Roadmap for 'new project' data sharing and governance

[tool 3 complementing the data-sharing agreement template developed by BLG]

This roadmap provides OHT members with a practical framework for planning collaborative projects that require new data-sharing arrangements under the data-sharing (DSA) template and, relatedly, the *Personal Health Information Protection Act, 2004* (PHIPA). It is not a list of mandatory requirements, but a tool designed to help guide your thinking and improve the chances of a project's success. It does not replace the DSA.

Technology enables integration, but people make integration happen—primary-care providers coordinating longitudinal care across multiple settings, clinicians working across organizational boundaries, privacy professionals ensuring responsible data stewardship, IT staff building and maintaining systems, executives committing resources and leadership, and patients trusting their care team with their information.

The ultimate measure of success is not technical sophistication or privacy perfection—it is better care for patients and families served by the OHT, with members enabled to serve as an effective health home and coordinator of that care.

To support this outcome, the roadmap is structured around the following five phases, each designed to help OHT members move from concept to sustainable, system-wide data sharing in a deliberate and accountable way.

Instructions: Click on a link below to the phase or sub-phase that best matches your need, or scroll through the entire document to see all five phases and the conclusion. Notes about this tool from BLG and RISE, as well as a proposed citation, can be found in a box at the end of the document.

Together, these five phases provide OHT members with a practical, adaptable roadmap for advancing integrated care through responsible data sharing that is grounded in strong governance, supported by technology, and ultimately driven by people working together to improve patient outcomes.

PHASE 1: Project foundation and governance alignment

1.1 Initial project scoping

- Objective: Establish clear project parameters and data sharing requirements
- Key activities
  - Define the integrated service or care pathway requiring data sharing
  - Identify specific data to be shared
  - Assess whether the project supports primary care providers' ability to deliver comprehensive, continuous care and identify primary-care and other information gaps that will be addressed
  - Identify whether the project involves Indigenous communities, patients, or data, and determine if Indigenous data sovereignty principles apply
  - Map current state of data handoffs and system gaps
  - Articulate the clinical/operational risks of NOT sharing data
  - Document expected patient outcomes and system efficiencies
- Deliverable: **Project charter** including clinical/operational rationale and risk of inaction

1.2 Executive leadership engagement

- Objective: Secure commitment from organizational leaders comprising the OHT governance structure
- Key messages for executive leaders
  - Strategic alignment: How this project advances integrated care and OHT performance goals
  - Risk balance: Comparing risks of data sharing vs. risks of fragmented care and information gaps
  - Shared accountability: Clear delineation of roles, responsibilities, and liability considerations
  - Resource commitment: Required investments in technology, training, and change management
  - Indigenous partnership: If the project involves Indigenous communities or data, ensuring meaningful engagement with Indigenous leadership and respect for data sovereignty principles from project inception
  - Competitive advantage: How integrated data positions the OHT for future funding and partnerships
  - Primary-care enablement: How this project strengthens primary care as the foundation of integrated care by providing timely access to specialist assessments, hospital events, community services, and other information needed for longitudinal patient management
- Activities
  - Present project charter to Collaboration Council or equivalent
  - Identify executive sponsor from each participating organization
  - Establish steering committee with decision-making authority, if possible leveraging existing governance and other committees
  - Secure in-principle agreement to explore data-sharing arrangements
  - If Indigenous communities are involved, engage Indigenous leadership to determine appropriate governance participation and decision-making authority
- Deliverable: **Executive endorsement document** with named sponsors and steering committee

Phase 2: Technical and legal architecture design

2.1 System architecture decision

- Objective: Determine technical approach for data sharing
- Steps
  - Step 1: Current state technology assessment - Map relevant existing systems across all participating organizations, considering:
    - Current systems with project relevant data
    - Interoperability between current systems
    - Age/lifecycle status
    - Capacity for additional users
  - Step 2: Assess technical architecture options
    - Option A: **Leverage single existing system (system expansion)**
      - Description: One organization extends access to their existing system to other OHT members
      - Example use case: Hospital extends EMR access to Family Health Team and home care for shared patients in complex care program
    - Option B: **Acquire new shared system (new technology purchase)**
      - Description: OHT members jointly procure and implement a new system for shared use
      - Example use case: OHT purchases new care coordination platform for cross-organizational case conferencing and shared care planning
    - Option C: **Connect multiple existing systems (interoperability)**
      - Description: Build data exchange connections between organizations' existing systems
      - Example use case: Hospital EMR exchanges lab results and discharge summaries with community health center EMR and long-term care home clinical system through shared integration engine
- Activities:
  - Engage digital lead in Ontario Health region to ensure alignment with Ontario Health priorities
  - Engage IT leaders from each organization in architecture design sessions
  - Conduct vendor demonstrations for new system options (if applicable)
  - Develop integration requirements and feasibility assessment
  - Analyze total cost of ownership for each option (five-year projection)
  - Pilot technical proof-of-concept for preferred approach
- Deliverable: **Technical architecture recommendation** with implementation timeline, budget, and risk assessment

2.2 Organizational roles and responsibilities

- Objective: Clearly define and assign organizational roles for the data sharing arrangement
- Roles – Any OHT data sharing arrangement may entail the following roles
  1) **Member organizations**
     - Who they are: All OHT member organizations participating in the data-sharing arrangement. They are custodians of their data and bear primary responsibility for it. They can include:
       - Health Information Custodians (HICs): hospitals, long-term care homes, Community Health Centres, Family Health Teams, etc.
       - Non-HICs: community service organizations, housing providers, social service agencies, etc.
     - Important distinction
       - HICs are subject to PHIPA and have specific legal obligations
       - Non-HICs have limited duties under PHIPA but must meet equivalent obligations

        - Both HICs and non-HICs have an obligation to oversee HINPs
    - Member organization responsibilities: Each member organization remains accountable for their own privacy obligations even when using a Managing member and HINP.
2) **Health Information Network Provider (HINP)**
    - Definition: The HINP is defined in relation to HICs under PHIPA that own and operates the technical infrastructure that enables data sharing
    - Who can be the HINP
        - Option A: **OHT member organization**
            - An OHT member organization directly owns, hosts and operates the technology infrastructure
            - The organization's IT department manages servers, security, user access, and technical support
            - This member organization IS the HINP under PHIPA
        - Option B: **External vendor**
            - An external vendor (e.g., cloud software provider, managed service provider) operates the technology infrastructure under contract
            - The vendor provides a service to the OHT members as a HINP
            - Common examples: cloud-based EMR vendors, care coordination platform providers, integration engine hosts
3) **Managing member**
    - Definition: A Managing member is an OHT member organization that manages a HINP relationship and is accountable to all other OHT member organizations for ensuring the HINP operates effectively and meets privacy, security, and service requirements
    - The importance of this role – When an OHT uses a HINP (whether member organization or external vendor), someone must
        - Hold the contract and manage the relationship
        - Oversee HINP performance and compliance
        - Ensure privacy and security safeguards are adequate
        - Act as the accountable party to other OHT members
    - The Managing member can fulfill this role.
    - Key point: The Managing member is NOT the HINP (unless the member organization is also directly operating the infrastructure); the Managing Member manages and oversees the HINP on behalf of all OHT members
4) **Indigenous governing authority** (where applicable)
    - Definition: When a project involves data about Indigenous communities or patients who are members of Indigenous communities, the relevant Indigenous governing body (First Nation, Métis Nation, Inuit organization, or Indigenous health organization) may exercise governance authority over how that data is collected, used, shared, and managed
    - Indigenous data sovereignty principles – Indigenous data sovereignty recognizes the right of Indigenous peoples to govern the collection, protection, use and sharing of data about their communities and members. This is guided by the follow principles (the 'OCAP' principles):
        - Ownership, Control, Access and Possession (the "OCAP Principles")
            - Ownership: First Nations collectively own their cultural knowledge, data, and information
            - Control: First Nations have the right to direct all aspects of research and information management that affect them
            - Access: First Nations must be able to access data about themselves and determine how others may access itPossession: Physical control of data enables First Nations to assert and protect ownership
        - Inuit Qaujimajatuqangit
        - Principles of Ethical Métis Research

        - Collective benefit, Authority to control, Responsibility and Ethics (the "CARE Principles") created by the Global Indigenous Data Alliance to ensure the principles of Findable, Accessible, Interoperable and Reusable (the "FAIR" Principles) respect Indigenous rights.
- Activities:
  - Identify who, if anyone, will serve as HINP and/or Managing member
  - Document specific responsibilities and accountabilities for each role
  - Confirm each participating organization's understanding and acceptance of their role

- Deliverable: **Role assignment matrix** with organizational commitments

2.3 Legal framework development

- Objective: Establish legally compliant agreements that govern data sharing and protect all parties
- Consider agreements
  - Between members - Data sharing agreement (DSA) to establish
    - Participants in sharing
    - Roles (e.g., HINP, Managing member)
    - Purposes for sharing/scope of services
    - Permitted uses and obligations
  - With HINP (if different) – Services agreement covering technical infrastructure
    - Privacy and security schedules
    - Liability and indemnification clauses
    - Termination and data portability provisions
- Activities:
  - Engage privacy and legal counsel from participating organizations
  - Draft template agreements aligned with PHIPA requirements
  - Identify any required amendments to existing bylaws or policies
- Deliverable: **Suitable legal agreement** for data sharing

Phase 3: Risk assessment

3.1 Comprehensive risk identification

- Objective: Identify and document all significant risks associated with both implementing and not implementing the data sharing arrangement
- Considerations
  - Consider risks of new data sharing
    - Failure to meet specific PHIPA requirements
    - Non-alignment with ten 'fair information practice principles'
    - Failure to respect Indigenous data sovereignty principles, resulting in harm to Indigenous communities, loss of trust, or misuse of Indigenous data
    - Foreseeable privacy breach scenarios
    - Data quality and availability risks
    - System downtime or technical failures
    - Role ambiguity
  - Consider risks of NOT sharing data:
    - Missed opportunities for early intervention
    - Patient safety incidents due to incomplete information

        - Unnecessary duplication of tests/procedures
        - Delayed care and poor patient experience
        - Perpetuation of fragmented care for Indigenous patients who may already experience systemic barriers to culturally safe, integrated services
        - Misalignment integrated care expectations
- Activities:
    - Conduct risk identification workshops with privacy, legal, IT, and clinical stakeholders
    - Review similar data sharing projects for lessons learned
- Deliverable: **Risk register** with likelihood and impact ratings for both data sharing AND non-sharing scenarios

3.2 Risk treatment / Mitigation planning

- Objective: Develop comprehensive strategies to address identified risks through appropriate treatment measures
- Considerations
    - Consider risk treatment options (avoid, mitigate, transfer, and accept) and develop plan with treatment elements:
        - Indemnification and other terms in legal agreements
        - Insurance
        - Training and communication plan
        - HINP/vendor oversight plan
        - Incident response protocol
        - Client/patient facing communications (e.g. consents, liability waivers)
- Activities:
    - Evaluate treatment options for each risk in the Risk register
    - Assign accountability for implementing and monitoring each control
    - Document rationale for any risks that will be accepted
    - Consult with insurance broker(s) regarding insurance coverage adequacy
- Deliverable: **Risk treatment / Mitigation plan** with specific controls and accountabilities

3.3 Appropriate additional assurance

- Objective: Validate planned risk mitigation measures and identify any gaps through objective assessment
- Options:
    - Privacy impact assessment
    - General security/threat risk assessment
    - Specialized security assessments
    - Internal or third-party
- Basis for assessment:
    - Data-sharing agreement
    - HINP/Vendor agreement
    - Risk register
    - Risk treatment / Mitigation plan
    - Operational policies and procedures
- Activities:
    - Determine appropriate type and scope of assessment based on risk profile, leveraging existing governance and other committees as well as subject matter experts for consultation
    - Engage qualified internal or external assessors
    - Conduct assessment and document findings

- Receive assessment and document response
- Deliverable: **Assessment report(s)** with identified gaps, plus responsive documentation that assigns responsibility for addressing identified gaps and weaknesses

Phase 4: Implementation

4.1 Stakeholder engagement strategy and respecting Indigenous data sovereignty

- Objective: Build support and address concerns among all stakeholder groups to ensure smooth implementation
- Key stakeholder groups:
  - **Clinical staff**
    - Understand workflow changes and efficiency gains
    - Address concerns about additional documentation or system access
    - Highlight patient safety and quality improvements
    - Involve champions in design and testing
  - **Primary Care Networks (PCNs) and primary-care practice administrators**
    - PCNs should be involved in workflow design for registration, consent processes, and information routing
    - Practice administrators within PCNs are often responsible for managing system access, printing reports, filing documents
    - May face increased workload during implementation without additional resources
    - Need clear processes for handling new information flows
    - Require training on new systems but often have limited time away from front desk
  - **Privacy & information management staff**
    - Address concerns through robust controls
    - Recognize increased workload during implementation
  - **IT & technical staff**
    - Assess capacity and resource needs
    - Involve in vendor integration planning
    - Plan for ongoing support and maintenance
    - Address concerns about system complexity
  - **Patients, families and caregivers**
    - Communicate benefits of integrated care
    - Explain data sharing and privacy protections
    - Provide opt-out mechanisms where appropriate
    - Gather feedback on experience
  - **Indigenous communities and leadership**
    - Engage early and meaningfully, not as consultation but as partnership
    - Respect Indigenous governance processes and timelines (may differ from institutional timelines)
    - Address historical harms and current mistrust of health data systems
- Activities
  - Recruit OHT leadership and technical staff for planning committee, if possible leveraging existing governance and other committees
  - Develop and test plan
- Deliverable: **Change-management plan** with communication calendar and stakeholder engagement activities

4.2 Training and competency program

- Objective: Provide reassurance to HICs that staff – including those in non-HIC organizations without direct oversight – are competent to handle personal health information appropriately
- Sample training curriculum
  - Module 1: Privacy fundamentals (all staff)
  - Module 2: Integrated-care data sharing (all staff)
  - Module 3: System-specific training (end users)
  - Module 4: Privacy and security for non-HIC staff (non-HIC organizations)
  - Module 5: Advanced privacy for managers/leads (leadership)
- Considerations
  - **Training delivery options**
    - Blended approach: e-learning for foundational content, in-person for system training
    - Mandatory completion before system access granted
    - Competency assessment (quiz or scenario-based)
    - Annual refresher training requirement
    - Just-in-time resources and job aids
  - **Primary-care practice constraints**
    - Physicians and nurses cannot easily leave practice for half-day training sessions
    - Administrative staff may change frequently, requiring ongoing training capacity
    - Practices range from highly sophisticated EMR users to basic adopters
    - Most primary care practices lack on-site IT staff
  - **Competency assurances for non-HIC staff**
    - Pre-access competency testing with minimum passing score
    - Observation and sign-off by supervisor for initial uses
    - Enhanced monitoring during first 90 days (access audit reviews)
    - Immediate remediation for any privacy incidents
  - **Training records and compliance tracking**
    - Centralized training registry vs. member training registries
    - Completion tracking and training analytics
    - Plan for addressing non-completion
- Activities:
  - Develop training materials for each module
  - Create competency assessment tools and establish passing criteria
  - Set up training delivery platform (learning management system)
  - Schedule training sessions for all staff before go-live
  - Establish system for tracking completion and maintaining records
- Deliverable: **Training curriculum**, delivery plan, and competency assessment tools

Phase 5: Go live

5.1 Pilot implementation

- Objective: Test the data sharing system in a controlled environment to validate functionality, workflows and controls before full rollout
- Pilot approach
  - Select 1-2 sites representing different organization types (e.g., one HIC, one non-HIC)
  - Limited scope (specific program or patient population)
  - Intensive support and monitoring
  - Structured feedback collection
- Pilot success criteria
  - System functionality meets requirements
  - Workflow integration achieves time savings or quality improvements
  - Privacy and security controls operate effectively
  - Staff demonstrate competency and satisfaction
  - No major incidents or breaches
  - Patient feedback is positive
- Activities
  - Daily huddles during first week
  - Weekly working group meetings
  - Real-time issue tracking and resolution
  - Audit of access logs and use patterns
  - Gather qualitative feedback from staff and patients
  - Refine training and support materials
- Go / No-go decision: Steering committee review of pilot results before broader rollout
- Deliverable: **Pilot evaluation report** with recommendations

5.2 Full rollout

- Objective: Deploy the data sharing system across all participating organizations in a controlled, phased manner
- Phased approach by organization
  - Sequence based on readiness, complexity, and strategic priority
  - Minimum two-week interval between organizations
  - Maintain pilot site support during rollout
- Rollout readiness checklist (per organization)
  - Legal agreements executed
  - Technical infrastructure tested and validated
  - All staff completed required training
  - Privacy and security controls in place
  - Workflows documented and communicated
  - Indigenous data governance requirements met (if applicable), including any community-specific protocols and approval processes
  - Support resources identified and available
  - Go-live communication sent to staff and patients
  - Rollback plan prepared
- Go-live support:
  - On-site super-users for first week
  - Extended help desk hours

    - Daily executive briefings
    - Real-time issue escalation process
    - Celebration and recognition of milestones
- Activities:
    - Confirm readiness for each organization using checklist
    - Execute go-live activities according to rollout schedule
    - Monitor system performance and user experience during first weeks
    - Provide intensive support and address issues immediately
    - Document lessons learned and refine approach for subsequent organizations
- Deliverable: **Rollout schedule** and go-live support plan

Conclusion

This roadmap is a framework to be adapted, not a rigid prescription. Every OHT's context is unique. Use these phases and tools as a starting point, customize to your specific clinical needs, organizational relationships, technical environment, and resources.

Critical success factors:

1. Balance risk perspectives: Weigh data sharing risks against risks of fragmented care
2. Invest in relationships: Legal agreements are necessary but trust and communication are essential
3. Design for sustainability: Ensure HINP and agent roles are viable long-term
4. Prioritize training: Competent staff are the best privacy protection
5. Start focused: Pilot with limited scope before expanding
6. Monitor and adapt: Use data to continuously improve
7. Respect Indigenous data sovereignty: Where Indigenous communities are involved, recognize their inherent right to govern data about their peoples and ensure meaningful partnership, not just consultation.

Ultimately, success depends not on technology alone, but on people and governance working together to enable integrated care that improves outcomes for patients and families across the OHT.

Important reminder from BLG: This roadmap is intended to facilitate internal discussion and decision-making. It does not constitute legal advice. Organizations should engage qualified legal counsel and privacy consultants when planning a data sharing project. The specific factors relevant to your organization may vary based on your circumstances, the proposed arrangements, and evolving regulatory guidance.

Proposed citation: BLG and RISE. Roadmap for 'new project' data sharing and governance [tool 3 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.