Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

LEGISLATIVE UPDATE

May 2024

Backgrounder
Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*

Context

On May 13, 2024, the provincial government tabled Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (Bill 194). This Bill is intended to provide new tools to prevent and respond to cyber security threats in the public sector, lay the foundation for the ethical use of artificial intelligence (AI) in the public sector, and expand privacy protections for personal information. The Bill applies to all public sector entities, including hospitals, and, if passed, would enact the *Enhancing Digital Security and Trust Act, 2024* (EDSTA) and amend the *Freedom of Information and Protection of Privacy Act, 1990* (FIPPA).

For further information on Bill 194, please refer to the government's news release here.

Key Highlights

Schedule 1 of Bill 194 would enact the EDSTA, which primarily sets out new regulation-making and directive-issuing authority with respect to:

- The development and implementation of cyber security programs by public sector entities as well as required reporting on such programs;
- The provision of information to the public about a public sector entity's use of AI;
- The development of an accountability framework for a public sector entity's use of AI;
- Prohibited and allowed uses of AI systems; and
- Oversight, risk management, and disclosure requirements for public sector entities that use AI.

Schedule 2 sets out proposed amendments to FIPPA, which include:

- Adding reporting and record-keeping requirements related to thefts, losses or unauthorized uses or disclosures of personal information;
- Requiring a written privacy impact assessment (PIA) to be prepared before an entity collects personal information;
- Adding requirements for safeguarding collected personal information;
- Expanding the authority of the Information and Privacy Commissioner (IPC) by enabling the IPC to conduct reviews and administer orders; and
- Providing protection to whistleblowers who report privacy wrongdoing to the IPC.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

The EDSTA also proposes new regulation-making and directive-issuing authority with respect to digital information and technology relating to minors, however, these provisions only apply to children's aid societies and school boards and will not be addressed further in this Backgrounder.

I. Cyber Security

The EDSTA, if enacted, would empower the government, specifically the Lieutenant Governor in Council (LGIC), to make regulations governing cyber security for prescribed public sector entities.[1] These regulations may require public sector entities to develop and implement programs for ensuring cyber security and may outline specific requirements for such programs, including:

- Required roles and responsibilities;
- Reporting on the public sector entity's progress in ensuring cyber security;
- Cyber security education and awareness;
- Response and recovery measures for cyber security incidents; and
- Oversight measures for the implementation of the program.

The LGIC would also be able to enact regulations that require public sector entities to submit cyber security incident reports to the Minister of Public and Business Service Delivery (Minister). The form and frequency of these incident reports would be set out in regulation.

Finally, with respect to cyber security, the EDSTA gives the Minister the power to make regulations setting technical standards and issue cyber security directives. The Minister's directive-issuing authority is very open-ended and directives may be general or particular in application.

Commentary:

The cyber security provisions of Bill 194 will not automatically come into effect upon the Bill receiving Royal Assent, as they require proclamation by the LGIC to come into effect, which may occur at a later date. Additionally, the specific implications of these provisions, including which public sector entities will be prescribed and required to comply with such provisions, will not be known until regulations under the EDSTA are enacted and/or the Minister issues directives.

II. Artificial Intelligence

Similar to the proposed cyber security provisions, the EDSTA would also empower the LGIC to make regulations relating to AI and the Minister to make regulations setting technical standards on AI, both of which would be applicable to prescribed public sector entities. Bill 194 proposes the following very broad definition of AI, which may also be expanded by regulation:

[1] "Public sector entity" is defined in the EDSTA to mean an institution within in the meaning of the *Freedom of Information and Protection of Privacy Act* (which includes hospitals), an institution within the meaning of the *Municipal Freedom of Information and Protection of Privacy Act*, a children's aid society and a school board.

> "a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments."

Prescribed public sector entities would be required to provide information to the public about the entity's use of AI, develop and implement accountability frameworks for the use of AI, take prescribed steps to manage risks associated with AI, which may include reporting and record-keeping, and name an individual to be responsible for the oversight of the entity's use of AI and the entity's compliance with prescribed disclosure requirements. Details with respect to disclosure requirements, accountability frameworks and oversight, as well as any allowed and prohibits uses of AI will be set out in regulation.

Commentary:

Please refer to the commentary above on the proposed cyber security provisions, which is also applicable to the proposed AI provisions in the EDSTA, with the exception of the reference to Ministerial directives, as the Minister would not be afforded directive-issuing authority with respect to AI.

III. FIPPA Amendments

Schedule 2 of Bill 194 introduces several significant amendments to FIPPA which aim to modernize the Act and enhance privacy protections for personal information across the public sector. These amendments relate to breach reporting and notice requirements, privacy impact assessments (PIA), safeguarding requirements, IPC authority to conduct reviews and administer orders, and whistleblower protection.

Commentary:

FIPPA and the proposed amendments set out in Bill 194 relate specifically to "personal information," as defined in FIPPA. FIPPA does not apply to "personal health information" (PHI), as defined in the *Personal Health Information Protection Act, 2004* (PHIPA), unless expressly referenced in subsection 8(2) of PHIPA. The proposed amendments to FIPPA in Bill 194 would not be applicable to PHI and will only impact a hospital's obligations with respect to personal information. Please see the Appendix for the definitions of personal information and PHI.

Several of the proposed privacy requirements in Bill 194 are similar in nature to requirements set out in PHIPA for PHI. However, as will be discussed in more detail below, there are some notable differences between PHIPA and the proposed FIPPA requirements. If Bill 194 is passed, hospitals will need to have clear processes in place to ensure that the PHIPA requirements are appropriately complied with when dealing with PHI and the FIPPA requirements are complied with when dealing with personal information.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

Breach Reporting and Notice Requirements

Bill 194 would introduce reporting and notice requirements relating to the theft, loss or unauthorized use or disclosure of an individual's personal information. If such a breach occurs, a report to the IPC and notice to the affected individual is required if there is reason to believe there is a real risk of significant harm (RROSH) to an individual as a result of the breach. The head of the institution[2] where the breach occurred will be responsible for submitting a report, in the prescribed form with the prescribed information, to the IPC as soon as feasible after determining the breach has occurred. Additionally, a record must be kept by the institution of any theft, loss or unauthorized use or disclosure of an individual's personal information that is reported to the IPC.

The head of the institution must also notify the affected individual of the breach as soon as feasible after determining the breach has occurred. The notice must be in the prescribed form with the prescribed information and must contain a statement that the individual is entitled to make a complaint to the IPC.

In determining whether there is a RROSH, the following factors should be considered:

- The sensitivity of the personal information;
- The probability that the personal information has been, is being or will be misused;
- The availability of steps that the individual could take to reduce the risk of harm occurring or mitigate the harm that does occur;
- Any direction, recommendation or guidance provided by the IPC with respect to what constitutes RROSH; and
- Any other prescribed factor.

Commentary:

The proposed reporting and notice requirements under FIPPA have a higher threshold for when reporting and notice is required than what is set out in PHIPA for PHI breaches. Any time PHI is stolen, lost or used or disclosed without authority, the health information custodian (HIC) must notify the affected individual, as there is no RROSH or other threshold that must be met. Similar to the proposed FIPPA requirement, notice must be provided at the first reasonable opportunity and the notice must include a statement that the individual is entitled to make a complaint to the IPC.

A report of the theft, loss or unauthorized use or disclosure of PHI to the IPC is only required in the prescribed circumstances set out in section 6.3 of Ontario Regulation 329/04 (General) under PHIPA, but notably these circumstances are significantly broader than the RROSH threshold. The report to the IPC must be made at the first reasonable opportunity.

Institutions subject to FIPPA are required to submit an annual report to the IPC. Bill 194 would require the number of thefts, losses or unauthorized uses or disclosures of an individual's personal

[2] For a hospital, the head of the institution is the Chair of the Board of Directors of the hospital. This authority is usually delegated to a lead FOI or privacy officer.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

information that an institution recorded in the previous calendar year to be included in the annual report.

Commentary:

Hospitals are already required to submit two annual reports to the IPC, one pursuant to FIPPA that addresses personal information and one pursuant to PHIPA that addresses PHI. The annual report pursuant to PHIPA requires similar breach reporting with respect to PHI that is proposed by Bill 194 with respect to personal information. If Bill 194 is passed, hospitals will have to ensure that each annual report provides the correct type of privacy breach information.

Privacy Impact Assessments

Another new requirement that Bill 194 would introduce for institutions is the preparation of a written PIA before personal information is collected. A PIA would have to contain the following information:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.

2. The legal authority for the intended collection, use and disclosure of the personal information.

3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.

4. The sources of the personal information that is intended be to collected.

5. The position titles of the officers, employees, consultants or agents of the institution who will have access to the personal information.

6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.

7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40(1) of FIPPA.

8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 40(5) of FIPPA and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.

9. The steps to be taken by the institution,
    i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    ii. to mitigate the risks to individuals in the event of such an occurrence.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

10. Such other information as may be prescribed.

Institutions would also be required to update a PIA and implement any risk mitigation steps outlined in the updated PIA before making any significant changes to the purpose for which personal information is used or disclosed.

Commentary:

Hospitals currently are not required to prepare PIAs under FIPPA or PHIPA, however, many hospitals already do so with respect to PHI. If Bill 194 is passed, hospitals will have to expand this practice to personal information and ensure the personal information PIAs include the required information and are updated in accordance with the formalized rules set out in FIPPA.

Safeguarding Requirements

Bill 194 would add the formal requirement for institutions to take reasonable steps to ensure that personal information in the institution's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing personal information are protected against unauthorized copying, modification or disposal.

Commentary:

The proposed safeguarding standard set out in Bill 194 for personal information is identical to the standard set out in PHIPA with respect to PHI.

IPC Authority and Whistleblower Protection

Bill 194 would expand and formalize the powers of the IPC. If passed, the Bill would allow the IPC to conduct complaint-based and proactive reviews of an institution's information practices.[3] Proactive reviews could be conducted if the IPC had reason to believe that the requirements of FIPPA were not being complied with. After conducting a review and providing the institution with an opportunity to respond, the IPC would be able to issue compliance orders such as requiring an institution to discontinue or modify an information practice, implement new practices, or make any other change it considers necessary to bring the institution into compliance with FIPPA.

Bill 194 additionally would introduce a new whistleblower protection. The IPC would be required to keep the identity of whistleblowers confidential, if confidentiality is requested by the whistleblower.

[3] "Information practices" is defined in Bill 194 to mean the practices and procedures of an institution for actions in relation to personal information, including (a) when, how and the purposes for which the institution collects, uses, modifies, discloses, retains or disposes of personal information, and (b) the administrative, technical and physical safeguards and practices that the institution maintains with respect to protection the information.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

Commentary:

The IPC already has formalized review and order-making authority with respect to PHI pursuant to PHIPA. Some noteworthy differences between the IPC's powers under PHIPA and the proposed powers under FIPPA are the following. PHIPA provides greater clarity as to what powers the IPC has in conducting a review, such as its inspection powers and powers to demand the production of documents or other materials. PHIPA also provides that documents or things produced in the course of a review are privileged in the same manner as if the review was a proceeding in court, whereas the proposed amendments to FIPPA do not set out any privilege or confidentiality requirements with respect to materials produced in the course of a review.

Another notable difference in the IPC's powers is that PHIPA enables the IPC to order administrative monetary penalties (AMPs), whereas the proposed amendments to FIPPA would only enable the IPC to make orders that are reasonably necessary to achieve compliance with FIPPA, which would not include AMPs.

With respect to whistleblowers, PHIPA does not have the same confidentiality requirement as proposed for FIPPA, however, it does set out a prohibition on retaliation against whistleblowers that is not proposed for FIPPA, which prohibits dismissing, suspending, demoting, discipling, harassing or otherwise disadvantaging the whistleblower.

Timeline and Next Steps

Bill 194 is currently at Second Reading in the Legislature. If the Bill receives Royal Assent, the EDSTA as well as the majority of the amendments to FIPPA will not come into effect until they are proclaimed into force by the LGIC. Additionally, as noted above, the implications of the EDSTA will be dependent on what requirements are subsequently set out in regulation or Ministerial directive(s).

The OHA will continue to monitor developments related to Bill 194 and will provide further updates as they become available. If you have any questions or wish to share feedback on the Bill, please contact *Ashley MacDougall, Legal and Policy Advisor,* at amacdougall@oha.com.

Ontario Hospital Association

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

LEGISLATIVE UPDATE

Appendix

Definition of "personal information" pursuant to FIPPA:

2 (1) "personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

Definition of "personal health information" pursuant to PHIPA:

Personal health information

4 (1) In this Act,

"personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,

(c) REPEALED: 2020, c. 13, Sched. 3, s. 8 (7).

(c.1) is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the *Connecting Care Act, 2019*,

200 Front Street West, Suite 2800
Toronto, ON M5V 3L1
416 205 1300
oha.com

(d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,

(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,

(f) is the individual's health number, or

(g) identifies an individual's substitute decision-maker.

Identifying information

(2) In this section,

"identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Mixed records

(3) Personal health information includes identifying information that is not personal health information described in subsection (1) but that is contained in a record that contains personal health information described in that subsection.

Exception

(4) Personal health information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if,

(a) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; and

(b) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.