activities?
- Regulatory risk: Are we comfortable with potential IPC complaints or investigations arising from our agent activities, even if the custodian is ultimately accountable?
- Termination planning: If the agency relationship ends, do we have plans for secure return or destruction of PHI? Is there a clear exit process?

2. Health Information Network Provider (HINP) role

A HINP operates infrastructure that enables health information custodians to share personal health information for the purpose of providing or assisting in the provision of health care.
By enabling the secure sharing of personal health information among OHT members, a HINP can support integrated care and help improve outcomes for patients and families across an OHT. For this reason, it may be appropriate for an OHT member with sufficient capacity to agree to take on the role of a HINP.

Organizational capacity assessment

- Technical infrastructure: Do we have or can we acquire robust, secure IT systems capable of handling high volumes of sensitive health data with appropriate encryption, redundancy, and disaster recovery?
- Financial resources: Can we sustainably fund the initial setup costs (legal, technical, PIA) and ongoing operational expenses (maintenance, security updates, audits, staff) for network infrastructure?
- Expertise and staffing: Do we have or can we recruit personnel with expertise in health informatics, privacy law, information security, network administration, and PHIPA compliance?
- Governance structure: Do we have appropriate governance structures to oversee HINP operations, including board oversight, privacy officer designation, and accountability frameworks?
- Liability management: Have we assessed our exposure to liability for privacy breaches, system failures, or data quality issues? Do we have adequate insurance coverage?
- Compliance track record: Do we have a demonstrated history of compliance with privacy legislation and strong information security practices?

Strategic fit and value considerations

- Mission alignment: Does serving as HINP align with our organization's mission and strategic objectives? Will it advance care coordination goals for our population?
- Need assessment: Is there a clear, demonstrated need for the network infrastructure we would provide? Have we validated demand with potential participating custodians?
- Alternatives analysis: Have we considered whether existing HINPs or alternative information-sharing mechanisms could meet the Ontario Health Team's needs more efficiently?

- Competitive landscape: Do we understand who else provides similar services? What differentiates our potential offering?
- Sustainability plan: Do we have a viable long-term financial model? Will the network be self-sustaining or require ongoing subsidies?

Relationship and collaboration factors
- Trust and credibility: Do we have strong, trusting relationships with the health information custodians and members who would participate? Are we viewed as a neutral, reliable partner?
- Stakeholder buy-In: Have we secured commitment from key stakeholders including custodians, executives, boards, and clinical leaders? Is there consensus on shared objectives?
- Decision-making authority: Is it clear how network governance decisions will be made? Do participating members have appropriate input while we maintain operational control?

Risk assessment
- Breach implications: Have we assessed the reputational, financial, and legal consequences if a major privacy breach or system failure occurs under our watch?
- Regulatory scrutiny: Are we prepared for potential investigations by the Information and Privacy Commissioner if complaints arise about network operations?
- Scope creep: Do we have clear boundaries around what the network will and won't do? Can we resist pressure to expand beyond our capacity?
- Exit strategy: If we need to discontinue HINP services, do we have a plan for data migration, service continuity, and orderly wind-down?

3. Managing Member role

A managing member oversees an external organization (such as a cloud service provider) that serves as HINP to Ontario Health Team members. The managing member provides due diligence and oversight services on behalf of the other members, who remain legally accountable for the HINP's actions.

Organizational capacity assessment
- Oversight expertise: Do we have or can we access expertise in vendor management, technology assessment and IT security, privacy auditing, and PHIPA compliance to effectively oversee an external HINP?
- Due diligence capability: Can we conduct thorough initial due diligence of HINP candidates, including technical assessments, security audits, financial stability reviews, and reference checks?
- Contract negotiation skills: Do we have legal and procurement expertise to negotiate favourable terms that protect member interests and ensure PHIPA compliance?
- Ongoing monitoring resources: Can we dedicate staff time and resources to continuous monitoring of HINP performance, compliance, and service levels?
- Incident response preparedness: Can we coordinate breach response, service disruptions, and other incidents involving the external HINP on behalf of members?

Authority and governance considerations
- Clear mandate: Have the other members granted us clear authority to act on their behalf in selecting, contracting with, and overseeing the external HINP?
- Decision-making framework: Is there a clear framework for how decisions about the HINP will be made? When do we have autonomy versus when must we consult members?
- Accountability structure: Do members understand that they remain accountable under PHIPA even though we provide oversight? Are members clear about their continuing obligations?

- Reporting relationships: Have we established clear reporting structures to keep members informed about HINP performance, compliance issues, and risks?
- Conflict-resolution process: Is there a process for resolving disagreements between us and other members about HINP oversight or performance issues?
- Member engagement: Can we effectively engage diverse members (hospitals, physicians, community services) with varying levels of technical and privacy sophistication?

Vendor selection and management

- Selection criteria: Have we developed comprehensive criteria for evaluating potential HINP vendors, including technical capability, security, privacy compliance, financial stability, and experience?
- Market knowledge: Do we understand the market for HINP services, including available vendors, typical pricing models, and industry standards?
- Contract terms: Can we ensure contracts include appropriate provisions for PHIPA compliance, audit rights, breach notification, service levels, liability, termination, and data return/destruction?
- Performance monitoring: Have we established key performance indicators and service level agreements that we can realistically monitor and enforce?
- Audit rights and execution: Can we exercise audit rights effectively, either directly or through qualified third parties, to verify HINP compliance?
- Relationship management: Can we maintain an effective working relationship with the HINP vendor that is both collaborative and appropriately arm's-length?

Compliance and risk oversight

- PHIPA expertise: Do we have sufficient understanding of PHIPA requirements for HINPs to identify compliance gaps and hold the vendor accountable?
- Privacy impact assessment (PIA) review: Can we review and assess the adequacy of PIAs completed by or for the external HINP?
- Breach-response coordination: Are we prepared to coordinate member response to privacy breaches or security incidents involving the external HINP, including IPC notification decisions?
- Risk assessment and reporting: Can we identify, assess, and communicate risks posed by the external HINP to members in a timely and actionable manner?

Financial and business considerations

- Cost structure: Have we established a fair and sustainable model for recovering our oversight costs?
- Value proposition: Does our oversight add sufficient value to justify the cost compared to members conducting their own due diligence?
- Scalability: If additional members wish to join or existing members; needs grow, can we scale our oversight accordingly?

Liability and insurance considerations

- Liability exposure: What is our potential liability for failures of the external HINP? Are we adequately insured?
- Risk: Is risk allocation between us and the members fair and appropriate?
- Standard of care: Do we understand what standard of care applies to our oversight role? Have we documented our oversight methodology and diligence?

4. Key decision points

Before committing to any role, leadership should ensure:

- board and executive leadership have reviewed this assessment and support the decision
- legal counsel with PHIPA expertise has reviewed proposed agreements and provided advice
- privacy officer or privacy lead has assessed readiness and identified compliance gaps
- IT/security leadership confirms technical capacity or has plan to achieve it (for HINP and agent roles)
- finance manager has confirmed sustainability of required investments and ongoing costs
- risk management lead has assessed liability exposure and insurance coverage is adequate
- other OHT members understand and support our proposed role (especially for managing member role)
- implementation plan with clear milestones and accountability has been developed
- there is clear consensus that taking on the role aligns with organizational mission and capacity
- there is documentation of the decision-making process and rationale for future reference.

Proposed citation: BLG and RISE. Data sharing 'role' decision framework [tool 4 complementing the data-sharing agreement template developed by BLG]. Hamilton: McMaster Health Forum, 2026 (under license from BLG).

Note from BLG and RISE: This tool is meant to be read in conjunction with the following RISE brief, which provides links to the data-sharing agreement (DSA) template and to the other three tools in the series: Lavis JN, Moat KA, Wood B, Black L. RISE brief 37: Supporting data sharing by OHTs with an agreement template and four tools. Hamilton: McMaster Health Forum, 2026.

Note from BLG: The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns

Note from RISE: RISE prepares both its own resources (like the RISE brief that introduces this and other DSA tools) that can support rapid learning and improvement, as well as provides a structured 'way in' to resources prepared by other partners and by the ministry. RISE is supported by a grant from the Ontario Ministry of Health to the McMaster Health Forum. The opinions, results and conclusions are those of RISE and are independent of the ministry and Ontario Health. No endorsement by the ministry or Ontario Health is intended or should be inferred.