Borden Ladner Gervais

Ontario Health Teams
UPDATE | February 2020

Personal Health Information Sharing, Client Privacy and PHIPA Compliance

Guidance for Ontario Health Care Providers and Organizations

This is the fifth in a series of BLG publications to assist Ontario health care providers and organizations as they work toward Ontario Health Team implementation.

More detail and insight will be provided in upcoming BLG publications, seminars and other communications: stay tuned!

Ontario Health Teams:

Personal Health Information sharing, client privacy, and PHIPA compliance

The transition towards Ontario Health Teams (OHTs) raises a number of important questions about Personal Health Information (PHI) sharing, client privacy, and compliance with the *Personal Health Information Protection Act, 2004* (PHIPA). PHIPA is the provincial legislation governing the collection, use, and disclosure of PHI by health information custodians (HICs), such as hospitals, primary care providers, and certain home care and community care organizations.

In light of the timelines for the OHT application process, prospective OHTs are already starting to consider how their members will share client PHI in a way that furthers the Ministry's Quadruple Aim (better client and population health outcomes; better client, family and caregiver experience; better provider experience; and better value), while also safeguarding client and client privacy. They are also starting to think about what PHIPA compliance will look like for OHTs, given that many of PHIPA's provisions are predicated on the view of HICs as independent healthcare entities – a framework that may no longer hold in an OHT world.

The Ontario government appears to appreciate that changes to PHIPA are required to facilitate the information sharing necessary to enable a full continuum of integrated and coordinated care for a defined population. In December 2019, the government passed new legislation, the *Plan to Build Ontario Together Act*. Among other things, the Act establishes new regulation making powers under PHIPA in respect of the circumstances under which an OHT will be able to collect, use, and disclose PHI. The proclamation date for these new powers is to be determined.

Before the new regulation making powers were enacted, the Information & Privacy Commissioner of Ontario (IPC) raised concerns about the fact that non-HICs may participate in OHTs. The IPC's concern was that non-HIC OHT members

will not be subject to the same PHIPA requirements as HICs, and therefore OHTs will not afford clients an appropriate level of privacy protection. In light of this concern, the IPC recommended that only HICs be permitted to handle PHI within an OHT, or that some framework be imposed that applies PHIPA-equivalent obligations on non-HIC OHT members.

It's not yet known what any new regulations under PHIPA might look like, or the extent to which they may address some of the challenges outlined in this article (or those raised by the IPC). In one scenario, new regulations could require all members of an OHT to "harmonize upward" – that is, they could impose PHIPA-equivalent requirements on all OHT members, including non-HICs, along the lines of the IPC's proposal. Operationally, this could prove onerous for some non-HICs. Alternatively, regulations could impose an altogether new (and in some respects less stringent) set of requirements on OHT members, or allow for implied consent to PHI disclosure in a broader set of circumstances. The government's ultimate plan for the privacy regulation of OHTs has not yet been fully revealed.

With this evolving landscape in mind, this article identifies and explores some of the data sharing and privacy-related questions that the shift toward OHTs poses. It offers practical suggestions for handling some of the legislative, regulatory, and operational issues that OHTs may encounter with respect to PHI sharing, client privacy and PHIPA compliance.

I. OHTs and PHIPA compliance

The shift to OHTs will require team members to harmonize and integrate their privacy infrastructures to some degree. This may prove challenging, given the potential variation in PHIPA readiness across a particular OHT. Some OHT members will be hospitals or other larger institutions with an extensive and sophisticated privacy framework in place: dedicated privacy and information security personnel, detailed policies and procedures, extensive staff training, annual breach simulation drills, and the like. Others may be smaller HICs with leaner levels of privacy staffing and less "on the ground" experience handling cybersecurity issues or privacy breaches. Still others, like social service organizations, may not be HICs at all. These members may well have their own privacy policies and practices in place, but those may not map precisely onto the systems that HICs have. They may not have policies addressing the full range of privacy issues, or the same range of safeguards in place to protect PHI.

An important early step will be to take inventory of the PHIPA compliance infrastructure of each OHT member.

An important area of focus in this process will be on the OHT members that are not HICs under PHIPA. Although non-HICs may not be subject to PHIPA's requirements by law, they will need to become PHIPA-compliant to some degree simply in order to function within the broader OHT. As a practical matter, for instance, HIC members of an OHT may be reluctant to disclose their clients' PHI to non-HICs that lack adequate PHIPA safeguards. (Disclosure to HICs and non-HICs is discussed below.)

To be a member of an OHT, an organization need not be considered a HIC under PHIPA. It is therefore likely that most OHTs will comprise a mix of HIC and non-HIC members. PHIPA defines a HIC as:

… a person or organization described in one of the following paragraphs who has custody or control of PHI as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:

1. A health care practitioner or a person who operates a group practice of health care practitioners.

2. A service provider within the meaning of the *Home Care and Community Services Act*, *1994* who provides a community service to which that Act applies.

3. Repealed: 2016, c. 30, s. 43 (1).

4. A person who operates one of the following facilities, programs or services:

   i. A hospital within the meaning of the *Public Hospitals Act*, a private hospital within the meaning of the *Private Hospitals Act*, a psychiatric facility within the meaning of the *Mental Health Act* or an independent health facility within the meaning of the *Independent Health Facilities Act*.

   ii. A long-term care home within the meaning of the *Long-Term Care Homes Act*, *2007*, a placement co-ordinator described in subsection 40 (1) of that Act, or a care home within the meaning of the *Residential Tenancies Act*, *2006*.

   ii.1. A retirement home within the meaning of the R*etirement Homes Act*, *2010*.

   iii. A pharmacy within the meaning of Part VI of the *Drug and Pharmacies Regulation Act*.

   iv. A laboratory or a specimen collection centre as defined in section 5 of the *Laboratory and Specimen Collection Centre Licensing Act*.

   v. An ambulance service within the meaning of the *Ambulance Act*.

   vi. A home for special care within the meaning of the Homes for *Special Care Act*.

   vii. A centre, program or service for community health or mental health whose primary purpose is the provision of health care.

5. An evaluator within the meaning of the *Health Care Consent Act*, *1996* or an assessor within the meaning of the *Substitute Decisions Act*, *1992*.
6. A medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act*.
7. The Minister, together with the Ministry of the Minister if the context so requires.
8. Any other person prescribed as a health information custodian if the person has custody or control of PHI as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons.

We recommend that each OHT evaluate what kind of privacy infrastructure, if any, its non-HIC members have implemented. This, in turn, will help the OHT assess the resource and operational burden that will likely be involved for the non-HICs to establish a basic privacy framework. It may also shed light on how the other OHT members may be able to assist in those PHIPA-readiness efforts, since ultimately collective PHIPA readiness will work to the benefit of the OHT as a whole.

OHT members that are HICs will also need to evaluate their respective PHIPA compliance infrastructures and determine whether there are any significant gaps or variations that need to be addressed. Ideally, the requirements for PHI privacy and security and breach management will be reasonably uniform across the OHT. As such, coming out of this assessment, **some OHTs may opt to have a single, unified roster of PHIPA policies and procedures, while others may decide simply to have their members undertake to make their policies and procedures substantively similar to the best practice within the OHT.**

If all of the OHT members are HICs, they may wish to consider whether to apply to the Ministry to be treated as a single HIC under PHIPA. The potential benefits and disadvantages to seeking this designation would need to be carefully considered in each individual instance. However, OHTs comprised of HICs alone are encouraged to consider this early on, with the advice of legal counsel.

Closer to the time of maturity, OHT members may wish to set forth in writing some of their basic privacy-related commitments to one another. One vehicle for doing this may be a data sharing agreement among OHT members. The benefit of this approach is that it compels OHT members to talk through the various PHIPA-related obligations that they have to one another and to their clients. It also clearly articulates the steps that individual OHT members continue to be responsible for as they start working together.

We recommend that OHT members discuss, and consider addressing through a data sharing agreement, the obligations of each OHT member for:

- Implementing policies and procedures on appropriate privacy and information security-related topics, and making these policies reasonably similar in substance to the best practice of other OHT members;
- Cooperating with other OHT members when necessary–for instance when a client asks to correct or have access to PHI from more than one OHT member, or when investigating or handling a privacy incident involving more than one OHT member;
- Imposing restrictions on access to, and the use and disclosure of, PHI by staff, including professional staff and independent contractors;
- Training staff on client privacy and information security; and
- Regulating individual user access to PHI.

II. OHTs and PHI sharing

Under PHIPA, there are certain circumstances in which HICs may disclose or share PHI without first obtaining express consent from the client to whom the PHI pertains. However, these exceptions to the express consent rule may prove limited in the OHT setting.

For example, PHIPA allows two or more HICs to disclose PHI to one another without express consent for the purpose of providing health care or assisting in the provision of health care. This is often referred to as the "circle of care" exception to the express consent requirement, although that phrase is not actually used in PHIPA itself. OHT members will be able to rely on this provision to permit PHI sharing without consent as well. For instance, if three HICs within an OHT want to share a client's PHI to care for the client, they may do so based on implied consent.

Under current law, however, an OHT will not be able to rely on this provision if any of the OHT members among whom the PHI is proposed to be shared are not HICs as defined in PHIPA. If a social service provider that does not fall within the definition of HIC is one of the client's care providers, it could not be party to this implied consent-based PHI sharing. Express consent would need to be obtained from the client to allow such a provider to receive PHI.

Moreover, as currently drafted, PHIPA would require express consent for many of the types of PHI sharing that OHT members may wish to undertake. For example, PHIPA would require express consent for any PHI sharing among OHT members for the purposes of health system planning and service delivery. Currently, such sharing is permitted without express consent only as between HICs and prescribed government entities, like the Canadian Institute for Health Information.

Similarly, PHIPA allows PHI sharing for quality improvement purposes without express consent, but only with respect to individual patients who have been cared for by both of the HICs involved in the PHI exchange, and only for the quality improvement purposes of the HIC receiving the PHI. This provision would likely allow a HIC home care agency to disclose PHI to a HIC acute care facility within the same OHT where the PHI relates to a shared client and where it is shared to enable the acute care facility to monitor the quality of the care it provides to that same client or similar clients. It would not allow PHI to be disclosed among OHT members who are not HICs, or even among those who are HICs but who lack a direct treatment relationship with the client.

if the acute care facility wanted to receive the home care agency's PHI in order to run a data analysis to help the home care agency assess its quality of care, this provision could not be relied on. Similarly, if the acute care facility wanted to run a data analysis designed to help the OHT as a whole monitor its collective quality of care, this provision could not be relied on. In either of these scenarios, express client consent would be required.

The narrow scope of the exceptions to the express consent rule makes sense in the traditional healthcare environment, where individual healthcare facilities generally need to exchange PHI only with similar facilities and only for client care or internal quality improvement purposes. In the OHT world, however, the exceptions may prove less helpful. Indeed, under PHIPA as currently drafted, any of the following scenarios would require express consent:

- A HIC member of an OHT seeks to disclose PHI for the purpose of care provision to another OHT member that is not a HIC.
- Two OHT members seek to share PHI for a purpose unrelated to client care, assisting in the provision of care, or quality improvement, but which is legitimate nonetheless. Given that the government may impose reporting obligations on OHTs that transcend these categories, this is an entirely plausible scenario.
- Multiple members of an OHT seek to disclose PHI to a single OHT member so that the recipient OHT member can run a data analysis and provide the other OHT members with information about their own (not the recipient's) individual or collective quality of care. This is a feasible scenario given the OHT system's focus on metrics and accountability.
- An OHT as a whole wishes to undertake a collective risk management or error management initiative under which a single OHT member will receive PHI from the others, analyze the data, and disseminate member-specific and OHT-wide information to all team members. This is a conceivable scenario given the focus on team-level performance under the OHT system.

In any of the situations described above, under current law, express consent would need to be obtained from a large volume of clients. This would undoubtedly be onerous and impede the efficiency and effectiveness of OHTs. The only alternative would be for OHTs to rely only on de-identified data, rather than PHI, to achieve their health system planning and quality improvement goals. This may be somewhat effective, but perhaps not to the degree necessary to enable OHTs to fulfill the Ministry's Quadruple Aim.

Unless and until PHIPA is amended or regulations are enacted under the new regulation-making power to facilitate more effective PHI sharing at the OHT level, OHTs may find themselves having to try to meet the care integration and improvement objectives of the OHT regime without access to all the data they feel they need to effectively satisfy those objectives. We recommend that OHTs understand the extent to which their members can and cannot disclose PHI to one another in the course of providing client care, assisting in the provision of client care, and monitoring and improving their quality of care. **Understanding the obstacles to information sharing will not remove the obstacles, but will help OHTs identify and address them in an organized and effective way.**

An OHT data sharing agreement may offer a way of doing this, by articulating the various situations in which express client consent will and will not be needed for members to share PHI or other data with one another. The agreement could, for instance, identify the limited situations in which PHI sharing is permitted among OHT members without express consent, and confirm that those exceptions to the express consent requirement continue to apply. It could also enumerate the situations in which express consent will be required. The legal landscape surrounding OHTs is shifting, and the priorities and requirements for OHT data sharing agreements may need to shift with them as amendments are passed or new regulations implemented. However, we encourage OHTs to start thinking about these issues now.

III. Practical suggestions

With all of this in mind, we recommend that during "**year one**," potential OHT members do the following:

1. **Take inventory of the OHT members' respective PHIPA compliance infrastructure. This inventory should identify,** for each member's privacy program, such things as general staffing levels, overall resourcing, major programs and major privacy and security policies and procedures. It may also be prudent to consider any gaps in terms of privacy and information security that members have identified through routine compliance monitoring and/or privacy and security incidents.

   The Ontario government will be requiring OHTs to prepare digital health plans that will, among other things, address OHT members' existing and eventual uses of supporting digital health technology. This process, too, will require taking an inventory of sorts. In many institutions the considerations underlying the digital health technology inventory will be different from those being discussed here. However, it may make sense to consider whether, for a particular OHT member, these two processes might be coordinated in some fashion.

2. **Determine how the OHT wants to achieve the goal of privacy infrastructure integration.** Does it ultimately want a single, unified privacy program and roster of policies? Or is the goal to ensure that members' respective programs and policies are substantively similar to the best practice within the OHT? The choice may depend in part on the current privacy policies of each OHT member and the resources it has at its disposal. On either approach, a number of steps may be required to build up and integrate the members' respective privacy infrastructures. The exact steps, the timeline along which they will proceed and the extent of involvement required from various OHT members will likely vary depending on which choice the OHT makes. The Ontario government's Ontario Health Teams: Digital Health Playbook offers a helpful discussion on the integration of privacy policies in an OHT setting.

3. **Identify what will be required in terms of time, money and organizational resources to carry out this integration. This assessment should consider:**

   - What will be needed to help any non-HIC members that lack basic privacy frameworks to get off the ground, either on their own or in partnership with other OHT members.
   - What it will take to address any significant variations that may exist among HIC members' PHIPA compliance programs.
   - The specific tasks associated with whichever approach to integration the OHT opts for (see step 2 above).

4. **Formulate a work plan and timeframe for privacy integration and map this onto the OHT's plans for implementing integrated client care programs, taking into account:**

   - The specific work associated with the integration effort and the actual resources that can be devoted to it (see step 3 above).
   - The need to identify which OHT members will lead and carry out the various components of the integration effort, recognizing expertise, resources and other relevant considerations.
   - How this privacy integration timeframe meshes with the broader planning around integrated client care. For example, an OHT's first foray into integrated client care may have to rely on particular OHT members that already have well established and easily integrated privacy systems. This is worth identifying and working toward early on.


EXIT
gettyima
Thomas Barwick

5. **Enter into a written agreement that positions the OHT to begin working as a cohesive, "privacy integrated" whole. The topics to be addressed in the agreement could include:**
    - A commitment by OHT members to continue to integrate their privacy programs and a statement as to whether they intend to have a single, unified privacy program and roster of policies, or to ensure that their respective programs and policies will be substantively similar to the best practice within the OHT.
    - A summary of the situations in which PHIPA authorizes them to share PHI with one another in the absence of express client consent.
    - An undertaking to enter into a data sharing agreement.

At maturity, OHT members should have the following:

1. **A functioning, integrated privacy infrastructure.** This could take the form of a unified privacy program, with coherent OHT-wide policies and procedures, programs, forms, staff training and compliance enforcement. Alternatively, the integration could entail OHT members collectively deciding what will comprise best practice within the OHT, and then ensuring that their respective privacy programs and policies are substantively similar to that best practice.
2. **A robust data sharing agreement. The agreement should include discussion of:**
    - The extent to which OHT members can and cannot disclose PHI to one another without express consent in the course of providing client care, assisting in the provision of client care, and monitoring and improving their quality of care.
    - OHT members' obligations toward one another with respect to privacy. These could include, for example, a commitment to continue working cooperatively to maintain and enforce appropriate policies on privacy and security (either individually or across the OHT). They could also include a promise to co-operate when necessary – for instance when a client seeks access to PHI from more than one OHT member, or when investigating or handling a privacy incident involving more than one OHT member.

    To the extent that an OHT intends to integrate members' electronic record systems, the DSA will likely need to address additional issues also (see, for example, IPC Decision 102). Those are not considered in this article.
3. **A system in place for regularly reviewing privacy agreements and practices, particularly as the rules and expectations surrounding OHTs continue to evolve.** This will enable OHTs to make sure that they remain nimble and PHIPA-compliant when generating the metrics that the Ministry requests. As those metrics change or are clarified over time, the kinds of information that OHTs need to collect may likewise change. By having a way of proactively addressing these changes and thinking through their implications for data sharing and analysis, OHTs will be able to respond to changes in Ministry requirements with agility and without compromising client privacy.

IV. Conclusion

The regulatory and operational landscape for OHTs will continue to evolve in the coming months. In time, OHTs and their stakeholders are likely to learn more about the expected metrics for assessing OHT effectiveness and the types of PHI and other data sharing likely to be required among OHT members, HIC and non-HIC alike. It is clear that there are many moving parts in the shift towards OHTs. While prospective OHTs await these announcements and impending changes, there are certain positive initial steps they can begin to take now.

Additional Resources

Governance Options: Getting Started and Evolving Towards Maturity (April 2019), which describes options for OHT governance;

Governance Best Practices for High Performing Health Provider Boards (August 2019), which describes governance best practices relevant to OHT participants;

Forming Ontario Health Teams: The Role of the Health Provider Board (August 2019), which provides guidance on core elements of an OHT governance framework in year one; and

Organizing an Ontario Health Team: Considerations when Creating a Governance Framework (September 2019), which outlines questions and considerations to guide the development of a governance model framework.

Authored by

Ira Parghi
Toronto
416.367.6458
iparghi@blg.com

About BLG

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

Borden Ladner Gervais