Office of the Information and
Privacy Commissioner of Alberta

February 27, 2014

Honourable Fred Horne
Minister of Health
208 Legislature Building
10800 – 97 Avenue
Edmonton, AB T5K 2B6

Dear Minister Horne,

Re: Proposed Amendments to the *Health Information Act* – Mandatory Breach Reporting and Notification

Further to public comments I made in January 2014, I am writing to formally request the Government of Alberta consider amending Alberta's *Health Information Act* (HIA) to include mandatory breach reporting and notification provisions.

Breach reporting and notification requirements in health privacy legislation in other jurisdictions

In Canada, nine jurisdictions have passed or introduced broadly focused health privacy legislation.[1] Of these, six include mandatory privacy breach notification and/or reporting requirements.

- Ontario: health information custodians must notify affected individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons.

- New Brunswick: a custodian must notify affected individuals and the Commissioner at the first reasonable opportunity if personal health information is stolen, lost, disposed of or disclosed to or accessed by an unauthorized person.

- Nova Scotia: health care custodians are required to notify affected individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons. If a custodian decides not to notify individuals, the custodian is required to notify the Review Officer (regulatory authority).

- Newfoundland and Labrador: health care custodians are required to notify affected individuals at the first reasonable opportunity where the information is stolen, lost, disposed of or disclosed to or accessed by an unauthorized person. If the custodian believes there has been a material breach, the custodian must inform the Commissioner. The Commissioner may recommend that the custodian, at the first reasonable opportunity, notify the affected individuals.

[1] Jurisdictions that have health privacy legislation in force include Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador. Yukon Territory passed legislation in 2013 that is not yet in force. Also in 2013, Northwest Territories introduced Bill 4 – Health Information Act. The Bill has passed second reading.

- Yukon: where there are reasonable grounds to believe that an individual is at risk of significant harm, a custodian must, as soon as reasonably possible, notify the affected individual. The custodian must provide the Commissioner with a copy of the notice within a reasonable time.

- Northwest Territories: a health information custodian must notify an affected individual as soon as reasonably possible if personal health information is used or disclosed other than as permitted by the legislation, lost or stolen, or altered, destroyed or otherwise disposed of without authorization.

Alberta's *Health Information Act* does not include privacy breach reporting and/or notification requirements as exist or have been introduced in these six jurisdictions.

Breach reporting and notification requirements in Alberta

I support the concept of mandatory breach notification and reporting in Alberta's private, public and health sectors. At this time, however, only Alberta's private sector law, the *Personal Information Protection Act* (PIPA) requires organizations to report a privacy breach to my Office where the organization determines there is a real risk of significant harm to an individual. PIPA also gives me the power to require an organization to notify affected individuals.

In my July 2013 submission to the Government of Alberta's Review of the *Freedom of Information and Protection of Privacy Act* (the FOIP Act), I recommended the FOIP Act be amended to "[r]equire public bodies to report privacy incidents meeting certain criteria to my Office and giving me the power to require public bodies to notify affected individuals." I recommend that similar amendments be considered for health custodians under the HIA.

Considerations when legislating breach reporting and notification

While there is general global agreement that mandatory breach notification and reporting can be an important component in protecting privacy, there are a number of issues that should be considered in designing an appropriate legislative scheme.

- **Who should be notified about the breach? Who should decide whether or not to notify?** The primary purpose of data breach notification and reporting is to ensure that affected individuals are informed of incidents so that they can take steps to protect themselves against harms such as identity theft and/or fraud. Other purposes include providing an incentive for regulated entities to implement safeguards, maintaining confidence in data protection laws, and obtaining information about the scope and frequency of privacy breaches with an eye to preventing them.

  To achieve these purposes, some data protection laws require that regulated entities notify affected individuals; others require that they notify a regulatory authority; still others require that they notify both affected individuals and the regulatory authority. In all cases, the responsibility to notify rests with the regulated entity.

  Alberta's PIPA requires that organizations notify me of a reportable incident, and gives me the power to require that the organization notify affected individuals. In practice, most organizations have already notified affected individuals on their own before reporting an incident to my Office.

I am not aware of any data breach reporting/notification laws that require the general public be notified of a privacy breach. As stated earlier, the primary purpose of notification is to enable individuals affected by a breach to take steps to protect themselves.

- **What are the triggers for notification? Will every breach require notification and/or reporting, or just those meeting certain criteria?** Requiring all breaches to be reported in every case can place undue burdens on the entities subject to the legislation and increase the risk of notification fatigue on individuals. Some breaches are minor and present no risk of harm to affected individuals. Therefore, a requirement to report every privacy breach may not be an effective or practical solution.

  Instead, many data protection laws identify a "trigger" for notification, or set out criteria for reporting/notifying. Alberta's PIPA, for example, requires that organizations report incidents to me "where a reasonable person would consider there is a real risk of significant harm." Other data protection laws propose or include triggers based on different thresholds for harm (e.g. "material breach of safeguards" or "risk of unauthorized disclosure"), the number of affected individuals, or the sensitivity of the information.

- **What should be reported (content and method of notification) and in what time frame?** Data protection laws vary considerably in terms of setting out the specifics of what should be included in a report to a regulatory body and/or a notification to affected individuals. Alberta's PIPA Regulation is specific as to both the content of a notice to me (s. 19), and a notification to individuals (s. 19.1).

  In terms of the method of notification (e.g. letter, email or telephone; direct notice vs. substitute notice), some data protection laws are general (e.g. notice should be in an "appropriate" form), and others are more specific. Alberta's PIPA Regulation requires that notice to me be "in writing" and include specific information set out in the Regulation. The form of notification to affected individuals, however, is not prescribed although the notification must include specific information set out in the Regulation (e.g. a description of the circumstances of the breach, the personal information involved, steps taken to reduce harm, etc.). Under PIPA, affected individuals must be notified directly unless I determine this would be unreasonable in the circumstances. As a general rule, this Office has only rarely authorized indirect notification (i.e. through a public notice) in circumstances where direct notice was not possible (e.g. the organization does not have contact information for the affected individuals). In almost all circumstances, direct notice to affected individuals has been the preferred approach.

  With respect to timing, section 34.1(1) of PIPA requires that an organization notify me of a reportable incident "without unreasonable delay" and I have the ability to require that an organization notify individuals "within a time period [that I have] determined." As noted above, in practice, most organizations have already notified affected individuals before reporting the incident to my Office. In very rare cases, it may be advisable to delay notification if, for example, the matter is under police investigation and notifying affected individuals could harm the law enforcement investigation.

- **Should there be penalties, sanctions or other consequences for failing to notify?** Data protection laws vary widely in terms of penalties, sanctions or other consequences for failing to notify. In many jurisdictions, there is no legal requirement to notify either affected individuals or a regulatory authority and, as a result, there are no legal consequences under data protection laws for failing to do so. There may, however, be consequences under other laws (e.g. *Criminal Code,* etc.).

In those jurisdictions where there is a mandatory reporting/notification requirement, sanctions vary and could include administrative penalties, civil penalties and/or 'naming and shaming'. Under Alberta's PIPA, it is an offence for an organization to fail to notify me of a reportable breach. A person who commits an offence is liable to a fine of up to $10,000 (individual) or $100,000 (organization).

Closing Comments

I have enclosed a copy of World Law Group's publication *Global Guide to Data Breach Notifications, 2013* (http://www.theworldlawgroup.com/files/file/WLG%20Global%20Data%20Breach%20Guide-Final.pdf) which outlines many of the different models and approaches adopted by jurisdictions around the world in relation to breach notification and reporting laws. The variety of breach notification laws and obligations worldwide reflects the challenges and complexity in legislating breach notification and reporting.

Including privacy breach notification and reporting requirements in all three of Alberta's access and privacy laws is an important component of protecting Albertans' privacy rights and will help to put Alberta at the forefront of privacy protection. I commend the government for considering amendments to the *Health Information Act*, and would welcome the opportunity to consult on any proposed amendments.

I hope the above information is helpful. Please be advised that I will be posting this letter on my Office's website as part of my mandate under section 84(1)(c) to inform the public about the Act.

Yours truly,

Jill Clayton
Information and Privacy Commissioner

Encl.: *Global Guide to Data Breach Notifications, 2013*