Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2015-IR-01

Privacy breach reporting in Alberta's health sector

December 9, 2015

Alberta Health

Investigation H6002

Table of Contents

Commissioner's Message

This report presents the findings and recommendations from my office's investigation of privacy breach reporting in Alberta's health sector.

I announced this investigation in January 2014, following a significant health sector privacy breach involving a stolen laptop. I also wrote to the former Minister of Health recommending that mandatory breach reporting and notification provisions be considered for custodians subject to the *Health Information Act* (HIA).[1]

On May 14, 2014, Bill 12, the *Statutes Amendment Act,* was passed. Bill 12 amended the HIA, introducing mandatory breach reporting and notification requirements, and new offence provisions for failing to report a breach. The amendments to the HIA are not currently in force, but are awaiting supporting regulations.

As the HIA does not currently require health custodians to report breaches, this investigation was not a compliance investigation. Instead, the purpose was to obtain information about how breaches are currently managed, tracked and reported in Alberta's health sector and how prepared the sector is for mandatory breach reporting and notification.

Overall, the investigation found that practices vary widely and the health sector is not uniformly prepared. The large custodians we surveyed (Alberta Health Services, Alberta Health, Covenant Health) and members of specific regulated health professions (for example, physicians, pharmacists and nurses) generally have privacy breach management frameworks in place that will enable them to comply with new legislated duties and responsibilities. For many other health professionals, however, significant work will be required if they are to establish robust programs. Overall, considerable training and education is necessary to ensure custodians understand their breach reporting and notification obligations under the amended HIA.

The recommendations in this report are intended to strengthen privacy breach management and response in Alberta's health sector and assist with the implementation of mandatory breach reporting and notification. In particular, I would appreciate the opportunity to consult on the specific wording of amendments to the *Health Information Regulation* before they are enacted to clarify any concerns and minimize potential unintended consequences.

Jill Clayton
Information and Privacy Commissioner

[1] My February 27, 2014 letter to the Minister of Health is available on my office's website at www.oipc.ab.ca.

Introduction

[1] On January 23, 2014, the Information and Privacy Commissioner (the Commissioner) announced an investigation into how privacy breaches are reported and managed by the health sector in Alberta.

[2] The Commissioner opened the investigation on her own motion under section 84(1)(a) of the *Health Information Act* (HIA or the Act), which reads,

> 84(1) In addition to the Commissioner's powers and duties under Divisions 1 and 2 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may
>
> (a) at the request of the Minister or otherwise, conduct investigations to ensure compliance with any provision of this Act …

Application of the Health Information Act

[3] Alberta's HIA was enacted in 2001. The Act applies to "custodians", which includes (among others) Alberta Health, Alberta Health Services, Covenant Health, nursing homes, and regulated health services providers that are designated as custodians under the *Health Information Regulation*, namely, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists, and dental hygienists. The Act applies to more than 50,000 custodians.

[4] The HIA also applies to "affiliates" who are employed by or perform a service for a custodian, such as contractors, students and volunteers. Health services providers who exercise privileges to admit and treat patients at hospitals are also affiliates to the custodians who operate those hospitals, i.e. Alberta Health Services or Covenant Health. Custodians are responsible for the collection, use and disclosure of health information by their affiliates.

[5] Section 60 of the HIA requires custodians to take reasonable steps to maintain safeguards to protect the confidentiality and privacy of health information. This includes protecting against any reasonably anticipated threat to the security or integrity of health information or of loss of health information, or unauthorized use, disclosure, modification or access to health information. A breach of health information, or simply a privacy breach, is what is referred to when one of these threats materializes.

[6] While custodians have a duty under the HIA to protect health information, there is currently no requirement for custodians to report privacy breaches. Consequently, a custodian's failure to report a privacy breach is not a contravention of the HIA.

[7] On May 14, 2014, however, Bill 12, *The Statutes Amendment Act*, was passed. The legislation includes a number of amendments to the HIA, including a requirement that custodians notify individuals affected by a breach, the Minister of Health, and the Commissioner…

> …of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.

[8] The amendments also include new offence provisions for failing to report a privacy breach and failing to take reasonable steps to protect against a reasonably anticipated threat to the security or integrity of health information or of loss of health information.

[9] As of the time of writing, the breach reporting and notification amendments to the HIA are not in force. They will come into force on proclamation.

[10] Please see Appendix B for the full text of the amendments.

Objectives of the Investigation

[11] Between fiscal years 2010-11 and 2014-15, the Office of the Information and Privacy Commissioner (OIPC) received a total of 302 self-reported breaches from the health sector. As reporting a breach to the Commissioner is voluntary at this time, this total reflects only those privacy breaches reported to the OIPC and does not reflect all of the breaches that may have occurred within the health sector during those four fiscal years.

[12] Health information is sensitive. A privacy breach involving health information can have significant impact on affected individuals and may cause hurt, humiliation and embarrassment, as well as pose a risk of identity theft or fraud. In some circumstances, a health information breach can also create risk to personal safety for those affected.

[13] The HIA requires that custodians take steps to maintain safeguards to protect health information. This requirement is intended to minimize the risk that a custodian or one of its affiliates does not accidentally or inappropriately collect, use, disclose or lose health information. Properly implemented safeguards reduce, but do not eliminate the risk of a breach; breaches may still occur despite the reasonable steps taken to prevent them. Breach reporting and notification are intended to bring such incidents into the light, where they can be addressed by those responsible and those affected.

[14] Since there is no current requirement under the HIA for custodians to report breaches or notify individuals affected by privacy breaches, this is not an investigation of compliance with the HIA. Rather, the objectives of this investigation are to obtain information about the following:

1. How are health information privacy breaches managed by Alberta’s health sector?
2. What privacy breaches are tracked or reported by Alberta’s health sector?
3. How prepared is Alberta’s health sector for mandatory breach reporting and notification?
4. What recommendations may strengthen implementation of mandatory breach reporting and notification requirements by Alberta’s health sector?

Methodology

[15] The OIPC sent questionnaires to custodians, and entities that are not custodians but have significant roles within Alberta's health sector, to obtain a broad overview of the knowledge level and current practices with respect to management of privacy breaches. Some questions varied to reflect the custodians' or entities' respective roles and responsibilities within the health sector. Completing the questionnaire was voluntary.

[16] The custodians who received a questionnaire were: Alberta Health, Alberta Health Services (AHS), and Covenant Health. These are large-scale custodians who manage significant health information assets related to the management or delivery of health services in Alberta. AHS employs approximately 100,000 staff and Covenant Health employs approximately 10,000 staff. Alberta Health, while it does not employ such large numbers, is responsible for health system management and policy development, as well as being the information manager[2] for the Alberta Electronic Health Record (Netcare).

[17] It was not practical to send questionnaires to individual custodians (e.g. physicians, registered nurses, pharmacists, etc.). Therefore, the OIPC sent questionnaires to the eleven regulatory colleges[3] whose members are designated as custodians under the *Health Information Regulation*. All of the colleges responded to the questionnaire.

[18] Questionnaires were also sent to the faculties of medicine at the University of Alberta and the University of Calgary. The universities are not custodians under the HIA. They are "public bodies" under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act). However, the universities, particularly within their medical faculties, do employ health services providers who are custodians subject to the HIA.

[19] A questionnaire was also sent to the University of Calgary – Conjoint Health Research Ethics Board and the Health Research Ethics Board of Alberta (which includes the Alberta Health Innovates Community Health Committee, the Alberta Health Innovates Cancer Committee and the Alberta Health Innovates Clinical Trails Committee). Research Ethics Boards (REBs) perform a critical function in reviewing research proposals that involve health information in the custody or under the control of a custodian. Without an REB's approval, a custodian cannot disclose health information to a researcher for a research purpose. When assessing a proposal, the REB must review whether adequate safeguards to protect privacy and confidentiality will be in place when the research is carried out. REBs are not custodians under the HIA, but given their role under the HIA, the OIPC felt information from REBs would be helpful for this investigation.

[2] Section 66 of the HIA says an information manager includes a person or body that provides information management or information technology services. Section 2 of the *Electronic Health Record Regulation* designates Alberta Health as the information manager for the Alberta Electronic Health Record.

[3] We limited survey participation to professional regulatory colleges because these bodies have the power to direct their members through professional standards. Some health professions combine their professional association and regulatory college, whereas physicians and pharmacists have separate professional associations. Both the Alberta Medical Association and the Alberta Pharmacists' Association have written model HIA policies for their members, which include privacy breach response and training. The large majority of physicians and pharmacists use these model policies, which have been reviewed and accepted by the OIPC.

[20] A questionnaire was also sent to the Information Stewardship Office (ISO). The ISO is a "neutral office" established to provide support to the Information Sharing Framework Governance Committee that oversees and manages information sharing in an Electronic Medical Record (EMR) system between AHS and participating physicians under a Memorandum of Agreement between AHS and the Alberta Medical Association (on behalf of participating physicians). The ISO is not a custodian under the HIA, but is responsible for receiving and investigating complaints relating to breaches of privacy and security by the EMR custodians and their affiliates.

[21] A complete list of the custodians, regulatory colleges, universities, REBs and entities that responded to the questionnaires is appended to this report.

[22] The OIPC considered a number of elements (such as policies, breach management and response protocols, training and education requirements and service provider management) in reviewing the current state of privacy breach reporting by Alberta's health sector.

[23] These elements are part of the "building blocks" or "baseline fundamentals" for a privacy management program set out in a guidance document entitled *Getting Accountability Right with a Privacy Management Program*. The guidance document was jointly released by the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia in April 2012. While the guidance document was written from the perspective of private sector privacy legislation, the elements for safeguarding/protecting privacy can also be applied to the health sector. A copy of the document is available at www.oipc.ab.ca.

Review of Privacy Impact Assessments Submitted to the OIPC

[24] As previously noted, it was not practical to survey individual custodians. However, hundreds of custodians in independent practice have submitted Privacy Impact Assessments (PIAs)[4] to the OIPC since proclamation of the HIA in 2001. These PIAs include information about privacy policies, breach response and training. Many are based on templates provided by custodians' professional associations, such as the Alberta Medical Association and the Alberta Pharmacy Association. By reviewing these PIAs the OIPC is able to comment on many of the controls custodians say are in place to manage and respond to privacy breaches. The table below shows the number of PIAs submitted to the OIPC for review by custodians who are members of a regulated health profession:

Regulated Health Profession	PIAs Accepted	College/Association Templates Include Breach Response
Chiropractors	60	Yes
Pharmacists	744	Yes
Dentists	0	Yes

[4] PIAs under the HIA must be submitted to the Commissioner prior to a custodian implementing a new system or practice or making changes to an existing system or practice that may affect privacy. Custodians must address their overall management of privacy functions, including organizational structure and policies. The OIPC publishes guidelines, the *PIA Requirements*, to assist health custodians completing PIAs as part of their responsibilities under the HIA. The *PIA Requirements* include a table listing the policies that custodians should have in place, which includes incident management policies and training. A copy of the *PIA Requirements* is available on the OIPC website.

Regulated Health Profession	PIAs Accepted	College/Association Templates Include Breach Response
Registered Nurses	94	Yes
Denturists	0	No
Midwives	16	Yes
Opticians	0	Yes
Physicians and Surgeons	1,763	Yes
Podiatric Physicians	0	No
Dental Hygienists	1	No
Optometrists	0	No
Total	**2,678**	**N/A**

Current State of Privacy Breach Management in Alberta's Health Sector

1. Are there policies and/or breach and incident management response protocols regarding health information breaches in Alberta's health sector? Are the policies and/or protocols reviewed periodically?

Custodians:

- Alberta Health, AHS and Covenant Health say they have breach response policies in place and that the policies are periodically reviewed.

Regulatory colleges:

- Five out of the eleven regulatory colleges say they recommend a breach response policy to their members. Of these five colleges, four say they periodically assess the policy.

- Only three out of the eleven regulatory colleges recommend their members periodically assess their own breach response policy.

Universities:

- The University of Alberta and the University of Calgary have breach response policies that extend to their respective faculties of medicine. Both universities indicate they periodically review their policies.

REBs:

- The University of Calgary – Conjoint Health Research Ethics Board says it has a breach response policy, which is the University of Calgary's policy, and that the University of Calgary periodically reviews the policy. The Health Research Ethics Board of Alberta does not have a breach response policy.

Other entity:

- The ISO says it has a breach response policy and that it periodically reviews the policy. The ISO said its current policy "does not fully contemplate the May 2014 amendments" and that it is waiting for the publication of the regulations.

OIPC Comments

[25] The OIPC did not assess the policies and protocols referenced by questionnaire respondents. Instead, the purpose of this question was to assess the extent to which breach response policies and protocols are in place in the health sector.

[26] Section 60 of the HIA requires that a custodian take reasonable steps to maintain administrative, technical and physical safeguards to protect confidentiality and privacy. Policies, including a privacy breach response policy/protocol are an expected administrative safeguard required by the HIA. A privacy breach response policy/protocol confirms organizational commitment that privacy breaches are a serious matter to be addressed and remedied. The policy/protocol also documents and communicates internally and externally the expectations and steps that will be taken by the custodian in the event of a breach.

[27] Section 8(3) of the Health Information Regulation requires custodians to periodically review their administrative, technical and physical safeguards to protect the confidentiality and privacy of health information. A periodic review ensures that the measures in place continue to be appropriate and effective in protecting confidentiality and privacy.

[28] Questionnaire responses indicate that while the large custodians have privacy breach response policies/protocols in place, the picture is less clear for the rest of the health sector. Guidance provided by regulatory colleges to their members is inconsistent: only slightly more than half of the regulatory colleges say they recommend a privacy breach response policy to their members, and even so, this does not mean their members have policies/protocols in place. In the absence of consistent, clear guidance, it seems likely that regulated health professions would not have breach policies/protocols in place. This concern is alleviated to some extent, however, based on the OIPC's review of PIAs submitted by regulated health professions over the years (primarily by physicians and pharmacists). The OIPC does not accept PIAs unless breach response policies and protocols are in place.

2. How are staff/members educated or trained about their responsibilities regarding health information breaches?

Custodians:

- Alberta Health, AHS and Covenant Health say a variety of methods are used to inform/train staff about their obligations to protect confidentiality and privacy and the steps to take in the event of a breach. These methods include corporate policies, mandatory training (face to face and online), ongoing education, presentations, and materials/information on internal websites, and confidentiality agreements.

Regulatory colleges:

- Only two out of the eleven regulatory colleges say they provide their members with best practices for privacy breaches. One of the colleges says it refers its members to the OIPC website and another college indicated it would welcome guidance on including breaches in its standards of practice relating to patient records.

Universities:

- Similar to the large custodians, the University of Alberta and the University of Calgary say a variety of methods are used to inform/train staff about their obligations to protect confidentiality and privacy and the steps to take in the event of a breach.

Other entity:

- The ISO says training for EMR users is provided by AHS.

OIPC Comments

[29] A significant number of health sector breaches reported to and investigated by the OIPC are due to unauthorized access (snooping) and human error, which can be mitigated with proper training, auditing, and monitoring. This underscores the need for regular staff training and education about privacy generally, and breach management specifically.

[30] On June 18, 2012, the OIPC released a report titled *A Snapshot – Two Years of Mandatory Breach Reporting* under the *Personal Information Protection Act* (PIPA) (a copy of this report is available on the OIPC website). In releasing the report, the Commissioner said:

> The majority of reported breaches involve human error such as misdirected email, faxes, stolen or lost unencrypted electronic devices and improper record and electronic media destruction. Many of these breaches are preventable with proper security systems and encryption.

[31] Training and ongoing education is essential to ensure custodians and their affiliates have the knowledge and expertise to identify, manage, and respond to privacy breaches. Privacy breach management training and education is an administrative safeguard required under section 60 of the HIA. Simply having a policy in place does not ensure the policy is understood and adhered to by staff within the organization.

[32] Questionnaire responses, however, indicate that only the large custodians and universities consistently require that staff receive training and education about breach management and response. The OIPC's concerns about this lack of training and education are again alleviated to some extent as a result of having reviewed PIAs submitted by members of regulated health professions (physicians and pharmacists, in particular). The OIPC does not accept PIAs that do not describe training and education programs.

3. Do contracts with service providers include clauses requiring notification[5] in the event of a breach?

Custodians:

- Alberta Health and AHS say their contracts contain clauses requiring service providers to notify them of security incidents or privacy breaches.

- Covenant Health said notification requirements are contained in its information manager agreements. However, contracts for service providers who are not information managers do not contain a specific clause requiring notification. Covenant Health says the contracts do include a clause requiring compliance with Covenant Health policies (which state that contractors shall inform Covenant Health of all security incidents or privacy breaches as soon as they become aware of such incidents or possible breaches).

Regulatory colleges:

- One regulatory college said its members do not have contracts with service providers. Two of the remaining ten recommend that their members' contracts with service providers include a clause requiring notification if they experience a breach.

Universities:

- The University of Alberta and the University of Calgary both state their contracts contain clauses requiring contractors to notify the University in writing "as soon as practicable" or "within 48 hours" in the event of a breach.

Other entity:

- ISO says AHS acts as the service provider for the shared EMRs and that AHS is "obligated to inform the ISO of any breach under the EMR Information Exchange Protocol, the Information Sharing Agreement and/or the Information Management Agreement".

OIPC Comments

[33] Including notification clauses in service provider contracts is a reasonable step to safeguard the confidentiality and privacy of health information by third parties acting on behalf of a custodian. It ensures the custodian is aware of privacy breaches and can decide what action to take. As stated earlier, custodians are accountable for the collection, use and disclosure of health information by their affiliates, which includes service providers.

[34] Section 60.1(1) of the amended HIA requires an affiliate of a custodian to notify the custodian of "any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian". This is a new provision that will come into force when the HIA amendments are proclaimed.

[5] "Notification" as used here refers to contracted service providers notifying custodians about breaches. It does not refer to notifying individuals affected by a breach.

[35] Including a similar requirement in contracts with service providers will help to ensure that service providers, as affiliates, comply with the section 60.1(1) requirement to notify the custodian of a privacy breach.

[36] Appendix 4, page 2, section 20 of Alberta Health's publication, the *HIA Guidelines and Practices Manual*, provides custodians with suggested wording for contractual provisions to address this issue.

[37] It is noteworthy that only two of ten regulatory colleges having members who may contract with a service provider, recommend that their members include breach notification clauses in their contracts. This does not mean these contractual clauses do not exist. However, in the absence of a requirement or direction from their regulatory college, members of regulated health professions are unlikely to include such clauses. While this increases the risk custodians will not be made aware of breaches they are ultimately responsible for, the OIPC's concerns about this are again alleviated somewhat for those regulated health professionals who have submitted PIAs to the OIPC. The OIPC reviews PIAs to ensure custodians include breach notification clauses in their contracts with service providers.

4. When disclosing health information to researchers, are researchers advised as to how to manage health information breaches or what to do if a breach occurs?

Custodians:

- Alberta Health and AHS say their agreements with researchers contain notification requirements and the steps to take in case of a breach.

- Covenant Health said it has not advised researchers regarding breach response protocols.

Universities:

- The University of Alberta said it would not disclose health information for a research purpose as it is not a custodian.

- The University of Calgary said it advises researchers to report to the custodian in the event of a breach.

Other entity:

- The ISO says its research agreements requires researchers to report any breaches of confidentiality and/or security immediately upon identification of such breaches and to implement any recommendations from the ISO to both remedy the breach and prevent similar occurrences in the future.

OIPC Comments

[38] Responses to this question were mixed. Two of the three large custodians surveyed say their agreements with researchers contain notification requirements and the steps to take in case of a breach. One of the Universities advises researchers to report a breach to the custodian.

[39] Section 54(1) of the HIA states that if a "custodian decides to disclose health information to a researcher or perform data matching or other services to facilitate the research, the researcher must enter into an agreement with the custodian". Under section 54(1)(a)(ii) of the HIA, a researcher must agree to comply with any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information.

[40] An agreement with a researcher should include a provision that requires that the custodian be notified of a breach, which would strengthen the protection of confidentiality and privacy of health information and meet the requirements of the HIA relating to the protection of health information.

5. **Questions to the research ethics boards only: does the board provide advice to researchers on how to manage health information breaches; and does the board require research submissions to include information about how a researcher will manage a breach?**

- Both the University of Calgary – Conjoint Health Research Ethics Board and the Health Research Ethics Board of Alberta indicate they do not provide advice to researchers on how to manage health information breaches. Both boards also said they do not require research submissions to contain information on how a researcher will manage a breach.

OIPC Comments

[41] When considering a research proposal, section 50(1)(b)(iii) of the HIA requires an REB to consider whether adequate safeguards are in place to protect the privacy of the individuals who are the subjects of the health information to be used in the research and the confidentiality of that information. Once an REB approves a research proposal, the researcher can then approach a custodian to request disclosure of health information necessary to conduct the research. The custodian must sign an agreement with the researcher prior to disclosing health information.

[42] When it comes to using health information for research, there is a shared responsibility for considering privacy issues. The REB weighs the value of the research against risks to privacy, and considers steps the researcher says will be taken to protect the information. The custodian shares responsibility through the required execution of an agreement prior to disclosure, and then the researcher must comply both with the proposal as approved by the REB and the terms and conditions of the agreement signed with the custodian.

[43] It is important to ensure that researchers are informed of their obligations to protect health information, which includes the steps they must take to report and manage a privacy breach. However, the REBs responding to the questionnaire indicated they do not provide advice to researchers about how to manage health information breaches, nor do they require research submissions to include information about how a researcher will manage a breach.

[44] REBs do not set the safeguards a researcher must implement, but they must consider whether the researcher's safeguards are adequate to protect the information. Therefore, it would be helpful for REBs to require that proposals include information about the steps

researchers will take if a breach occurs, as this is information that is relevant to ensuring there are adequate safeguards in place to protect privacy and confidentiality.

6. Do you actively monitor for health information breaches? Do you recommend members actively monitor for health information breaches (question for regulatory colleges)?

Custodians:

- Alberta Health does not actively monitor for breaches. Alberta Health says staff report breaches in accordance with policy.

- AHS and Covenant Health indicate that they do actively monitor for breaches. Covenant Health says it receives proactive audit reports from AHS as its information technology services provider and information manager. However, Covenant Health says it has no specific documentation to describe its processes or demonstrate the level of activity. AHS said it has proactive auditing procedures in place and that these are documented in the PIAs submitted to the OIPC.

Regulatory colleges:

- Eight out of the eleven regulatory colleges say they have not recommended to their members to actively monitor for health information breaches. However, two colleges did indicate "not yet", which may mean such a recommendation may be forthcoming in the future.

Universities:

- The University of Alberta says proactive audits are undertaken periodically and that random sampling is done from time to time at its health clinic. The University's auditing procedures are documented in the PIAs it has submitted to the OIPC.

- The University of Calgary says it monitors its in-house clinics.

Other entity:

- The ISO says AHS, as information manager, is required to notify the ISO of any breaches and proactively audits and investigates user activity in the shared EMR.

OIPC Comments

[45] The two most common types of breaches reported to the Alberta OIPC are due to human error and unauthorised access by an authorised individual ("snooping").

[46] Breaches that result from human error can be detected by the realisation that information is missing, such as a lost laptop or work bag, or alternatively, a custodian may be informed that a fax or letter was directed to the incorrect recipient.

[47] "Snooping" breaches on the other hand commonly rely on individuals identifying themselves as an affected individual and notifying the custodian of the unauthorised activity, or via technical detection methods such as system auditing and monitoring.

[48] The Alberta Electronic Health Record (Alberta Netcare) is a provincial electronic health information system. The HIA requires that audit logs be kept documenting all accesses to Netcare records. Individuals may ask Alberta Health for a copy of this log in relation to their own health information and may file privacy complaints with the OIPC if they believe their health information has been inappropriately accessed (see the OIPC publication *Alberta Netcare: Know Your Rights,* available on the OIPC website). This is one way in which individuals may self-identify as an affected individual.

[49] However, relying only on breach reports from parties such as an affected individual is not sufficient. In most cases an individual would have to be aware of an unauthorized access, or suspect it has occurred. Conducting proactive audits or random sampling will assist in identifying breaches that are not known to affected individuals.

[50] Active monitoring for breaches is currently being conducted in some, but not all, areas of the health sector. The inconsistency in proactive monitoring increases the risk that certain breaches remain undetected.

Tracking and Reporting Breaches in Alberta's Health Sector

[51] In examining the current state of privacy breach reporting in Alberta's health sector, the OIPC reviewed what breaches are tracked or reported, and to whom, for fiscal years 2010-11 to 2014-15. In addition to information provided by questionnaire respondents, the OIPC also considered breaches self-reported by custodians over these four years.

7. Do you track the number of health information breaches that occur?

Custodians:

- Alberta Health recently began tracking the number of breaches that occur within Alberta Health, but did not do so in the past. Alberta Health said some breaches were reported to the OIPC, to the Provincially Reportable Incident Report Process (PRIRP) and to the Electronic Health Record Data Stewardship Committee (EHRDSC)[6].

- AHS tracks the number of breaches that occur within AHS, and says it has reported breaches to Alberta Health, the police (if the incident involved theft) and the relevant regulatory college (if the individual committing the breach is a member of a regulated health profession).

[6] The Electronic Health Record Data Stewardship Committee (EHRDSC) is a multi-disciplinary data stewardship committee established by the Minister of Alberta Health whose function is to make recommendations to the Minister with respect to the rules related to access, use, disclosure and retention of prescribed health information that is accessible via the Alberta EHR (Netcare).

- Covenant Health says it did not track the number of breaches that occurred within Covenant Health in 2010/11, but did so subsequently. Covenant Health says it has reported breaches to the OIPC but it does not track this data by fiscal year.

Regulatory colleges:

- Three out of the eleven regulatory colleges say their members have reported breaches to them. One of the three colleges reported a privacy breach to another authority such as the OIPC. One of the colleges says it is the member's responsibility to report the breach. It is important to note that there is no requirement to report a privacy breach to health regulatory colleges.

Universities:

- Both the University of Alberta and the University of Calgary track the number of breaches that occur within the universities. The universities say some of the breaches were reported to the OIPC and in one case to AHS.

REBs:

- The University of Calgary – Conjoint Health Research Ethics Board says it received one breach report in 2011 and reported the breach to the OIPC.

- The Health Research Ethics Board of Alberta includes the Cancer Committee and the Community Health Committee. The Cancer Committee says it received one breach report in 2012 and in turn reported the breach to the OIPC. The Community Health Committee says it has not received breach reports from researchers.

Other entity:

- The ISO says it tracked the number of breaches reported to it for only the 2012 year. ISO says the numbers were in relation to a pilot undertaken that year. However, the information manager for the EMR began formal reporting of privacy breaches to the ISO on May 10, 2014, commencing with April 2014 data. ISO says it did not report any of these breaches to another authority.

OIPC Comments

[52] Reporting and tracking privacy breaches can indicate if the number of breaches is increasing or decreasing, which is a measure of the effectiveness of privacy and security protocols, and can help to identify particular areas which may be prone to breaches as well as systemic issues. For large electronic health records systems that enable the sharing of health information amongst hundreds or thousands of authorized users, reporting and tracking privacy breaches ensures incidents are brought forward to those responsible for investigation and resolution. Analysis of this data would be helpful in determining causes and methods to reduce and prevent breaches from occurring or re-occurring.

[53] The responses to the questionnaires reveal that privacy breaches are not consistently tracked or reported by the health sector. Alberta Health only recently began tracking breaches, some of which were reported to the OIPC, to the Provincially Reportable Incident Report Process (PRIRP) and to the Electronic Health Record Data Stewardship Committee (EHRDSC)[7]. Covenant Health did not track breaches in 2010-11, but did so subsequently, and said it has reported breaches to the OIPC. AHS provided information to demonstrate that it diligently tracks breaches that occur within AHS, and reports breaches to the appropriate entity positioned to take action, including the OIPC.

[54] The regulatory colleges do not require that their members report breaches to them, and the REBs do not require researchers to report privacy breaches. While three regulatory colleges and two REBs say they have received breach reports, the total number of breaches within the membership of the colleges is unclear because the reporting is ad hoc. In addition, breaches reported to an external authority are not always tracked by the custodian making the report.

[55] In the absence of consistent breach tracking and reporting, it is difficult to estimate the number of breaches occurring within the health sector, or the likely impact of mandatory breach reporting legislation.

8. What breaches are reported using the Provincially Reportable Incident Response Process?

[56] In August 2005, Alberta Health implemented its "Provincially Reportable Incident Response Process" (PRIRP). This process was subsequently updated in 2007 and 2009. The PRIRP states that incidents involving a potential threat to the confidentiality, integrity or availability of health information are to be reported to Alberta Health in accordance with the process outlined within the PRIRP. The PRIRP sets out how these incidents are reported, classified, investigated, resolved and concluded.

[57] AHS, Covenant Health, three of the colleges (CARNA, Pharmacists and CPSA), the universities and the ISO were asked if they were aware of Alberta Health's PRIRP. These custodians or entities were selected to respond to this question because they themselves, or their affiliates, regulated members or employees have access to the Alberta Electronic Health Record (Netcare). In the case of the ISO, it provides information stewardship for an electronic medical record that makes information available to Netcare. The questionnaires also asked the custodians whether they have used the PRIRP to report a breach.

Custodians:

- Alberta Health says it received 13 reports in 2010, four in 2011, six in 2012, and two in 2013 for a total of 25 privacy breach reports using the PRIRP between 2010 and 2013. These breach reports are numbered and electronically tracked by Alberta Health.

[7] The Electronic Health Record Data Stewardship Committee (EHRDSC) is a multi-disciplinary data stewardship committee established by the Minister of Alberta Health whose function is to make recommendations to the Minister with respect to the rules related to access, use, disclosure and retention of prescribed health information that is accessible via the Alberta EHR (Netcare).

- AHS and Covenant Health indicate they are aware of Alberta Health's PRIRP. AHS provided the number of breaches it reported using the PRIRP: three in 2010; two in 2011; three in 2012; and six in 2013.

- Covenant Health says it has not used the PRIRP. Covenant Health indicates it had understood the PRIRP was limited to information technology security/technical incidents involving Alberta Netcare but recently realized that it was also intended to report inappropriate user accesses. Subsequently, Covenant Health informed the OIPC that it had attempted to report a breach using the PRIRP, but that the online form did not "seem to be set up in a fashion conducive to data entry". Covenant Health says it sent the report via email to Alberta Health but did not receive a confirmation of receipt or any further message from Alberta Health as to any action taken in response to the report.

Regulatory colleges:

- The three colleges all say they were not aware of Alberta Health's PRIRP.

Universities:

- The University of Alberta says it is aware of the PRIRP, but was not aware of any incidents applicable to this process. The University of Calgary says it was not aware of the PRIRP.

Other entity:

- The ISO says it was only involved with breaches involving the shared EMR (eClinician) system, which does not fall under the PRIRP.

OIPC Comments

[58] The questionnaire responses suggest that the PRIRP reporting process is not consistently understood or applied. This is of particular concern, as the PRIRP provides an established process to report privacy breaches to Alberta Health, and ensures there is a mechanism to address confidentiality, data integrity and availability incidents involving the Alberta Electronic Health Record (Netcare). A lack of awareness and understanding of the PRIRP may lead to under reporting, and inconsistent reporting and tracking of incidents.

[59] Section 56.7 of the HIA requires that the Minister of Alberta Health establish a multi-disciplinary committee to make recommendations to the Minister with respect to the rules related to access, use, disclosure and retention of prescribed health information that is accessible via Netcare. Membership includes health professional representatives and, pursuant to section 56.7(2) of the HIA, must include at least two members of the public. The committee is known as the Electronic Health Record Data Stewardship Committee (EHRDSC), and its mandate involves overseeing the stewardship of:

- The Alberta Electronic Health Record;

- Health information that the Alberta EHR receives from an electronic medical record (EMR);

- Health information that the Alberta EHR sends to an EMR; and
- Health information that passes through the Alberta EHR from one EMR to another.

[60] The EHRDSC reports and provides advice to the Minister of Alberta Health. It guides the development of Netcare rules through the management of information exchange protocols, information manager agreements and standards.

[61] Properly overseeing stewardship of the areas noted above requires that the EHRDSC has knowledge of incidents affecting the operation of Netcare, to guide development of rules and standards necessary for effective data stewardship. The last meeting of the EHRDSC took place on October 23, 2013. The appointment terms of the majority of committee members expired on November 1, 2013, and the committee has not been re-established.

[62] It is a significant concern that the committee with legislated responsibility to oversee stewardship of data made available through the Alberta Electronic Health Record (Netcare) has not met for more than two years. This is a significant gap in legislative compliance and the governance of Netcare. EHRDSC guidance on the development of rules and standards necessary for effective data stewardship is absent.

[63] Health information is sensitive. The HIA enables its use, including for the purposes of providing health services, approved research, quality improvement and health system management. The HIA balances use with a number of duties designed to protect the confidentiality and privacy of Albertans' health information. Mandatory breach reporting and notification amendments have been passed as one more mechanism to strike a reasonable balance. The EHRDSC is required to ensure that a multi-disciplinary perspective guides data stewardship issues, which should include privacy breaches, particularly where they may present a systemic data stewardship issue.

9. What breaches are self-reported to the OIPC?

[64] The table below lists the number of self-reported breaches received by the OIPC by fiscal year:

Custodian	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	Total
Alberta Health	3	2	1	-	1	7
Alberta Health Services	17	15	11	20	31	94
Covenant Health	-	1	1	1	0	3
Nursing Homes	5	3	1	-	1	10
Chiropractors	-	-	4	-	2	6
Dentists	-	2	-	-	0	2
Denturists	-	-	-	1	0	1
Pharmacists/Pharmacies	1	3	4	2	4	14
Physicians	14	29	30	31	28	132
Faculty of Medicine	1	-	-	1	0	2
Researchers	-	1	-	-	0	1

Custodian	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	Total
Affiliates and Information Managers	-	1	-	-	0	1
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies created by custodians	-	-	-	1	0	1
Colleges and Associations	-	-	-	1	1	2
Primary Care Networks	2	-	2	4	5	13
Subsidiary Health Corps.	-	2	3	3	2	10
Other	-	-	-	3	0	3
Total	**43**	**59**	**57**	**68**	**75**	**302**

OIPC Comments

[65] It is not clear what "triggers" a custodian to report a breach to the OIPC. However, the OIPC encourages custodians to report breaches so that the OIPC can assist with risk assessment, and provide guidance for responding to the breach and preventing similar breaches in the future. The OIPC tracks the number of self-reported breaches it receives from Alberta's health sector and reports these numbers in its annual report. A self-reported breach is a breach that has been reported by the custodian that experienced it, rather than being generated by a complaint from an affected individual. Complaints of breaches by individuals are not reflected in these numbers.

[66] The OIPC received 302 self-reported breaches from the health sector between 2010-11 and 2014-15. There has been a 75% increase in the number of breaches self-reported by the health sector to the OIPC during this time.

[67] It is important to reiterate that there is currently no mandatory requirement for custodians to report breaches to the OIPC. Consequently, the statistics above are only the breaches that custodians have chosen to report to the OIPC. They do not represent all breaches that may have occurred. However, the numbers do emphasize that there are a significant number of breaches that occur that require breach response management.

Health Sector's Readiness for Mandatory Breach Reporting and Notification

10. How prepared do you feel you or your members are to respond to a breach? (not at all prepared; somewhat prepared; fully prepared)

[68] With the exception of the REBs, we asked survey respondents to assess their level of preparedness to respond to a privacy breach.

Custodians:

- All three large custodians (Alberta Health, AHS and Covenant Health) rate their level of preparedness as "3-fully prepared". However, Covenant Health added that staff in general could be rated as “somewhat prepared” and require the support of their Information and Privacy Office to properly respond to a privacy breach.

Regulatory colleges:

- Only one of the ten regulatory colleges rates their members’ level of preparedness as “3-fully prepared”. Four of the regulated colleges say their members are “1-not at all prepared” and five others indicate their members are “2-somewhat prepared”. The remaining college did not respond to this question.

Universities:

- The University of Alberta and the University of Calgary indicate they are “3-fully prepared”.

Other entity:

- ISO says that it is “3-fully prepared”.

[69] The table below summarizes the level of preparedness identified by the colleges and the approximate number of members for each college.

College	Level of Preparedness	Approximate Number of Members
College of Physicians and Surgeons of Alberta	1 – not at all prepared	12,627 *include independent, out of province, post grads and students
College of Podiatric Physicians of Alberta	1 – not at all prepared	Number not provided
College of Alberta Opticians	1 – not at all prepared	1,000
College of Alberta Denturists	1 – not at all prepared	305 practicing members
College and Association of Registered Nurses of Alberta	2 – somewhat prepared	37,700
Alberta College and Association of Chiropractors	2 - somewhat prepared	1,014
College of Registered Dental Hygienists of Alberta	2 – somewhat prepared	3,143 regulated members 149 non-practicing members
College and Association of Midwives	2 – somewhat prepared	88 practicing members 7 non-practicing 37 students
College of Pharmacists	No response	Number not provided
Alberta Dental Association and College	3 – fully prepared	Number not provided
Alberta College of Optometrists	2 – somewhat prepared	Number not provided

OIPC Comments

[70] The questionnaire responses indicate that the large custodians, universities and the ISO believe their staff are "fully prepared" to respond to a breach, while regulatory colleges generally feel their members are not "not at all prepared" or "somewhat prepared".

[71] The responses suggest that a significant portion of the health sector (regulated members of colleges) may not be prepared or are only somewhat prepared to respond to a breach. The colleges' assessments of their respective members indicate there may be a lack of knowledge within Alberta's health sector regarding privacy breach response. The OIPC's concern about a general lack of preparedness is alleviated to some extent, however, for those regulated health professionals that have submitted PIAs to the OIPC for review as the OIPC ensures that PIAs include breach response policies. It is possible though that some custodians with written policies and training may not be fully aware of their own administrative controls and should review and update them in preparation for mandatory breach reporting. Overall, the questionnaire responses reveal a need for training, education and guidance on privacy breach management and response.

11. Are you aware that legislation was passed in May 2014 requiring custodians under the HIA to notify the Commissioner, the Minister of Health and affected individuals of health information breaches?

Custodians:

- AHS and Covenant say they are aware of the May 2014 legislation.

Regulatory colleges:

- Seven out of the eleven regulatory colleges say they are aware of the May 2014 legislation. Of the remaining colleges, one said it was not aware of the HIA amendments until it received the OIPC questionnaire, but its members are also subject to Alberta's *Personal Information Protection Act* (PIPA) and have been subject to breach reporting since 2010.

Universities:

- The Universities say they are aware.

REBs:

- The University of Calgary – Conjoint Health Research Ethics Board says it is aware.
- The Community Health Committee within the Health Research Ethics Board of Alberta says it was not aware, while the Cancer Committee says it was aware.

Other entity:

- The ISO says it was aware.

OIPC Comments

[72] Based on the responses, it appears most areas of the health sector are aware of the HIA amendments regarding breach reporting and notification.

[73] One of the colleges indicated that some of its members were subject to both the HIA and the *Personal Information Protection* Act (PIPA). This is also the case for some members of some of the other colleges. The amended HIA requires custodians to notify the Commissioner, the Minister of Health and affected individuals if a custodian determines there is "a risk of harm" to an individual. Determining the threshold for what constitutes a risk of harm depends on assessment of a number of factors that will be set out in the *Health Information Regulation*. In contrast, a PIPA organization must report a privacy breach "where a reasonable person would consider there exists a real risk of significant harm to an individual". The OIPC has not reviewed the draft regulation; therefore, it is not possible to compare the actual threshold for a required report between the HIA and PIPA. Nevertheless, the wording and construct for mandatory breach reporting in these Acts is distinctly different. In a news release issued May 7, 2014, the Commissioner said this difference "may cause confusion among those who are regulated by both Acts".

[74] Considerable training and education will be required to ensure custodians understand their breach reporting and notification obligations under the amended HIA. Those custodians who are also subject to PIPA must be educated as to the different requirements under the HIA and PIPA.

Summary of Investigation Findings

1. Breach response policies/protocols

[75] The large custodians surveyed have privacy breach response policies/protocols in place. However, guidance provided by regulatory colleges to their members is inconsistent: only slightly more than half of the regulatory colleges say they recommend a privacy breach response policy to their members, and even so, this does not mean their members have policies/protocols in place. In the absence of consistent, clear guidance, it seems likely that regulated health professions would not have breach policies/protocols in place. To some extent, concerns may be alleviated for those regulated health professions that have submitted privacy impact assessments (PIAs) to the OIPC for review (i.e. physicians and pharmacists in particular), as the OIPC reviews PIAs to ensure breach response policies and protocols in place.

2. Education and training

[76] Large custodians and universities have breach management and response education and training programs in place. There is less consistency among other segments of the health sector. There is little indication that consistent training and education is provided to custodians who are members of a professional college or their affiliates to ensure they have the knowledge required to manage a privacy breach. To some extent, this concern is alleviated for those regulated health professions that have submitted PIAs to the OIPC for

review (physicians and pharmacists), as the OIPC reviews PIAs to ensure education and training programs are in place.

3. Service provider contracts

[77] Alberta Health and AHS contractually require service providers to notify them of privacy breaches. Covenant Health includes similar provisions in information manager agreements. Only two of ten regulatory colleges recommend their members address breach notification in contracts with service providers. This increases the risk that custodians will not be aware of breaches they are ultimately responsible for. To some extent, concerns may be alleviated for those regulated health professions that have submitted PIAs to the OIPC for review, as the OIPC reviews PIAs to ensure service provider contracts address privacy breach reporting.

4. Breach management when disclosing health information to researchers

[78] Two of the three large custodians include breach response and notification requirements in their agreements with researchers. One of the Universities advises researchers to report a breach to the custodian. Section 54(1) of the HIA states that if a “custodian decides to disclose health information to a researcher or perform data matching or other services to facilitate the research, the researcher must enter into an agreement with the custodian” and agree to comply with any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information.

[79] An agreement with a researcher should include a provision that requires that the custodian be notified of a breach, which would strengthen the protection of confidentiality and privacy of health information and meet the requirements of the HIA relating to the protection of health information.

5. REB requirements for researchers

[80] When assessing a research proposal, the HIA requires REBs to consider whether adequate safeguards are in place to protect the privacy of research subjects. However, the REBs surveyed do not advise researchers about managing health information breaches, nor do they require research submissions to include information about how a researcher will manage a breach. It is difficult to know how REBs can assess the adequacy of safeguards without this information.

6. Proactive monitoring to identify breaches

[81] Proactive monitoring for breaches allows a custodian to detect breaches, and “snooping” in particular. AHS and Covenant Health proactively monitor to identify breaches. Alberta Health does not. Eight of eleven regulatory colleges do not recommend proactive monitoring to their members. The Universities proactively monitor to some extent. The inconsistency in proactive monitoring increases the risk that certain breaches remain undetected, and places Albertans at risk of being unaware of a breach affecting them, and unable to take steps to protect themselves.

7. Tracking privacy breaches

[82] Tracking the incidence of breaches allows a custodian to assess whether or not breaches are increasing, and to identify areas of concern or systemic issues, which can then be addressed. However, breach tracking varies widely within the health sector. Of the large custodians, only AHS has consistently tracked privacy breaches since 2010-11. Alberta Health only recently started to track breaches. Covenant Health began tracking breaches in 2011-12. It appears the Universities and REBs track breaches. The ISO tracked breaches in 2012 as part of a pilot program.

[83] Breach reporting within the health sector is also inconsistent. As breach reporting is currently voluntary, it is not clear what triggers a custodian to report breaches to any particular authority (e.g. the OIPC, Alberta Health, or to a regulatory college).

[84] In the absence of consistent breach tracking and reporting, it is difficult to estimate the number of breaches occurring within the health sector, or the likely impact of mandatory breach reporting legislation.

8. The Provincially Reportable Incident Response Process (PRIRP)

[85] The PRIRP is an established process for reporting breaches to Alberta Health, and ensures there is a mechanism to address incidents involving the Alberta Electronic Health Record (Netcare). However, there appears to be limited awareness of the PRIRP in the health sector, which may mean there is under-reporting and inconsistent reporting of breaches.

[86] The Electronic Health Record Data Stewardship Committee (EHRDSC), which the Minister of Alberta Health is required to establish pursuant to section 56.7 of the HIA, is responsible for overseeing stewardship of data made available through Netcare, and reports and provides advice to the Minister. The EHRDSC has not met for over two years. This is a significant compliance issue, which undermines confidence in governance of the provincial electronic health record.

9. Breaches reported to the OIPC

[87] The OIPC received 302 self-reported breaches from the health sector between 2010-11 and 2014-15. There has been a 75% increase in the number of health sector self-reported breaches to the OIPC over this time period.

[88] It is not clear what "triggers" a custodian to voluntarily self-report a breach to the OIPC. The OIPC encourages custodians to report breaches to receive assistance in risk assessment and responding to the breach, and to review steps that could prevent similar breaches in the future.

10. Breach preparedness

[89] A significant portion of the health sector (regulated members of colleges) is not prepared, or only somewhat prepared, to respond to a breach. There may be a lack of knowledge within Alberta's health sector regarding privacy breach response, management and notification. To

some extent, concerns may be alleviated for those regulated health professions that have submitted PIAs to the OIPC for review. The OIPC reviews PIAs to ensure custodians have breach response policies/protocols in place, as well as education and training programs.

11. Awareness of HIA amendments

[90] Most, but not all areas of the health sector are aware of the HIA amendments regarding breach reporting and notification.

[91] Members of some professional colleges are subject to both the HIA and the *Personal Information Protection* Act (PIPA). This could lead to confusion as the breach reporting and notification schemes under the two Acts differ markedly (e.g. the threshold that triggers reporting of a breach). To some extent, concerns may be alleviated once HIA Regulations are available.

[92] Considerable training and education will be required to ensure custodians understand their breach reporting and notification obligations under the amended HIA. Those custodians who are also subject to PIPA must be educated as to the different requirements under the HIA and PIPA.

Recommendations

[93] The OIPC makes the following recommendations to enhance privacy breach reporting in the health sector and assist with the implementation of mandatory breach reporting and notification under the amended HIA, when these amendments come into force.

Custodians

1. Review existing breach notification policies and procedures and make staff aware of their obligations under these policies. Alternatively, develop and implement policies if none are currently in place.

[94] Many custodians have breach policies or procedures in place. These policies and procedures are only useful when staff are aware of them and understand their responsibilities with respect to them. Regular reminders to staff about organizational breach policies and procedures are vital to successful privacy breach management.

2. Include specific breach reporting and notification clauses in contracts with service providers/information managers.

[95] Including breach reporting and notification clauses in service provider and information manager contracts is a reasonable step to safeguard the confidentiality and privacy of health information by third parties who may be acting on behalf of a custodian.

[96] Including these clauses in contracts will also help to ensure compliance with section 60.1(1) of the amended HIA, which requires an affiliate of a custodian to notify the custodian of "any loss of individually identifying health information or any unauthorized access to or

disclosure of individually identifying health information in the custody or control of the custodian".

3. Include breach reporting and notification requirements in agreements with researchers.

[97] Section 54(1) of HIA states that if a "custodian decides to disclose health information to a researcher or perform data matching or other services to facilitate the research, the researcher must enter into an agreement with the custodian". Under section 54(1)(a)(ii) of the HIA, a researcher must agree to comply with any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information.

[98] An agreement with a researcher should include a provision that requires that the custodian be notified of a breach, which would strengthen the protection of confidentiality and privacy of health information and meet the requirements of the HIA relating to the protection of health information.

Alberta Health

4. Consult with the Commissioner on the draft mandatory breach reporting and notification regulation.

[99] Section 60.1(3) of the amended HIA requires custodians to give notice to the Commissioner, the Minister of Health and affected individuals. The notice must be "in accordance with the regulations" (section 60.1(2)).

[100] It is not known at this time whether the HIA regulations will prescribe a common format for notifying the Commissioner, the Minister and affected individuals. This raises concerns for the Commissioner, including:

- The Commissioner's powers under the amended HIA are limited to reviewing a custodians' decision to not notify an individual of a privacy breach. Any legislated format for notifying the Commissioner must include the information the Commissioner requires to review a custodian's decision not to notify affected individuals.
- Any common format should ensure affected individuals receive enough information so they can take action they deem necessary to protect their own privacy.
- The amended HIA requires custodians to report certain breaches to the Minister; however, it is not clear what action the Minister will take upon receiving notification of a privacy breach. Therefore, it is unclear as to what information the Minister will require from a breach notice report submitted by a custodian.

[101] Under section 60.1(4) of the amended HIA, a custodian "must consider all relevant factors, including the factors prescribed by the regulations" in assessing whether there is a risk of harm to an individual. It is not known at this time what factors will be prescribed by regulation, but any such list should be non-exhaustive. That is, any list of factors to be considered in determining what constitutes a risk of harm should not be so prescriptive as to limit decision-making. The regulations should state that none of the factors should be considered in isolation, but should be considered in concert with other relevant factors.

[102] Generally, breach notifications should be sent directly to affected individuals. However, there may be circumstances where indirect notification is a preferred option. The mandatory breach notification requirements already set out in Alberta's PIPA allow for the Commissioner to authorize indirect notification of affected individuals. It is recommended that the mandatory breach notification requirements under the HIA consider a similar scheme.

5. Amend s. 54(1) of the HIA to require custodians to include breach reporting and notification requirements in their agreements with researchers.

[103] Section 54(1) of the HIA sets out the requirements of a research agreement. Requiring that a provision for breach reporting and notification be included in such an agreement would ensure that such a provision is not ommitted.

6. Work with health regulatory colleges and professional associations to ensure materials are produced and training provided to educate regulated health services providers, who are custodians, about breach reporting and notification requirements under the amended HIA.

[104] Considerable training and education will be required to ensure custodians understand their breach reporting and notification obligations under the amended HIA. Those custodians who are also subject to PIPA must be educated as to the different requirements under the HIA and PIPA.

7. Clarify what privacy breach incidents are to be tracked and reported within the health sector, and clarify those which must also be reported through the Provincially Reportable Incident Response Process (PRIRP).

[105] Consistent tracking of privacy breach incidents can assist in identifying trends or issues with respect to the reasons breaches occur, and can be useful in reducing or preventing breaches from occurring or re-occurring.

[106] The requirements and the process for reporting must be clearly communicated and readily available to individuals and custodians reporting privacy breaches. Furthermore, there should be confirmation of receipt of the reports and information regarding actions that will be taken to manage the breach.

8. Take immediate steps to re-establish the Alberta Electronic Health Record Data Stewardship Committee (EHRDSC).

[107] Section 56.7 of the HIA requires the Minister of Health to establish the EHRDSC. The committee has not met for over two years. This is a compliance issue.

[108] It is also important to clarify how privacy breach incidents that affect the Alberta Electronic Health Record (Netcare) will be identified and raised to the EHRDSC. This is essential in order for the EHRDSC to fulfill its legislated mandate to provide effective stewardship of health information made available through Netcare.

Research Ethics Boards

9. Require researchers to include information in their proposals describing the researchers' plans to respond to and report a privacy breach while the research is being carried out.

[109] REBs are responsible for assessing whether research proposals include adequate safeguards to protect the confidentiality and privacy of health information (section 50(1)(b)(iii) of HIA). Requiring researchers to include information in their proposals about the steps they will take in the event of a breach would assist the REB in determining whether adequate safeguards are in place and further enhance the protection of health information to be used for research.

Rachel Hayward
Senior Information and Privacy Manager