David Young Law
Compliance Bulletin

May 2015

Ontario's New Electronic Health Information Law – Impact on Existing EHR Networks

David Young

May 2015

In April 2013 the Ontario Government tabled Bill 78, the *Electronic Personal Health Information Protection Act, 2014* ("EPHIPA") amending the *Personal Health Information Protection Act, 2004* ("PHIPA") to add a new Part v.1, "Electronic Health Records". The government's stated goal for EPHIPA is to support better information sharing and coordination among the variety of complex health systems within Ontario. In the government's words, EPHIPA will establish enhanced privacy and security requirements for EHRs and will clarify the rules under which healthcare providers collect, use and disclose personal health information within shared EHRs.

The Bill progressed to second reading debate before the 2014 election was called. Recently, the Minister of Health and Long-Term Care, while commenting on proposals to address the issue of medical records snooping in healthcare institutions, stated that the Bill would be reintroduced, including increased penalties for privacy breaches (presumably not restricted to those involving electronic records).

As originally introduced, EPHIPA is intended to facilitate and enhance the security and privacy protections required in connection with EHR systems and thereby encourage and expedite the adoption of those systems generally within the province. It will be recalled that the establishment of a "single" province-wide EHR for all Ontario residents was the announced goal when the government created the Smart Systems for Health Agency, later to become eHealth Ontario. However, many pitfalls and hurdles at later, including some successes, Ontario *has moved* towards the adoption of a province-wide EHR system, but, as currently envisaged, not one that will involve a single EHR, or a single repository for all electronic health records for Ontario residents. Instead, we have progressed to what might be characterized as a network of "distributed" systems both category-specific (such as the OLIS Diagnostic Imaging Network) and regional (networks or "integration hubs" the main ones being Connecting GTA, Connecting Southwest Ontario, Connecting Northeast Ontario). In addition, we have a wide diversity of specific-focus "networks" ranging from a small number of participants situated within local health care catchment areas to diverse participants across the province who may or may not connect on a local basis.

Notwithstanding that the government's characterization of the legislation as providing for a "safe and secure EHR" (suggesting a single record), significantly, EPHIPA supports the evolving distributed EHR

systems. Understanding how EPHIPA will impact and be integrated within the current EHR systems is important for the future development of those systems.

The framework proposed by EPHIPA builds on the distributed networks and enhances the legal rules already contained within PHIPA in a manner that at once represents a consistent progression of these systems towards the goal of a province-wide and universally-adopted EHR system as well as adding certain key functionalities designed to ensure that such a universal system both functions effectively and provides individuals with the option to withdraw their information from the EHR system. In sum, the key distinguishing characteristic of the EPHIPA model is that it contemplates continuance of the distributed EHR framework as we know it and, at least in the foreseeable future, is not intended to serve as the underpinning of a single province-wide EHR.

The distributed framework involves a wide diversity of EHR systems – some province-wide such as the community care-focused *Community Integration* model and other locally- or regionally-based care-specific functions and/or institutions. Most if not all of the existing distributed EHR networks are based on a legal framework comprising one or more Data Sharing Agreements among health information custodians, providing for mutual obligations regarding privacy and security, and a Network Services Agreement, setting out the obligations of the organization providing hosting and other network services. How will these existing frameworks transition to the EHR framework contemplated by the EPHIA and is it contemplated that all existing networks will do so?

Prescribed Organizations –the successors to HINPs

To understand the potential transition of existing networks, it is necessary to understand certain key precepts of the EPHIPA and how they relate to the rules under the existing law as articulated within the contractual framework of the existing networks.

The focus of the EPHIPA is on the role and obligations of a "prescribed organization" – essentially the service provider providing the electronic health records database and, potentially, the connecting systems enabling communication of EHRs the health information custodians using its services. Under PHIPA in its current form, these service provider organizations are the "health information network providers" (or "HINPs" established pursuant to section 6 of the PHIPA Regulations. These regulations, HINPs prescribe minimum standards/procedures/requirements for HINPs (including security policies and procedures, logging of data accesses and transfers, conducting TRAs and PIAs, plain language descriptions of their services and their privacy and security protections, and obligations for notification of data breaches). As well, HINPs must have in place agreements with the custodians for which they provide services, describing those services as well as the security safeguards that they have in place; this agreement requirement is typically satisfied by the Network Services Agreement.

A review of the key operational/compliance requirements that EPHIPA lays down for POs shows that for the most part they are not new, but are consistent with the existing HINP requirements under PHIPA. The EPHIPA provisions build on these HINP requirements, creating a more detailed code, adding provisions respecting consent directives and making the PO's full privacy and security framework subject to a tri-annual audit by the Information and Privacy Commissioner. In addition, significantly, EPHIPA contemplates the Ministry of Health and Long-Term Care stipulating minimum standards for privacy and security systems for the EHR networks – a power that is not contained within the current PHIPA. Apart from the addition of rules responding to consent directives, the power to stipulate minimum practices, procedures and safeguards respecting privacy and security represents EPHIPA's most significant change to the existing law. This continuity will be helpful in transitioning from the existing HINP regime to the PO regime contemplated by PHIPA, although it can be anticipated that the ministerial power to stipulate rules respecting privacy and security may lead to more stringent requirements meeting a Province-wide unified standard.

Presumably, given the potential for more rigorous compliance requirements, the designation of POs will result from a negotiated process between the government and service provider organizations who are candidates for the designation. It can be anticipated that the three key regional integration networks currently supported by E health Ontario likely will be among the first POs designated. What is not clear is whether the government intends to move proactively to designate other regional or category-specific EHR Networks. To the extent that this is the intention, significant discussions can be contemplated addressing the timing and expectations with respect to any such transitions.

Refinements to PHIPA

In addition to understanding the transition from the current HINP regime EPHIPA's PO regime, it is useful to note EPHIPA's adjustments to some of the defined terms and relationships as currently stipulated with in PHIPA. In essence, EPHIPA's stipulations largely clarify what can be understood as recognized precepts within PHIPA – collection, use, and disclosure of personal health information –in their application to the EHR regime. So, for example, EPHIPA states that a health information custodian that provides personal health information to the EHR is not considered to have "disclosed" that information to the EHR and that a disclosure only occurs when that information is accessed by another custodian. This concept is consistent with PHIPA and privacy law precepts generally that consider provision of personal information by a custodian to a service provider (HINP; PO) not to be a disclosure, but a continued use by that custodian, and that disclosure only occurs when the HINP provides access to a second custodian (typically one that is part of the EHR network provided by the HINP). This approach maintains the basic privacy law distinctions between a "data collector" (a HIC under PHIPA) and a "service provider", the latter being understood to perform functions/services as an agent on behalf of a data collector. These amendments to the defined terms are paralleled by substantive rules making clear that providing PHI to at PO is not a disclosure to, or collection by, the PO. Note: the logical approach

reflected in these provisions regarding collection/use/disclosure under EPHIPA are muddied a bit since the legislation seems to enable a PO to collect certain personal health information – specifically an individual's health number (section 34 (2) (e)).

Impact of EPHIPA on network agreements

What impact will EPHIPA have on existing EHR/data sharing networks? This is a potentially complicated question that bears a separate, more focused analysis. However, certain key considerations may be noted here. To be understood, is that EPHIPA will only impact directly networks in which the system service provider (i.e. HINP) is designated as a PO. However it can be expected that EPHIPA's more comprehensive (and potentially more rigorous) requirements for POs eventually will become adopted as recognized standards for EHR even in networks not formally subject to the PO obligations.

As noted, EPHIPA can be viewed as a transition of obligations currently met by HINPs to the more rigorous and detailed code required to be met by POs. Does this eliminate the need for Network Services Agreements between a PO and participants in the network? As currently understood, EPHIPA does not stipulate this requirement. It may be posited that the current HINP requirement for agreements (s. 6, PHIPA regulation) may reasonably be satisfied by the more explicit provisions of EPHIPA. However one can envisage there to be an appropriate role for a Network Services Agreement under the PO framework. Firstly, on some basis, there will need to be a commitment/agreement by the PO to provide the network services. This commitment would necessarily involve a description/statement, or reference to a roles and responsibilities document, setting out not only the obligations of the PO but also the responsibilities of the participants toward the PO. Finally and not unimportantly, the respective liabilities and, as appropriate, limitations on those liabilities, of the PO and the participants should be addressed in an agreement.

Will there continue to be a role for DSAs within the EPHIPA regime? It should be remembered that DSAs are entered into among the participants of a network and typically do not include the HINP (unless it is also a participant). They address not only the basic "agreement" to share data but also the mutual obligations between participants to protect that data, as well as any liability limitations and indemnity obligations among the participants. While the enhanced obligations under EPHIPA may give network participants confidence that their data will be protected within the EHR hosted by the PO, this protection does not extend to data when shared with (i.e. as received by) another participant. Furthermore, the EPHIPA contains no provisions addressing potential liability limitations or indemnity among the participants.

In sum therefore, it can be envisaged that, at least within the environment currently sketched out by EPHIPA, the contractual framework including obligations and responsibilities as are currently set out

within, or provided for by, NSAs and DSAs, will continue to be relevant for EHR networks governed by EPHIPA's rules.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.