Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2014-IR-01

Report concerning theft of unencrypted laptop containing health information

August 26, 2014

Medicentres Canada Inc.

Investigation H5880

TABLE OF CONTENTS

Introduction

[1] On October 10, 2013, the Office of the Information and Privacy Commissioner (OIPC) received a formal breach report[1] from Medicentres Inc. ("Medicentres" or the "information manager") about a possible breach of the *Health Information Act* (HIA). Medicentres reported that an information technology consultant's (the "IT Consultant") laptop containing billing information for an estimated 631,000 Albertans had been stolen on September 26, 2013. The laptop was password protected, but not encrypted. In its report to the OIPC, Medicentres stated it contacted the OIPC to obtain "assistance and recommendations on how best to respond to the incident".

[2] On October 10, 2013, the Information and Privacy Commissioner ("Commissioner") opened Case File H5714 under section 84(1)(h) of the HIA, which authorizes the Commissioner to "give advice and recommendations of general application to a custodian on matters respecting the rights or obligations of custodians under this Act".

[3] On January 22, 2014, Medicentres issued a release to the media about the incident. The same day, the Minister of Health wrote to the Commissioner requesting an investigation.

[4] On January 23, 2014, Medicentres published notices concerning the incident in the *Edmonton Journal* and the *Calgary Herald*, and posted a notice on the Medicentres' website.

[5] On January 23, 2014, the Commissioner announced she was initiating an investigation of the incident on her own motion, pursuant to section 84(1)(a) of the HIA, which states the Commissioner may, "at the request of the Minister or otherwise, conduct investigations to ensure compliance with any provision of this Act…". In deciding to investigate, the Commissioner considered, among other things: the number of affected individuals; the likelihood that affected individuals would submit complaints; and the Minister of Health's letter requesting an investigation.

[6] Between January 29, 2014 and the issue date of this report, the OIPC received 23 formal complaints about this incident. Each of the complainants verified with Medicentres that their own health information was involved in this incident. However, as the complaints were about matters that were already the subject of this Commissioner-initiated investigation, they were placed in abeyance pending the outcome of this investigation.

[7] The Commissioner authorized me to investigate. This report outlines my findings and recommendations.

[1] Medicentres has noted that it sent the report on October 9, 2013. The report was sent via email to the OIPC at 10:49 pm on October 9, 2013 and logged the next business day. Medicentres also phoned the OIPC on October 4, 2014 to advise that a privacy breach report was on the way and to discuss the matter informally, however only summary details were provided at the time. The OIPC considers October 10, 2013 to be the day it received formal notification about the incident in question.

Background

[8] Medicentres is comprised of a number of family health care clinics, and operates 27 clinics in four Canadian cities in Alberta and Ontario. It employs over 400 nurses, receptionists and associated health care personnel and administrates the practices of approximately 250 independently practicing physicians at any one time.

[9] The IT Consultant left work as usual on September 26, 2013 with his laptop bag. A few hours later, whilst at a public venue, the IT Consultant discovered his laptop was missing. On September 27, 2013 the IT Consultant informed Medicentres his laptop computer containing health information "was missing". On October 1, 2013 the IT Consultant confirmed by email to Medicentres that he had not found his laptop, and on October 5, 2013 the IT Consultant and Medicentres reported the incident to the Edmonton police. To date, the laptop has not been recovered and is assumed to be stolen.

[10] A database containing the health information of 621,884 (actual number) Medicentres patients was stored on the laptop computer's hard drive. Patients seen in Medicentres clinics in Alberta between May 2, 2011 and September 19, 2013 were affected.

[11] Medicentres reported that the information stored on the laptop computer was in a database format and the IT Consultant was developing, modifying and troubleshooting a tracking and reconciliation application to manage Alberta Health Care Insurance Plan (AHCIP) claims. Medicentres refers to this system as the Aged Trial Balance Application (ATBA).

Jurisdiction

The health information

[12] The HIA applies to "health information" in the custody or control of a "custodian".

[13] The information at issue in this matter includes:

- patient name;
- personal health number (PHN);
- date of birth;
- ICD9 diagnostic codes;[2]
- health service billing codes; and
- dollar amount billed.

[2] ICD9 codes are diagnostic disease codes. ICD9 is an international standard for diagnostic codes. Health Service codes reflect the service provided and are associated with a dollar amount. These codes are necessary for the physician to obtain payment for the health services provided.

[14] This information was collected by Medicentres physicians in the course of providing health services to patients in Alberta. It qualifies as "health information" as defined in section 1(1)(k) of the HIA.

The custodians

[15] Section 1(1)(f)(ix) of the HIA states that a custodian includes "a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause."

[16] Section 2(2)(i) of the *Health Information Regulation* states that "regulated members of the College of Physicians and Surgeons of Alberta" are designated as custodians for the purposes of section 1(1)(f)(ix) of the HIA.

[17] Each physician practicing at Medicentres in Alberta is a member of the College of Physicians and Surgeons of Alberta. Therefore, each of these physicians is a "custodian" to whom the HIA applies.

[18] Not all physicians working at Medicentres or those working during the period in question were affected by the incident. Therefore, I refer to two distinct categories of physicians at certain points in this report:

- physicians practicing at Medicentres whose patients' health information was stored on the stolen laptop.
- physicians practicing at Medicentres whose patients' health information was not stored on the stolen laptop.

[19] Because the information at issue in this investigation is "health information" and the physicians practicing at Medicentres are "custodians," the HIA applies.

[20] I note that Medicentres is also an "organization" as defined under section 1(1)(i) of Alberta's *Personal Information Protection Act* (PIPA). However, section 4(3)(f) of PIPA states that PIPA "does not apply to the following: (f) health information as defined in the *Health Information Act* to which that Act applies." As I have already found that the information at issue in this matter is health information as defined in the HIA to which the HIA applies, PIPA does not apply in this case.

Medicentres is an "information manager" to the custodians

[21] Section 66 of the HIA sets out a custodian's power to enter into an agreement with an information manager. Section 66(1) defines "information manager" as follows:

> **Power to enter agreement with information manager**
>
> 66(1) In this section, "information manager" means a person or body that
>
> (a) processes, stores, retrieves or disposes of health information,

(b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or

(c) provides information management or information technology services.

(2) A custodian must enter into a written agreement with an information manager in accordance with the regulations for the provision of any or all of the services described in subsection (1).

(3) A custodian that has entered into an agreement with an information manager may provide health information to the information manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement.

(4) An information manager to which information is provided pursuant to subsection (3) may use or disclose that information only for the purposes authorized by the agreement.

(5) An information manager must comply with

(a) this Act and the regulations, and

(b) the agreement entered into with a custodian

in respect of information provided to it pursuant to subsection (3).

(6) Despite subsection (5)(a), a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information provided by the custodian to the information manager.

[22] Medicentres submitted that it is an information manager in relation to the custodians and each custodian working out of Medicentres enters into a "Practitioner Agreement". I reviewed a sample Practitioner Agreement which states:

> Medicentres Inc. will provide facilities and services to the custodians. These services include storage, maintenance and retrieval of patient "health information" and other administrative functions.

[23] I agree that Medicentres is an "information manager" as defined in the HIA in relation to the custodians.

[24] As an information manager, Medicentres must comply with the HIA and the regulations, as well as its agreement with the custodians practicing at Medicentres, pursuant to section 66(5) of the HIA, cited above. Despite Medicentres' duty to comply with the HIA, section 66(6) of the HIA goes on to say that the custodians continue to be responsible for compliance with the HIA in respect of the health information they provide to their information manager, Medicentres.

Medicentres as respondent in this investigation

[25] Medicentres reported the incident to the OIPC in October 2013 and continued to communicate with the OIPC until January 2014 as it developed its response plan. Once this investigation was launched in January 2014, the OIPC communicated with Medicentres' Vice President of Finance and Operations, asking questions and receiving answers from Medicentres through exchanges of letters.

[26] A draft of this report was given to Medicentres on April 17, 2014 to comment on any factual errors. In responding to this draft, Medicentres stated in a letter dated May 12, 2014,

> "Medicentres is not making any statements on behalf of the custodians. Medicentres is responding solely to this investigation in its role as an Information Manager".

Medicentres subsequently reiterated this position in demand letters to the OIPC dated July 17, 2013. Similarly, the Chief Medical Officer of Medicentres has stated that he, "…is not authorized by the individual custodians to respond on their behalf".

[27] These assertions were surprising, given the following.

[28] First, physicians sign the "Medicentres Practitioner Agreement" when agreeing to work at Medicentres. The Agreement contains the following clauses on the duties of Medicentres and custodians regarding compliance with the HIA:

> 7.1 DUTIES UNDER THE HIA
>
> The Physician and MEDICENTRES covenant and agree to strictly comply with their respective duties, responsibilities and obligations arising under or pursuant to the HIA with respect to Health Information of Patients in their respective capacities.
>
> 7.2 POLICIES AND PROCEDURES RELATING TO HEALTH INFORMATION
>
> MEDICENTRES shall have the right from time-to-time to establish, amend and implement policies and procedures for the protection and release of Health Information of Patients and the conduct of the Physician with respect to the Physician's Practice at the Clinics relating to Health Information of Patients and associated security systems, maintenance and storage systems, including but not restricted to policies and procedures to:
> (a) Identify and maintain a written record of all administrative, technical and physical safeguards in respect of Health Information of Patients;
> (b) Designate an individual who is responsible for the overall security and protection of Health Information of Patients in the custody or under the control of the Physician and MEDICENTRES;
> (c) Periodically assess the adequacy of the administrative, technical and physical safeguards; and
> (d) Facilitate the implementation of the HIA as required thereunder; (such policies and procedures being herein referred to as "Health Information Policies").
>
> 7.3 OBLIGATIONS RELATING TO HEALTH INFORMATION POLICIES
>
> The Physician covenants and agrees to cooperate and assist MEDICENTRES in the development and implementation of Health Information Policies and comply with and adopt and implement such Health Information Policies, provided such policies and procedures are not in contravention of the HIA or the obligations of the Physician pursuant to the H IA.
>
> 7.4 INQUIRIES AND INVESTIGATIONS UNDER THE HIA
>
> The Physician and MEDICENTRES shall cooperate and provide such information and assistance as may be required from time to time relating to any inquiry or investigation under the HIA relating to Health Information of Patients or the Health Information Policies in effect and adopted from time to time relating to Health Information of Patients and/or the implementation of their respective obligations under and pursuant to the HIA.

[29] Under section 7.2 of the Agreement, cited above, Medicentres has established a "Health Information Privacy and Security Manual". Policies in this Manual are approved by a Medicentres' executive. The first policy in this Manual is "Roles and Responsibilities", which identifies a "Privacy Committee" as the body responsible for privacy compliance within Medicentres. The Privacy Committee is comprised of the Controller, the Clinic Operations Managers in Edmonton and Calgary and the IT Project Manager. Under this policy, the Privacy Committee is responsible for the following duties (among others):

> - Ensuring policies and procedures around Health Information are developed, implemented, monitored and reviewed for appropriateness.
> - Taking appropriate action(s) on potential HIA privacy breeches [sic] within Medicentres when discovered by or reported to the Privacy Committee, including but not limited to: internal training or disciplinary actions, disclosure to the patient, and self-reporting to the Office of the Information and Privacy Commissioner (OIPC), as applicable.
> - Acting as contacts when dealing with the Office of the information and Privacy Commissioner (OIPC).

[30] When reviewed together, the Practitioner Agreement and Medicentres' Health Information Privacy and Security Manual, established under the authority of the Practitioner Agreement, indicate to me that:

- The physicians practicing at Medicentres have authorized Medicentres to carry out their duties under the HIA to name an individual responsible for HIA compliance and to establish HIA policies.
- Medicentres has established policies stating that Medicentres will act as the point of contact when dealing with the OIPC.
- In responding to investigations under the HIA, Medicentres and the physicians will cooperate.

[31] Next, when in January 2014 I asked Medicentres for a list of the physicians whose patients' health information was directly affected by this incident, Medicentres replied: "Considering the issues which have been identified for this investigation we do not see the need to breach the privacy of these physicians." Furthermore, when I posed questions to Medicentres about its relationship to the custodians and about the custodians' knowledge of the IT consultant's work, Medicentres offered no objection regarding its ability to respond to these questions without conferring with the custodians. It was only on May 14, 2014, fifteen weeks into the investigation and after it had seen a first draft of the investigation report, that Medicentres raised this concern.

[32] Last, in addition to the above documentary evidence, I note Medicentres' history in dealing with the OIPC:

- Medicentres has previously submitted privacy impact assessments (PIAs) to the OIPC signed by Medicentres officials on behalf of the custodians practicing at Medicentres; and,
- Medicentres has consistently reported previous privacy breaches to our office on behalf of the custodians at Medicentres (in these cases, Medicentres promptly informed the affected individuals).

[33] Medicentres' position that it is not responding to this investigation on behalf of custodians is inconsistent with the Practitioner Agreement, its own policies and past interactions with the OIPC. From January to May 2014, Medicentres certainly appeared to be responding to this incident on behalf of the custodians and it seemed Medicentres was authorized to do so by the same custodians through the Practitioner Agreement. In my view, Section 7.4 of the Practitioner Agreement created an expectation that Medicentres would be working in cooperation with the custodians when responding to this investigation under the HIA. This view is supported by Medicentres' actions.

[34] After carefully considering all of the foregoing evidence, I do not accept Medicentres' position that it is not responding to this investigation on behalf of the custodians, despite Medicentres' denial. If I am wrong in this conclusion, then Medicentres' role is unclear and that lack of certainty has the potential to place patients' privacy at risk in the future. Therefore, I will be recommending that Medicentres and the custodians clarify their roles and responsibilities under the HIA.

[35] Section 66(5) of the HIA cited above says information managers must comply with the HIA. The Commissioner has authority to investigate to ensure compliance with any provision of the HIA under section 84(1)(a) . Therefore, this investigation can, and has, proceeded with Medicentres as the respondent. As such, all findings in this investigation apply to Medicentres as an information manager to the custodians. At the same time, section 66(6) of the HIA says that custodians continue to be responsible for compliance with the HIA. This means that there are no findings for or against the custodians practicing at Medicentres in this report. However, the HIA says that the custodians whose patients' health information was affected by this incident are ultimately responsible for any contraventions of the HIA attributed to their information manager, Medicentres. This also means that all custodians practicing at Medicentres, whether their patients were affected by the incident or not, are responsible for Medicentres' continuing compliance with the HIA and any recommendations I make regarding HIA compliance.

[36] As mentioned above, the OIPC has previously reviewed Privacy Impact Assessments and privacy breach reports submitted by Medicentres, ostensibly on behalf of the custodians practicing there. The OIPC can only deal with persons who are subject to the legislation or persons who are authorized to deal with the OIPC on behalf of persons who are subject to the legislation. If, after all these years, Medicentres is now telling the OIPC that it never did, and does not now, have the authority to respond to the OIPC on behalf of custodians, there are consequences that flow from that denial. Specifically, I will be asking the Commissioner to review any PIAs that Medicentres previously submitted to the OIPC or may now have before the OIPC, to ensure, among other things, that only persons who are authorized to submit PIAs are signatories to those PIAs.

The IT Consultant

[37] The IT Consultant whose laptop was stolen is an employee of an information technology services provider based in Edmonton (the "IT Consulting Company"); the IT Consulting Company is one of a number of IT services providers for Medicentres. According to its agreement with Medicentres, the IT Consulting Company was contracted to supply consulting and support services to Medicentres with respect to the Medicentres IT systems. Therefore, the IT Consulting Company is a subcontractor to the custodians' information manager, Medicentres. The HIA does not provide specific guidance to custodians regarding subcontracting arrangements their information managers may make, but the HIA does impose a duty on information managers to comply with the HIA and with the terms of their agreement with the custodian (section 66(5) of the HIA).

Issues

[38] Because Medicentres has a general duty to comply with the HIA, I identified the following compliance issues in this investigation:

1. Did Medicentres collect, use and/or disclose health information with the highest degree of anonymity possible, in compliance with section 57 of the HIA?

2. Did Medicentres collect, use and/or disclose health information in a limited manner, in compliance with section 58 of the HIA?

3. Did Medicentres protect health information, in compliance with section 60 of the HIA?

4. Did Medicentres prepare and submit a privacy impact assessment, in compliance with section 64 of the HIA?

5. Is the Agreement Medicentres entered into with the custodians in compliance with section 66 of the HIA and 7.2 of the Regulations?

6. Did Medicentres comply with the HIA, its regulations and the agreement entered into with the custodians, in compliance with section 66(5) of the HIA?

Analysis and Findings

[39] During the course of my investigation, I communicated with Medicentres' officials. I also reviewed the facts of the incident, the security provisions in place on the laptop computer and the follow-up actions taken by Medicentres. My analyses of each of the issues above, and my findings, are set out below.

Issue 1: Did Medicentres collect, use and/or disclose health information with the highest degree of anonymity possible, in compliance with section 57 of the HIA?

[40] Under section 57(2) of the HIA, custodians and their information managers have a duty to collect, use or disclose health information with the highest degree of anonymity possible. Section 57(2) states:

> 57(2) A custodian that intends to collect, use or disclose health information must first consider whether collection, use or disclosure of aggregate health information is adequate for the intended purpose, and if so, the custodian must collect, use or disclose only aggregate health information.

[41] Medicentres reported that the health information in question was used to reconcile and manage AHCIP claims in the ATBA. Due to a high volume of billing activity across multiple sites, Medicentres determined that a system was required to manage AHCIP claims, specifically tracking unpaid (outstanding) billings for services provided by the custodians.

[42] The ATBA copies health information used for billing from the Medicentres electronic medical record system (EMR). Medicentres had been experiencing errors in its billing submissions and the IT Consultant was refining and troubleshooting the part of this application which produces a detailed "aged accounts receivable report". This report is generated to track unpaid AHCIP billings.

[43] In my opinion, reconciliation and troubleshooting is authorized under section 27(1)(g) of the HIA, which allows custodians and their information managers to use health information for internal management purposes and to process payment for health services (among other uses). At the same time, pursuant to section 57(2) of the HIA, health information must be collected, used and disclosed with the highest degree of anonymity possible.

[44] Medicentres reported that the source of the error or issue within the database was unknown and the consultant would have been unable to identify the error using aggregate or test data. Using identifiable health information allowed the IT Consultant to troubleshoot and discover the origin of the error.

[45] After taking into consideration the rationale provided to support the use of identifying health information it appears that Medicentres considered and rejected the use of aggregate health information for the intended purpose. As stated above the use of aggregate health information must be considered before collecting, using or disclosing identifiable health information. As Medicentres did so in this case, I find Medicentres complied with section 57(2) of the HIA.

Issue 2: Did Medicentres collect, use and/or disclose health information in a limited manner, in compliance with section 58 of the HIA?

[46] The HIA gives custodians broad authority to collect, use and disclose health information to provide health services and manage their practices. These tasks may be performed

by an information manager. This broad authority is, however, limited by an important duty to consider the amount of health information essential to the task. Section 58(1) says:

> 58(1) When collecting, using or disclosing health information, a custodian must… collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose.

[47] In this case, Medicentres reported that "…the consultant was provided with a copy of the database on [Medicentres'] secure network for purposes of testing and development" and that Medicentres determined that "all data parameters were required to identify errors and to modify and troubleshoot the ATBA". Medicentres also stated that it made the decision to give the consultant access to the ATBA database on behalf of the custodians and that the custodians "may not have been specifically aware of [the decision]". The IT Consultant then copied the database from Medicentres' network to his own laptop.

[48] I asked Medicentres whether providing the IT Consultant with access to a copy of the entire ATBA database was essential to carry out the intended purpose. Medicentres responded that "the consultant determined the amount of information that was required to properly test and validate the application." Medicentres said the IT Consultant determined:

- whether or not he required erroneous and non-erroneous data to test the ATBA
- the need to include or exclude outstanding, stale-dated and unreconciled claims to test the ATBA
- the need to include or exclude all available claims on the database to test the ATBA.

[49] Medicentres stated,

> …we required all of the individually identifying information to modify and troubleshoot the application. The application was identifying errors or issues with outstanding claims on the aged trial balance, the source of the problem could not be identified until further investigation was completed. The investigation required using all of the personal information parameters in the data on the laptop. This identifying data was necessary in the investigation process because it permitted identification of the specific claim problems.

[50] Medicentres has provided a plausible explanation as to why the IT Consultant needed access to the entire ATBA database. I am satisfied that Medicentres used only the amount of health information essential to carry out the intended purpose. Therefore, I find Medicentres complied with section 58(1) of the HIA. Whether it was appropriate to then store the entire ATBA database on a mobile device is a separate question that I consider next.

Issue 3: Did Medicentres protect health information, in compliance with section 60 of the HIA?

[51] I will now consider whether Medicentres took reasonable steps to protect health information as required by section 60 of the HIA, which states:

60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

(a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,

…

(c) protect against any reasonably anticipated

(i) threat or hazard to the security or integrity of the health information or of loss of the health information, or
(ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
and

(d) otherwise ensure compliance with this Act by the custodian and its affiliates.

[52] Additional security requirements are set out in section 8 of the *Health Information Regulation*. The relevant portions read as follows:

8(1) A custodian must identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information.

(3) A custodian must periodically assess its administrative, technical and physical safeguards in respect of …

(b) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information, and

…

(6) A custodian must ensure that its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information.

[53] Section 60 of the HIA and section 8 of the *Health Information Regulation* require custodians and their information managers to protect against reasonably anticipated threats to the security and confidentiality of health information. Laptop computers and other mobile devices are vulnerable to loss and theft. In my view, these threats are reasonable to anticipate. Following the theft of a laptop from a custodian in 2006, the former Commissioner made the following recommendations to all custodians in Alberta's health sector regarding the storage of health information on mobile devices:

- Perform a Privacy Impact Assessment (which should include an assessment of security risks) before implementing mobile computing.
- Do not store personal or health information on mobile computing devices unless you need to – consider technologies that allow secure, remote access to your network and data instead.
- If you must store personal or health information on a mobile device, use encryption to protect the data – password protection alone is not sufficient.
- Keep the amount of personal or health information stored on mobile computing devices to a minimum, based on your business needs.
- Periodically check your policies against practice to ensure they reflect reality and remain effective.

- Provide specific training on mobile computing to staff to ensure they understand the risks and understand how to protect their equipment. [OIPC Investigation Report H2006-IR-002, paragraph 62].

[54] The OIPC has issued several Investigation Reports since 2006 that repeat the above recommendations for the health sector, the public sector and the private sector. The OIPC has consistently found that failing to meet the above recommendations contravenes section 60 of the HIA, as well as the relevant provisions of Alberta's other privacy laws.

[55] In order to ensure health information is protected, custodians must identify areas of risk and implement reasonable safeguards to mitigate those risks. Further, custodians must maintain a written record of safeguards in place, ensure they are communicated to their affiliates, and monitor to ensure they are adhered to. As noted earlier, the custodians have authorized Medicentres to carry out these tasks through the Medicentres Practitioner Agreement. I will examine the administrative, technical and physical safeguards Medicentres had in place to meet the obligations set out under section 60 of the HIA and section 8 of the *Health Information Regulation*.

Administrative Safeguards

[56] Under section 63 of the HIA, custodians must "establish or adopt policies and procedures that will facilitate the implementation…" of the HIA and its regulations. Policies and procedures are essential as they provide affiliates with guidance on how to protect health information.

[57] One of the policies Medicentres established required all staff, contract workers and volunteers to commit to an Oath of Confidentiality and an IT User Agreement. Medicentres also established an Information Handling and Security – Technical Safeguards policy, which states "No confidential data is stored on local computer disks".

[58] Under section 8(6) of the *Health Information Regulation* custodians must ensure affiliates are aware of and adhere to administrative safeguards. In this case, Medicentres did not communicate its Technical Safeguards policy to the IT Consultant. Rather, Medicentres relied on a Confidentiality and Non-Disclosure Agreement to meet its obligation under section 8(6), stating,

> There was no requirement for the Confidentiality and Non-Disclosure Agreement to reference the Medicentres Information Handling and Security – Technical Safeguards policy specifically, as it was clear that the Consultant was not permitted to copy information without the permission of Medicentres. Clause 4C of the Confidentiality and Non-Disclosure Agreement, states 'The Consultant will not copy or reproduce any of the Confidential Information, except as expressly authorized in writing by Medicentres.'
>
> Medicentres had no knowledge that the database was copied onto the consultant's laptop nor did Medicentres authorize the database be copied onto the consultant's laptop. In fact, Medicentres provided the consultant access to the ATBA on a private, secure test and development area on a secure local server.

[59] I reviewed a copy of the Confidentiality and Non-Disclosure Agreement referenced above, which was signed by the CEO of the IT Consulting Company and Medicentres officials in January of 2008, almost 6 years before the incident that gave rise to this investigation. Other than the statement that the IT Consulting Company must "take all necessary security precautions, but in no event less than the precautions the Consultant takes to protect its own confidential information…".

[60] When interviewed for this investigation the IT Consultant provided his understanding of Medicentres' privacy and security requirements.

[61] Prior to the incident in question, the IT Consultant had worked for Medicentres for six years on various projects to automate payroll and billing reconciliation. Medicentres created a testing, staging and production environment for the ATBA (the "staging area" is where users are shown program changes prior to going live while the "production environment" is where software runs once fully implemented). However, according to the IT Consultant, Medicentres' IT infrastructure was unable to support the testing environment. The IT Consultant said that when he attempted to run test queries on the database, computer systems performance would degrade to unacceptable levels. Further, the testing tools he needed to do his work were not available in the Medicentres test environment. As a consequence, the IT Consultant said that he always kept a local copy of data. (A "local copy" refers to a copy stored on his computer, rather than a computer in the Medicentres environment.)

[62] When asked whether Medicentres knew about this local copy, the IT Consultant provided emails showing he communicated with Medicentres officials regarding the transfer of payroll and billing data between himself and Medicentres for various projects. The dates of the emails range from 2008 to 2011. One of the emails from 2008 referred to the IT Consultant and Medicentres using a File Transfer Protocol (FTP)[3] service to allow him to copy data. Notably, this email dates from just three months after the IT Consulting Company and Medicentres signed the Confidentiality and Non-Disclosure Agreement, prohibiting data copying without Medicentres' express permission. The IT Consultant said that Medicentres later allowed him remote access to its systems via a Virtual Private Network (VPN)[4]. I was not provided any evidence that this activity was sanctioned with Medicentres' "express permission". This is inconsistent with the terms of the Confidentiality and Non-Disclosure Agreement.

[63] The IT Consultant reported that he had received the Confidentiality and Non-Disclosure Agreement via cc in an email. However, no one from Medicentres or his own company had reviewed the Agreement with him. Further, he confirmed Medicentres did not

[3] File Transfer Protocol ("FTP"): A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.).

[4] Virtual Private Network ("VPN"): A secure private network that uses the public telecommunications infrastructure to transmit data. http://www.isaca.org/Pages/Glossary.aspx

provide any guidance to him or to his company regarding IT security, Medicentres' policies or the HIA.

[64] According to the IT Consultant, Medicentres had a long-established practice of allowing him to copy health information outside of their secure network to perform tests and otherwise provide IT support. While there was no explicit authorization in place to allow the IT Consultant to copy the ATBA database to his computer, the emails he provided indicate Medicentres was not enforcing the Confidentiality and Non-Disclosure Agreement. For example, in a 2011 email the IT Consultant refers to downloading data to his laptop. To further illustrate this pattern, the IT Consultant provided a more recent email from 2013, showing that he and Medicentres were exchanging data via Dropbox, an internet-based file storage and sharing service. This activity appears unrelated to the ATBA, but shows the IT Consultant and Medicentres exchanging data outside Medicentres' secure network without explicit authorization, in apparent contravention of the Confidentiality and Non-Disclosure Agreement.

[65] At one point in this investigation, Medicentres asked, "How exactly should Medicentres, short of watching every keystroke made, have monitored the consultant when there were administrative safeguards and secure areas for the consultant to carry out its work"? In follow up, the OIPC asked Medicentres what reasonable steps it had taken to monitor the IT Consultant's compliance with the Confidentiality and Non-Disclosure Agreement between 2008 and the date the laptop was stolen. Medicentres refuted the notion that there was any requirement to monitor compliance.

[66] Under section 60(1)(d) of the HIA, a custodian must take reasonable steps to ensure its affiliates are compliant with the HIA. Furthermore, under section 8 of the *Health Information Regulation,* custodians must periodically assess their administrative, technical and physical safeguards and ensure their affiliates are aware of and adhere to said safeguards.

[67] It is impossible to implement the HIA provisions without taking some reasonable steps. As stated above, section 8 of the *Heath Information Regulation* requires a custodian to carry out periodic assessment and review of safeguards and ensure affiliates are adhering to those safeguards. Some common methods used to ensure compliance include:

- Regular privacy and security training,
- Signing of confidentiality agreements,
- Regular auditing,
- Sign off on privacy and security policies and procedures.

[68] In response to the above, Medicentres submitted 44 pages of email correspondence between itself and the IT Consultant, sent between 2008 and 2013. The emails document discussions between Medicentres and the IT Consultant regarding connectivity, testing and ongoing projects.

[69] Medicentres stated the emails demonstrate that "Medicentres is communicating with the consultant and reasonably monitoring security and access of health information and compliance". Medicentres also stated, "the consultant has always sought permission from Medicentres for changes to access, changes to agreed upon work processes and changes that may impact security." Periodic assessment and review of safeguards is necessary to ensure affiliates continue to adhere to the HIA.

[70] The emails Medicentres submitted to the OIPC show the IT Consultant had some awareness of Medicentres' policies and procedures. The emails also show the IT Consultant had an awareness of the need for security and the protection of health information. However, in my opinion, this alone does not demonstrate compliance with the HIA. Medicentres provided no evidence to show it had taken any active steps to "periodically assess" its safeguards (to see if they were appropriate or effective) or to "ensure" that the IT Consultant was aware of and adhering to those safeguards. Medicentres also failed to provide evidence that the Confidentiality and Non-Disclosure Agreement had been refreshed or reviewed with the IT Consultant or the IT Consulting Company in the six years since it was signed.

[71] Medicentres failed to communicate its administrative and technical safeguards to the IT Consultant. Further, Medicentres did not take any action to periodically assess its safeguards, ensure the IT Consultant's compliance with the Confidentiality and Non-Disclosure Agreement or to enforce the Agreement. In my view, this does not meet the HIA requirement to take reasonable steps to ensure compliance with the HIA and to ensure adherence to Medicentres' safeguards.

Administrative Safeguards – Privacy Breach Response Policy

[72] Privacy breaches[5] may occur even when otherwise reasonable safeguards have been implemented. Therefore, it is reasonable for a custodian to anticipate that it will face a privacy breach at some point and to take reasonable steps to address the associated risks to privacy. Custodians typically respond to this risk by implementing a privacy breach response policy.

[73] All international information security and privacy standards the OIPC has reviewed include a breach or incident response policy. The Alberta Medical Association's HIA policy guide recommends that physicians establish breach response procedures[6]. The OIPC's *Privacy Impact Assessment Requirements for the* HIA[7] and *Getting Accountability*

[5] The HIA does not define the term "privacy beach." However, the OIPC Privacy Breach Reporting Form, which Medicentres used to report this incident, describes a privacy breach as follows:

> A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal or health information. The most common privacy breach happens when personal or health information about your employees, customers or patients is stolen, lost or mistakenly disclosed. Examples: computer, memory stick, or documents containing personal/health information are stolen; personal/health information is mistakenly emailed or faxed to the wrong person.

[6] Alberta Medical Association, 2003, *Health Information Act Guide to Policies and Procedures for Physician Offices*, https://www.albertadoctors.org/Advocacy/Advocacy_HIA__guide_to_Policies_and_Procedures_for_Physician_offices.pdf, p. 23.

[7] Office of the Information and Privacy Commissioner of Alberta, 2010, *Privacy Impact Assessment Requirements for use with the Health Information Act*, http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf, p. 38.

Right with a Privacy Management Program[8] both recommend establishing breach and incident management protocols. The OIPC does not accept Privacy Impact Assessments (PIAs) that do not include breach response policies and the vast majority of the over 4000 PIAs this Office has reviewed under the HIA do include such provisions.

[74] Therefore, to meet the current standard of reasonable safeguards[9] set in Alberta's health sector, custodians must implement a privacy breach response policy. The OIPC has provided guidance on privacy breach response,[10] which identifies four key steps in responding to a privacy breach:

1. Contain the breach
2. Evaluate the risks associated with the breach
3. Notify affected individuals
4. Prevent reoccurrence

[75] Medicentres has a "Privacy Breach Management Policy" that includes all of the above elements and, in fact, refers the reader to the OIPC's breach response guidance. I will analyze the effectiveness of Medicentres' privacy breach response in light of the OIPC's guidance later in this report. However, Medicentres has met the basic HIA requirement of implementing a breach response policy.

Physical Safeguards

[76] Common physical security measures that may be used to protect laptop computers include cable locks, locked hard cases, locking the laptop in a safe or other secure location, or locking the laptop in the trunk of a vehicle. In this case, the IT Consultant transported the laptop in a computer bag. No physical security measures were applied.

[77] As stated above, Medicentres has a policy and an Agreement in place with the IT Consulting Company to prohibit storage of confidential information on local computers. However, these arrangements were not enforced or monitored.

Technical Safeguards

[78] Medicentres described the following technical controls that the IT Consultant applied to the stolen laptop:

- the laptop's operating system was password-protected;

[8] Offices of the Information and Privacy Commissioner of Alberta and for British Columbia and Office of the Privacy Commissioner of Canada, 2012, *Getting Accountability Right with a Privacy Management Program*, http://www.oipc.ab.ca/Content_Files/Files/Publications/Accountability_Doc_April_2012.pdf, p. 14.

[9] Current industry best practice is a factor in determining what constitutes "reasonable steps." However, where an industry's current practice is sub-par, the OIPC may recommend a higher standard. In this case, this Office believes the current practice is reasonable.

[10] Office of the Information and Privacy Commissioner of Alberta, 2010, *Key Steps in Responding to a Privacy Breach*, http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf.

- the information in question was stored in a database system on the laptop, which also required a password;
- the passwords for the operating system and database accounts were different, were of reasonable length and included "complex characters" (i.e. capital letters, numbers and/or symbols);
- the laptop was set up so that the accounts would be locked after 3 failed login attempts;
- the custodians asserted that the database was set up in a semi-random way so that standard methods of viewing would yield unintelligible information; and
- the custodians claimed that the above protection was equivalent to encryption.

[79] In my view, the above measures would likely deter a casual attacker. However, someone with technical aptitude and time could access the health information stored on the laptop. Password cracking tools are widely available, free of charge on the internet. These tools circumvent systems that check for failed login attempts and can crack both operating system and database passwords. The format of the database may be difficult for someone unfamiliar with this format to view, but the database system on the laptop is in common use and free help is available online.

[80] Section 60 of the HIA says custodians must take "reasonable steps" to protect health information. Therefore, the standard of protection under the HIA is reasonableness, not perfection. To determine what is "reasonable", industry best practices and precedents set in past Investigation Reports issued by the OIPC should be considered. Since 2006 the OIPC has consistently found that password protection alone is not sufficient to safeguard health information [see Investigation Reports H2006-IR-002, P2006-IR-005, and H2007-IR-002]. Rather, the OIPC has said that encryption is the only reasonable way to protect health information stored on a mobile device. The current standard for taking "reasonable steps" to protect health information on a mobile device is to implement encryption. Therefore, although some technical security measures were in place to protect health information stored on the laptop, the information was not protected according to the current standard of reasonableness.

Overall assessment of safeguards

[81] Medicentres did not provide its policy prohibiting the storage of confidential information on local computer disks to the IT Consultant, nor did it enforce its agreement with the IT Consulting Company to this same effect. After being given access to a copy of the ATBA database on Medicentres' secure network, the IT Consultant copied the database to a mobile device. The IT Consultant did not encrypt the health information, nor were any physical security measures applied. Medicentres did not monitor to ensure its policy and the Agreement were being followed. This does not meet the reasonable standard of safeguards for mobile devices set in 2006, which has been consistently and publicly enforced since that time.

[82] Medicentres, as information manager, was authorized by the custodians to create and implement HIA policies and procedures. I therefore find Medicentres failed to take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information, in contravention of section 60 of the

HIA. Under section 66(6), the custodians continue to be responsible for Medicentres' compliance with the HIA.

Issue 4: Did Medicentres prepare and submit a privacy impact assessment, in compliance with section 64 of the HIA?

[83] Custodians have a duty under section 64 of the HIA to submit a privacy impact assessment (PIA) to the Commissioner before implementing a new administrative practice or information system that collects, uses, or discloses individually identifying health information. Section 64 of the HIA states:

> 64 (1) Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.
>
> (2) The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

[84] Medicentres has a privacy policy in place that covers PIA submission (HIA 3 Information Handling and Security policy). This policy states, "Before implementing new administrative practices or information systems related to the collection, use or disclosure of health information, Medicentres will complete a Privacy Impact Assessment (PIA) for submission to the Office of the Information and Privacy Commissioner."

[85] The OIPC's *Privacy Impact Assessment Requirements* (the Requirements) referenced earlier include guidance on determining if a PIA is required, when to submit a PIA, and the required format of the PIA. The Requirements state a PIA must be completed when there are changes to practices or systems or information management technology that stores health information.

[86] As stated previously, Medicentres determined that, due to the high volume of billing activity across multiple Medicentres sites, a new system was required to manage AHCIP claims. Medicentres implemented the ATBA database on May 2, 2011.

[87] In response to this investigation, Medicentres reported that a PIA was not completed before implementing the ATBA system. Medicentres did not believe that the ATBA posed any new risks to the privacy of the health information. The rationale for not carrying out a PIA was based on the following:

- the ATBA does not:
    - use or store any information that is not already in the electronic medical record (EMR);
    - collect new information (not already in the EMR), transmit or submit any information;
    - change data and there are no external linkages; and
    - provide access or information to any new parties.

- the information used by the accounting staff to perform reconciliation, collection and adjustments and other related accounting is the same as prior to May 2, 2011;
- the purpose for which the information is used has not changed from or prior to May 2, 2011;
- the users of the ATBA have access to the identical level of information in the EMR systems which are the minimum required to perform their jobs; and
- the ATBA is contained on secure servers on Medicentres' internal local network in the same manner as the existing EMR systems.

[88] Medicentres' rationale for not conducting a PIA for the ATBA appears to be based on a belief that the ATBA system is not qualitatively different from Medicentres' existing EMR system. This argument is at odds with Medicentres' previous assertion that the ATBA was needed to facilitate billing reconciliation (see paragraph 41 above). Based on Medicentres' submissions for this investigation, it is clear that the ATBA system was implemented to accomplish something the existing systems were unable to do – namely, reconcile billing activity across multiple Medicentres sites. In my view, this represents a new system and practice.

[89] Medicentres, as information manager to the custodians, added a new system and practice to the billing process by implementing the ATBA system. The system was implemented without conducting a PIA. Further, Medicentres implemented the ATBA system without consulting or informing the custodians. Therefore, I find that Medicentres, as information manager, contravened section 64 of the HIA when it failed to prepare and submit a PIA to the Commissioner for review and comment. Section 66(6) of the HIA states, "a custodian continues to be responsible for compliance with [the HIA] and the regulations in respect of the information provided by the custodian to the information manager".

Issue 5: Is the Agreement Medicentres entered into with the custodians in compliance with section 66 of the HIA and 7.2 of the Regulations?

[90] As stated earlier in this report, Medicentres provides storage, maintenance and retrieval of health information and other administrative functions to the custodians, making it an information manager as defined in the HIA.

[91] Section 66(2) of the HIA says "[a] custodian must enter into a written agreement with an information manager in accordance with the regulations…". Section 7.2 of the *Health Information Regulation* establishes the requirements for an agreement between a custodian and information manager. In summary, the agreement must include:

- the objectives and principles of the agreement;
- whether the information manager is permitted to collect, use or disclose health information on behalf of the custodian and for what purposes;
- whether and how the information manager is directed to respond to access and correction requests from individuals under Part 2 of the HIA;

- whether and how the information manager is directed to address individuals' expressed wishes about disclosure of their health information under sections 56.4 and 58(2) of the HIA;
- a description of whether and how the information manager is to protect, manage, return or destroy health information provided by the custodian; and
- set out how the agreement can be terminated.

[92] Medicentres reported that each custodian must enter into a Practitioner Agreement with Medicentres. I reviewed the Practitioner Agreement against the requirements of section 7.2 of the *Health Information Regulation* and note that it:

- sets out the principles and objectives of the agreement;
- states that Medicentres may collect, use and disclose health information on behalf of the custodians for management and billing purposes;
- authorizes Medicentres to release health information to patients on behalf of the custodians. Further details regarding how Medicentres and the custodians respond to access, correction and expressed wish requests are included in policies, which the Practitioner Agreement references, and which the parties agree to follow;
- provides a description of whether and how the information manager is to "protect, manage, return or destroy health information provided by the custodian"; and
- includes a termination clause.

[93] Overall, I find that the custodians have entered into an agreement with their information manager, as required by section 66(2) of the HIA, and that agreement addresses the requirements set out in section 7.2 of the *Health Information Regulation.*

[94] Despite my finding that the basic requirements of section 66(2) of the HIA and section 7.2 of the *Health Information Regulation* are met by the Practitioner Agreement, I have concerns about the accountability framework established therein.

[95] Under section 8 of the *Health Information Regulation*, custodians have a duty to maintain a written record of safeguards (section 8(1)), designate an individual responsible for security (section 8(2)) and periodically assess safeguards (section 8(3)).

[96] Under the terms of the Practitioner Agreement cited above, each custodian has authorized Medicentres to perform these duties under the HIA on their behalf.

[97] Of note, the Practitioner Agreement as written does not include any mechanism requiring that Medicentres report to the custodians about work Medicentres does on their behalf. The current privacy incident investigation is an example that illustrates why this is of concern. Under the terms of the Practitioner Agreement, Medicentres is not obliged to inform the custodians about privacy incidents and, in fact, did not officially inform the custodians about this incident until January 21, 2014.

[98] The mechanism I am referring to – a reporting structure whereby Medicentres regularly informs the custodians of matters related to HIA compliance, including privacy incidents

– is not specifically required by the *Health Information Regulation*; therefore, its absence does not represent a contravention of the HIA or the *Health Information Regulation*. Further, although Medicentres may not be contractually obliged to report to the custodians, the custodians are nonetheless responsible to ensure that Medicentres, as their information manager, complies with the HIA. Outsourcing health information management and HIA compliance to their information manager does not absolve the custodians of accountability.

[99] While the arrangement as set out in the Practitioner Agreement meets the basic requirements of the HIA and the *Health Information Regulation*, it poses problems for the custodians to meet their obligations under the HIA if they are not aware of or engaged in decisions made by their information manager on their behalf.

Issue 6: Did Medicentres, as information manager, comply with the HIA, its regulations and the agreement entered into with the custodians, in compliance with section 66(5) of the HIA?

[100] Section 66(5) of the HIA states:

> 66(5) An information manager must comply with
>
> (a) this Act and the regulations, and
> (b) the agreement entered into with a custodian
>
> in respect of information provided to it pursuant to subsection (3).

[101] I have found already that Medicentres contravened the HIA by failing to:

- take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information (section 60); and
- prepare and submit a privacy impact assessment to the Commissioner on behalf of the custodians (section 64).

In each case, Medicentres made the decisions that led to these contraventions, although the custodians are ultimately responsible.

[102] Nonetheless, in making these decisions, I find that Medicentres contravened the HIA, and specifically section 66(5)(a) which says that an information manager must comply with the HIA and the regulations.

Medicentres' Breach Response

[103] As part of my investigation of this matter, I reviewed Medicentres' response to the breach. Under the HIA, custodians have no legal requirement or duty to notify the Commissioner of a privacy breach, and no legal requirement to notify individuals affected by a breach. Further, the Commissioner does not have the power to require that custodians notify individuals about privacy breaches, or set terms and conditions

regarding the timeliness and form of notification. These matters are not HIA compliance issues.

[104] Nonetheless, the OIPC has published a number of guidance documents on its website to assist custodians, organizations and public bodies in responding to privacy breaches. In particular, Key *Steps in Responding to a Privacy Breach* (the Guide) was published in 2007, and subsequently revised and updated in 2010. The Guide sets out four key steps in responding to a privacy breach. The best practices in the Guide, including the four key steps, are very similar to those included in breach response guidelines issued by the Office of the Information and Privacy Commissioner for British Columbia, the Information and Privacy Commissioner of Ontario, and the Office of the Privacy Commissioner of Canada.

[105] Medicentres reported it was aware of the Guide and reviewed and applied it to the incident under investigation. In fact, Medicentres' Privacy Breach Management policy appears to be based on and refers to, the OIPC's Guide.

[106] I have reviewed Medicentres response to this incident against the four key steps in responding to a privacy breach, as outlined in the Guide.

Step 1: Contain the breach

[107] The Guide recommends that, in the event of a privacy breach, a custodian should take immediate steps to limit the breach by containing it (e.g. stop the unauthorized practice, recover the records, shut down the system, revoke access), ensure the staff responsible for privacy are made aware, and notify the police if theft or other criminal activity are at issue.

[108] Actions that could be taken to contain a breach resulting from a stolen or missing laptop include attempting to locate the missing laptop, remotely disabling the laptop (if the appropriate software is installed) or contacting the police.

[109] In this case, Medicentres reported they undertook the following steps to contain the breach.

- Contacted Medicentres' landlord regarding the incident.
- Engaged a Security Advisor who spoke to the administrative office staff where the laptop was stolen and he interviewed the IT Consultant to gather the facts and his further whereabouts on the day in question.
- Offered a reward (no responses received).
- Communicated with the Edmonton Police and provided all the information related to the incident. Police interviewed the IT Consultant who cooperated with the police investigation.
  Note: This is still an active police investigation and the laptop has not been recovered.

[110] In terms of the Guide's direction to ensure staff members responsible for privacy are aware of the breach, the IT Consultant reported the loss of the laptop to Medicentres. Medicentres informed the custodians in January, three months after the incident.

Step 2: Evaluate the risks associated with the breach

[111] The second step in responding to a privacy breach is to evaluate the associated risks. A number of factors to be considered are set out in the Guide, including the nature of the information involved, the cause and extent of the breach, the individuals affected by the breach, and the possible harm that could result from the breach.

[112] Medicentres formally reported this matter to the OIPC referring to the incident as a "possible privacy breach". Medicentres considered the risk of harm to be low because the laptop in their opinion had protection equivalent to that of encryption. However following an initial review of the facts the OIPC determined the incident gave rise to a risk of harm and informed Medicentres that the affected individuals should be notified.

[113] On October 28, 2013, Medicentres provided the OIPC with a written assessment of the risks associated with the incident, and requested that the OIPC "consider this information and reconsider the extent of the recommendation of the notification". Medicentres assessed the risk of harm resulting from this incident to be low for two reasons: first, the laptop contained two levels of password protection; and, second, the passwords for the two login accounts were different. Medicentres assessed this protection to be equivalent to that of encryption.

[114] After reviewing Medicentres' risk assessment, the OIPC wrote to Medicentres on November 18, 2013 stating "[t]he Commissioner has determined that password protection is not a sufficient safeguard in the protection of personal information. As a result of this, it is the position of this office that the information contained on the lost laptop could be accessed by an unauthorised user".

[115] For purposes of this investigation, I reviewed the risk assessment submitted by Medicentres. I considered the type of information at issue, the security measures in place to protect the information, the circumstances surrounding the loss of the laptop, the probability of the information being accessed, and the potential harm that could result.

[116] As outlined previously, the health information stored on the laptop included patient name, date of birth and personal health number, as well as diagnostic and billing codes.

[117] The laptop is assumed to be stolen, not lost. The laptop was password protected, but not encrypted. As discussed previously in my analysis of safeguards, someone with technical aptitude and time could break these passwords using freely available tools. Given the likely circumstance of theft, it is not unreasonable to assume that whoever took the laptop or whoever ultimately purchased it (if it has been sold) may have criminal intent.

[118] Patient name, personal health number, and date of birth are identifiers. The combination of three identifiers provides a starting point for a criminal to gather more information and may increase the possibility of the information being used to commit identity theft or fraud. Breach notification decisions issued by the OIPC under PIPA have found this to be the case.

[119] Health information is highly sensitive. The health information on the laptop included diagnostic and billing codes. These codes alone do not reveal the physical and mental health of an individual; however, the diagnostic codes used in Alberta follow the ICD9 international standard for diagnostic codes and their meaning can be found online. An individual's diagnostic, treatment and care information can be inferred from the information on the missing laptop. This information if accessed could be used to cause hurt or humiliation to the affected individuals.

[120] I consider identity theft, fraud, hurt and humiliation to be harms that might result from this incident. The information would be accessible by anyone with moderate technical aptitude. It is reasonable to assume that whoever took the laptop, or ultimately ended up with possession of it, had some criminal intent. For the above reasons, I consider there is a risk that harm could result from this incident.

Step 3: Notification

[121] The third step set out in the Guide is to consider whether notification of the affected individuals is necessary in order to avoid or mitigate harm. The Guide states that "[o]rganizations, public bodies or custodians that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs".

[122] During a conversation with Medicentres the day the incident was reported (October 10, 2013), the OIPC informed Medicentres that, based on an initial review of the circumstances, the affected individuals should be notified. Notification was again recommended in a conference call with Medicentres held on October 24, 2013, and again in the OIPC's November 18, 2013 letter to Medicentres.

[123] Following my review of Medicentres internal correspondence, I noted in an email from October 4, 2013 that Medicentres was considering notifying individuals. In their email Medicentres mention they will speak to the OIPC regarding notification options and the posting of a notice. Thereafter, Medicentres considered various methods of notification. For example, on December 11, 2013 Medicentres informed the OIPC of its intention to post notices in local newspapers prior to Christmas. On December 20, 2013, Medicentres advised the OIPC that the notification date was being moved to January 2014 due to concerns "that the notification would not reach as many affected individuals over the holiday season and [Medicentres] would have insufficient resources in place to handle incoming calls…". On January 8, 2014, Medicentres advised the OIPC that its plans had changed and direct notification was being considered. On January 17, 2014 Medicentres advised the OIPC that notices would be published in local

newspapers. Throughout this process, the OIPC repeatedly requested that Medicentres confirm its plans and provide copies of notification statements/advertisements.

[124] Medicentres ultimately decided to notify the affected individuals via a press release combined with notices on the Medicentres website and advertisements in the classifieds sections of the *Calgary Herald* and *Edmonton Journal*. The press release was issued on January 22, 2014; the website notice and newspaper advertisements appeared on January 23, 2014.

[125] The OIPC Guide says "[t]he preferred method of notification is direct – by telephone, letter or in person…". Indirect notification is an option, however, where…

> … direct notification could cause further harm, is prohibitive in cost, contact information is lacking, or where a very large number of individuals are affected by the breach such that direct notification could be impractical. Using multiple methods of notification in certain cases may be the most effective approach.

[126] Medicentres decided to notify affected individuals and decided the method and timing of that notification. In my view, given the number of individuals affected by this incident, indirect (or substitute) notice, in combination with website notices and a press release, is a reasonable method of notification. This approach is consistent with recommendations made by the OIPC in Investigation Report H2005-IR-001, which affected a similar number of individuals.

[127] I note again that the HIA does not require custodians to notify individuals affected by a privacy breach, and does not set any timelines for such notification. However, the primary purpose of notification is to ensure that individuals who may be at risk of harm resulting from an incident are able to take steps to mitigate that risk.

[128] With respect to timing, the OIPC's Guide states "[t]he most important step you can take is to respond immediately to the breach [emphasis in original]" and also "[n]otification of individuals affected by the breach should occur as soon as possible following the breach".

[129] Medicentres' own Privacy Breach Management policy states that "[t]he Privacy Committee, with assistance of the Clinic Manager and Medicentres IT Department (if required) will: consider … notification to affected individuals". Although the policy indicates that notification will be considered, there does not appear to be any direction that, once the decision is made to notify affected individuals, the notification should occur as soon as possible. Despite this lack of direction, my review of internal correspondence revealed Medicentres was concerned about the timeliness of notification in early December 2013.

[130] Finally, the OIPC Guide says consideration should be given to notifying parties other than the affected individuals. Medicentres notified the police and sent a formal report of the incident to the OIPC.

Step 4: Prevention

[131] With respect to the four key steps in responding to a privacy breach, the OIPC's Guide states "[y]ou should undertake steps 1, 2 and 3 … immediately following the breach and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies".

[132] Following the best practices set out in the Guide, the final step in breach response involves a thorough investigation of the cause of the breach, and developing, or improving as necessary, long term safeguards to protect against further breaches. Policies may need to be reviewed and updated, staff training should be undertaken to ensure employees are aware of their responsibilities. An audit should be conducted at the end of the process to ensure that the prevention plan has been fully implemented.

[133] In this case, while this investigation was underway, Medicentres undertook the following actions:

- set up a telephone helpline to respond to calls and questions about the incident (to date approximately 2700 individuals have contacted Medicentres);
- implemented new security procedures, including encryption on mobile devices;
- implemented a mobile device policy;
- committed to enforcing its policy to ensure consultants working with health information use Medicentres secure network and data is not removed from the network;
- implemented mandatory privacy and HIA awareness training for contractors and consultants and continued training for employees (The IT Consultant involved in the incident confirmed he took the Medicentres privacy training in an email dated December 16, 2013);
- reviewed physical security and implemented additional measures where necessary;
- completed review of HIA and IT policies and procedures;
- reviewed the use of encrypted, server-based hard drives as an additional security measure;
- submitted revised Information Manager and Practitioner Agreements to the OIPC for review;
- reviewed all relevant service agreements to ensure compliance with HIA where applicable; and,
- started work on a Privacy Impact Assessment (PIA) for the Aged Trial Balance application.

Overall assessment of breach response

[134] In this case, Medicentres had a breach response protocol in place, which in many ways incorporated the steps outlined in the OIPC's Guide. Medicentres attempted to contain the breach, and notified internal management, the police and the OIPC. Medicentres assessed the risk, made a decision to notify, and ultimately notified affected individuals through indirect (substitute) notice. From the date of the incident and throughout this

Commissioner-initiated investigation, Medicentres has taken preventative steps to reduce the risk of a reoccurrence.

[135] In my view, Medicentres followed the four key steps in responding to a breach, as set out in the Guide; however, Medicentres spent considerable time considering and rejecting various methods of notification. I note again that the HIA does not require custodians to notify individuals affected by a privacy breach, and does not set any timelines for such notification. Nonetheless, the OIPC's Guide states "[t]he most important step you can take is to respond immediately to the breach [emphasis in original]" and also "[n]otification of individuals affected by the breach should occur as soon as possible following the breach".

[136] Medicentres' internal breach response protocol, which is based on the OIPC Guide, addresses notification of individuals but does not provide any guidance concerning the timeliness of such notification. In my view this is a deficiency and I have made suggestion(s) to address this in my recommendations set out below.

Summary of Findings and Recommendations

[137] My findings from this investigation are as follows:

- Medicentres complied with section 57(2) of the HIA by considering whether collection, use or disclosure of aggregate health information was adequate for the intended purpose.

- Medicentres complied with section 58(1) of the HIA by only using the amount of health information essential to carry out the intended purpose.

- Medicentres failed to take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information, in contravention of section 60 of the HIA.

- Medicentres contravened section 64 of the HIA when it failed to prepare and submit a PIA to the Commissioner for review and comment.

- Medicentres has entered into an information manager agreement with the custodians as required by section 66(2) of the HIA and that agreement addresses the requirements set out in section 7.2 of the Health Information Regulation. However, the Practitioner Agreement as written does not include any mechanism requiring that Medicentres report to the custodians about HIA compliance work Medicentres does on their behalf. While not specifically required by the HIA or the Health Information Regulation, the lack of such an accountability mechanism is of concern, as the custodians do not always seem to be aware of or engaged in decisions made by their information manager on their behalf.

- Medicentres did not offer guidance to the IT Consultant regarding the protection of confidential health information or enforce their related agreement. Therefore Medicentres, as the custodians' information manager, failed to comply with section 66(5) of the HIA.

- Medicentres followed the four key steps in responding to a privacy breach, as set out in OIPC's published Guide; however, in my view, it spent considerable time doing so. Although Medicentres' internal breach response protocol addresses notification of individuals, it is deficient in that it does not provide any guidance concerning the timeliness of such action.

[138] Based on my findings, I made the following recommendations to Medicentres:

1) Review and, where necessary, modify the Practitioner Agreement to clarify Medicentres' roles and responsibilities (if any) in ensuring HIA compliance on behalf of the custodians, including responding to investigations, making submissions to the OIPC and communicating with the OIPC.

2) Cease collecting, using and disclosing health information via the ATBA system until the custodians (or Medicentres, if authorized by the custodians to do so) submit a PIA to the Commissioner for review and comment.

3) Submit a PIA to the Commissioner for the ATBA system within 30 days of receiving this report.

4) Review and update agreements with all IT services providers to ensure they comply with the HIA and *Health Information Regulation.*

5) Implement an internal governance mechanism that ensures the custodians are aware of and engaged in decisions Medicentres makes on their behalf regarding the collection, use, disclosure and protection of health information, including privacy incident reporting. This internal governance mechanism needs to be included in relevant agreements between the custodians and Medicentres, as well as in the privacy management sections of the PIA.

6) Review and revise Medicentres' Privacy Breach Management policy to ensure it includes guidance regarding the timeliness of notification, as well as consequences for breaching the policy.

7) If the use of mobile devices is considered in the future:

   - provide specific training to ensure all affiliates are aware of the risks associated with mobile computing.
   - give affiliates detailed instructions on securing mobile devices.

   or

- enforce existing policy and the Agreement prohibiting the storage of health information on mobile devices and ensure the policy is communicated to all affiliates.

8) Regularly train all staff, including contractors, on HIA policies and procedures.

9) Audit to ensure protective measures have been implemented. Report the results back to OIPC within 6 months.

10) Share this investigation report with all Medicentres custodians.

Conclusion

[139] Under the Practitioner Agreement, the custodians authorized their information manager, Medicentres, to carry out their duties regarding health information security. This investigation found that Medicentres contravened the HIA by failing to consider privacy risks and by failing to take reasonable steps to safeguard health information on a laptop computer. As custodians, the physicians practicing at Medicentres continue to be responsible for compliance with the HIA.

[140] Information managers and custodians subject to the HIA can learn from this incident. While it is permissible to authorize others to carry out duties regarding health information management and protection, custodians cannot divest themselves of responsibility. Custodians continue to be responsible for the actions of their information managers. Therefore, custodians need to be aware of and engaged in decisions their information managers make on their behalf.

Elaine Fitzgibbon
Senior Information and Privacy Manager