Eastern Health

Round 3 Submission to the PHIA Review Committee

March 2017

TABLE OF CONTENTS

A. EXECUTIVE SUMMARY

Eastern Health's Round 3 submission to the PHIA Review Committee puts forth a response to some of the items identified in the submissions provided in Round 1. The following items being responded to are:

- Inclusion of a mandatory Privacy Impact Assessment provision;
- Reduction regarding release of information timelines;
- Breach reporting and notification;
- Removal of Memorial from PHIA; and,
- Voluntary oversight mechanism.

Eastern Health, as the largest custodian in Newfoundland & Labrador, appreciates this opportunity to put forth this response.

B. ADVANCING THE CONVERSATION

B.1. PRIVACY IMPACT ASSESSMENT

Issue: Inclusion of a Privacy Impact Assessment provision.

A Privacy Impact Assessment ("PIA") is a formal risk management tool used to identify the actual or potential effects that an activity or proposal may have on an individual's privacy. PIAs also identify ways in which adverse privacy risks can be managed. A PIA is desirable when assessing the following types of risks in health care:

- Risks arising from a new technology or the convergence of existing technologies;
- Risks arising from the use of a known privacy-intrusive technology in new circumstances (e.g. radio frequency identifiers or some implantable medical devices); and/or
- Risks arising from a new project or from changing information handling practices with significant privacy effects (e.g. providing access to multiple disparate information systems to new user groups through an integrated viewer).

PIAs are to be completed whenever personal information or personal health information ("Information") is being collected, used, or disclosed in a given program, project, or system.

At Eastern Health, PIAs are already an integral part of an established and thorough privacy review process. Departments looking to implement or update an existing process wherein Information is collected, used, disclosed, or retained complete a PIA and submit it to the Regional Manager, Access and Privacy ("Manager"), Information Security and Privacy ("ISP") Office. Upon receipt of the completed PIA, the Manager reviews the PIA, consults with the requesting department as required, and then writes a report on the analysis of the PIA (or consultation). The analysis, which forms the basis of the report, is done in accordance to the ten (10) fundamental privacy principles. The report identifies any privacy-related issue, assigns a risk level to that issue, and puts forth a possible mitigation strategy. The report is reviewed by the Regional Director ("Director") of the ISP Office. The Manager and Director, once the report is finalized, sign the report, and provide a copy of the signed report to the requesting department for their records.

A proposed change in a Round 1 submission was that the revised PHIA include a provision that PIAs become not only mandatory but that such PIAs also be reviewed by the OIPC. Such a provision may add a level of complexity and lead to time delays. Not every project requires a full PIA; rather, in

some situations a Preliminary Privacy Impact Assessment (PPIA) is all that is needed. For example, the Human Resources department ("HR") recently revised its process to facilitate employee performance appraisals wherein it moved from a paper-based system to an electronic system. The type of personal information collected and how it was used was not changing; everything remained the same. The only thing that changed was the process by which the performance appraisals were conducted. This is one such project where a PPIA was sufficient. If the suggested provision were implemented, the HR project would have required a complex privacy review that may have resulted in delays. It is worthy to note that, at Eastern Health, even when a PPIA is submitted, the report process outlined above is still followed.

Additionally, a mandatory review by the OIPC may extend timelines. Eastern Health is continually looking to improve and make more efficient the ways in which it provides patient care and delivers health services, and as such a large number of PIAs are completed annually at Eastern Health. In the fast-paced and ever changing environment that is health care, delays in making necessary and worthwhile changes to a program could negatively impact health care operations, and requiring that PIAs be reviewed by the OIPC could result in delays. The proposal did not impose timelines on how long an OIPC review would take, nor did it stipulate obligations regarding feedback provided pursuant to an OIPC review. Many custodians currently have dedicated privacy-trained employees who are diligent at reviewing and providing comment on privacy-related matters.

Lastly, in the event that PIA completion does become mandatory, it is best that it be applicable to all custodians. Custodians, as named in PHIA, regardless of size, should follow any PIA completion requirement.

B.2. RELEASE OF INFORMATION TIMELINES

Issue: Reduction in the timelines to process a release of information request.

When someone is looking for their Information at Eastern Health, it is considered a release of information request ("ROI"). The ISP Office processes ROIs, which are initiated by a variety of sources including but not limited to patients, lawyers, insurance companies, and the police. Under PHIA, a maximum time of 60 days is permitted to respond to ROIs. The resources available within Eastern Health are currently functioning near this level.

Eastern Health receives and responds to a large volume of, and often complex, ROIs, and has a compliment of dedicated employees who work diligently to process ROIs in a timely and efficient manner. A decrease from 60 days may lead to unattainable timeframes or an increase in required resources. A timeframe of 60 calendar days would be optimum.

B.3. BREACH REPORTING AND NOTIFICATION

Issue: Impact on custodians with increase in breach reporting and notification.

Notification regarding privacy breaches is beneficial, in that it better informs and protects individuals who may be the subject of a privacy breach, and it highlights to a custodian the importance of adhering to the requirements to protect privacy. Currently in the event of a material privacy breach, notification to both the person who is the subject of the Information and the OIPC must occur.

Eastern Health diligently adheres to the current requirements of PHIA and makes every effort to complete the notification process in a reasonable time period. Under the current wording, the OIPC is to be notified when a privacy breach is deemed to be material "…as per the regulations…" Section 5 of the Regulations outlines a number of criteria to be used to determine if a breach is material in nature. However, this results in a latitude of discretion with respect to determining when a breach is material. Improving the definition of material in the regulations may reduce this level of latitude in discretion. An improved definition can lead to improved privacy and human resources practices. The consistent approach will provide a standard methodology to custodians when processing material breaches.

Additionally, the current national climate regarding breach notification is to notify when it has been determined there is risk of serious harm. Given PHIA requires notification in the event of a material breach, current practices are harmonized with the national practices and requirements. We believe that modifying PHIA to address the issues regarding the definition of material breach will better enable custodians to remain consistent.

B.4. REMOVAL OF MEMORIAL AS A CUSTODIAN

Issue: Memorial's view that students, during a placement, act on behalf of a custodian.

It is Memorial's view that students, when accessing or using Information while on the premises of a custodian, do so on behalf of the custodian and not Memorial. Their submission purports that students are part of the circle of care for a patient and as such, are under the supervision of the attending practitioner who is the responsible member of the circle of care. Depending on the academic program, however, students are under the supervision of a faculty member during the tenure of their placement with the custodian, and while the faculty member may have a cross appointment between Memorial and the custodian, at the point of supervision – and by extension, dealing with any disciplinary measure bestowed the student – the supervisor is acting under the purview of their faculty member responsibilities. This means that the faculty member may be privy to Information, which could be considered a collection and use of Information by Memorial.

Memorial submits that Information is better protected if the student is acting on behalf of the custodian. The concern with this view is that students coming to a custodian are doing so in order to complete a requirement for their particular education program and not so much as a requirement of the custodian. There is a difference between someone coming at the request of the custodian as opposed to the custodian permitting someone come to them. The duties and responsibilities, which are set primarily by the academic program, of a student are diminished from those of an employee of the custodian. In the event there is an issue with the student requiring disciplinary measures, the custodian's involvement with such could be impacted (e.g. a student's tenure with the custodian is program-dependent, a student is not an employee of the custodian, etc.).

Additionally, if a student is required, as part of their program, to write a report (or some other academic task) based on their experiences, it is plausible that the report may contain some level of Information. Such a report would be submitted to the academic institution for grading. So, while the academic institution is collecting Information, it is, albeit, a more of an indirect manner but such ought to be treated the same way we treat Information collected by a custodian.

B.5. VOLUNTARY OVERSIGHT MECHANISM

Issue: Logistics of having a voluntary oversight mechanism.

A third-party organization, according to their submission, is planning to conduct research in Newfoundland and Labrador on genetic information derived from biological samples provided by residents of Newfoundland and Labrador. Such Information collected in the purview of research is just as sensitive as that Information collected in the clinical setting, and needs to be held to the same rigors as Information collected in a clinical setting. The proposal is requesting a voluntary oversight mechanism, but there are concerns that such approach may result in confusion and ambiguity. How would a voluntary oversight mechanism work? Would such a mechanism permit an organization to determine, at their discretion, when to collaborate with the OIPC? What about participants whose Information with is breached, with a voluntary oversight mechanism, what definitive recourse or options would they have available?

Implementing the option for a voluntary oversight mechanism presents for an environment where there could be an uneven application of PHIA to organizations that collection, use, disclose, or retain Information. The OIPC is an important and beneficial oversight body. Through collaboration with them, custodians have been able to enact measures and promote appropriate standards to reduce the risk of harm that may accompany the collection, use, disclosure, and retention of Information. For the protection of the Information of the people of Newfoundland and Labrador, it is critical that any measure to monitor and assess organizations that collect, use, disclose, and retain Information be equally applied to all organizations.

C. SUMMARY

The *Personal Health Information Act* (PHIA) has proven to be very beneficial in aiding in the protection of Information. Improvements will, once implemented, impact all custodians (e.g. private physician, physiotherapy, etc. clinics) and patients. It is beneficial that consideration be given to the impact on custodians and patients that any changes made may have.

Eastern Health thanks the PHIA Review Committee for the opportunity to make this submission to advance the conversation. We take our responsibility as a custodian of Information very seriously. We are committed to, and will continue to exceed, our responsibilities with privacy legislation.