Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2019-IR-01

Investigation into alleged unauthorized accesses and disclosures of health information at Consort and District Medical Society Clinic

May 21, 2019

Dr. Peter Idahosa

Investigation 008702

Commissioner's Message

This investigation marks the fourth report over two years that I have released under the *Health Information Act* (HIA) where the focus of an investigation into a privacy breach shifted from an affiliate of the custodian to the custodian itself. This is a troubling trend.

This investigation did indeed find that affiliates (employees) of the custodian (physician) accessed and used patient information in contravention of HIA. However, the investigation also found that the physician failed to establish or adopt policies and procedures to facilitate implementation of HIA and the *Health Information Regulation*, and failed to ensure that employees were made aware of and adhering to the administrative and technical safeguards put in place to protect health information.

These are disappointing findings, considering that physicians previously practicing at the clinic submitted a PIA to my office in November 2013 which assigned responsibilities for privacy and HIA compliance, and included detailed policies and procedures concerning the collection, use and disclosure of health information at the clinic. My office accepted the PIA at the time, indicating that the policies and procedures were adequate to meet the requirements of HIA and safeguard against risks to privacy.

This investigation, however, found that when the physician began working at the clinic in 2015, he was not made aware of and did not appear to make any effort to become acquainted with the clinic's privacy policies and procedures. Further, an employee who knew that HIA policies and procedures had been developed in 2006 and updated in 2013, admitted that the PIA was in a binder that was "never opened" (the binder appears to be missing and was not accounted for during this investigation.)

Equally troubling is the fact the PIA submitted to my office in 2013 said, "We have educated our employees about our Privacy Policy and their role in protecting your privacy." Yet all employees interviewed for this investigation – including former employees not subject to the investigation – said they had never received privacy training.

I have frequently said that one of the most effective proactive measures in Alberta's privacy laws is the requirement under HIA for custodians to complete PIAs and submit them to my office for review. This helps to ensure that custodians develop and implement rigorous privacy management programs that include delegated responsibilities, policies and procedures, training and awareness, and safeguards to protect health information. However, there is no value in this exercise if a custodian considers completing a PIA to be a checklist activity, and that once the "box is ticked", the PIA can be shelved, never to be communicated, implemented, revisited or revised.

When my office accepts a PIA submitted by a custodian it is with the expectation that the controls described to protect patient privacy will be implemented immediately.

Not only does my office expect more of custodians when protecting patient privacy, Albertans do too. Protection of health information is consistently rated among the most important of privacy issues in public opinion surveys.

This investigation made four recommendations, including that the clinic complete a review of the implementation of safeguards at the clinic and report back to me on the review's findings.

Jill Clayton
Information and Privacy Commissioner

Contents

Background

[1] On July 4, 2016, the Office of the Information and Privacy Commissioner (OIPC) received a letter enclosing a "…Privacy Breach Report Form regarding privacy breaches that occurred at the Consort Medical Clinic in Consort, Alberta" from Dr. Peter Idahosa Professional Corporation. At the time, Dr. Idahosa practiced at the Consort Medical Clinic (the Clinic) as a family physician.

[2] The breach report said:

> On January 19, 2016 between approximately 22:30 to 23:10, [Employee A] (who was on… leave at the time) and [Employee B] gained access to the Clinic with keys and accessed the electronic medical records database known as Wolf using [Employee B's] access code. Medical records were accessed and may have been printed. On January 21, 2016, [Employee A] was still on … leave but visited the clinic during office hours and may have accessed a number of electronic medical records with [Employee B's] access codes. On February 10 and 11, 2016, while still an employee of the Clinic, [Employee A] accessed and may have printed electronic medical records of her friends and family members…

[3] The report also said that another staff member observed Employee A…

> …making multiple visits to the file room and making copies, as well as shredding paper on February 10 and 11, and subsequently leaving the clinic with concealed [sic] envelopes. However, we do not know what documents [Employee A] was copying and do not know what physical medical records, if any, were copied by [Employee A].

[4] In summary, the breach report alleged that:

- On January 19, 2016, between approximately 22:30 and 23:10, Employee A and Employee B (together, "the Employees") entered the Clinic and accessed the electronic medical records database using Employee B's access code. Medical records may have been printed.
- On January 21, 2016, Employee A was on leave but visited the Clinic during office hours and may have accessed a number of electronic medical records with Employee B's credentials.
- On February 10 and 11, 2016, Employee A accessed and may have printed, copied, shredded and/or taken medical records from the Clinic.

[5] The OIPC opened a self-reported breach file and assigned a Senior Information and Privacy Manager to follow-up with Dr. Idahosa (the Physician).

[6] On August 5, 2016, the Consort and District Medical Centre Society (the Society) notified individuals impacted by the reported breach that their health information may have been accessed in contravention of the *Health Information Act* (HIA).

[7] On October 13, 2016, based on information provided by the Physician and the Society, the Information and Privacy Commissioner (Commissioner) opened separate, related files to consider possible offences under HIA. The investigations were conducted between October 2016 and January 2018. In January 2018, the Commissioner determined that there was insufficient evidence to substantiate charges.

[8] The investigation nonetheless proceeded as a compliance investigation on the Commissioner's own motion under section 84(1)(a) of HIA (OIPC File #008702). The original self-reported breach file was closed at this time, as affected individuals had been notified.

[9] I was assigned to review and follow up the original breach report, investigate and collate information collected throughout these proceedings. This report outlines my findings and recommendations.

[10] As a matter of procedural fairness, it is the practice of the OIPC to send the parties a draft version of the investigation report so that they can advise us of any factual errors, and comment on any such error they identify during their review. On March 18, 2019, I sent a draft version of this investigation report to the parties for fact-checking.

[11] On March 20, 2019, the Physician, through his lawyer, objected to some of the findings in this report and offered information that contradicted evidence received or statements made by individuals during the investigation. In addition, the Physician's lawyer stated that "it is contrary to the principles of natural justice to make findings regarding [the Physician's] obligations under the *Health Information Act* without affording him an opportunity to be apprised of the allegations and an opportunity to respond to the information obtained through the investigation", on the basis that the Physician "was not interviewed as part of the above investigation nor was he given an opportunity to respond to statements by Employee A and Employee B concerning the Consort Medical Clinic's policies, procedures and practices regarding the handling of health information".

[12] In response to the assertion by the Physician's lawyer that I did not give the Physician the opportunity to respond or have input, I note that in the course of gathering evidence in this investigation, I had contacted the Physician's lawyer and requested information on the following occasions.

[13] On July 22, 2016 letter, I wrote to the Physician's lawyer to ask 10 questions about the breach the Physician had reported to our office. In her response, the Physician's lawyer asked to discuss my questions over the phone. My contemporaneous notes from this conversation indicate that the lawyer stated that "the Physician was a mere employee of the clinic, had not been there for long, and was not in a good position to be answering our questions, as he has not had a leadership role at the clinic".

[14] On March 23, 2017, I sent the Physician's lawyer a two-page letter asking the Physician to provide evidence on 16 points related to the investigation. The Physician's lawyer wrote back on March 24, 2017 that "[The Physician] has no documentation regarding privacy training provided to former employees nor does he have any information regarding privacy policies and procedures in effect at the Clinic at the time of the incident. [The Physician] was not the Clinic's Privacy Officer and was not in charge of privacy training… Given the above, it appears that the information you are seeking will need to come from the Clinic."

[15] On August 30, 2017 I sent the Physician's lawyer a three-page letter with 32 questions. In her September 20, 2017 response letter, the Physician's lawyer indicated that “in so far as questions that [the Physician] is able to answer, he started at the Consort Medical Clinic on November 9, 2015 and last worked there on October 27, 2016. [The Physician] has no information in respect of the other questions raised”.

[16] Where indicated in this report, it was revised based on the comments received from the parties, including the Physician.

Jurisdiction

[17] HIA applies to health information in the custody or under the control of a custodian.

[18] "Health information" is defined in section 1(1)(k) of HIA and includes "diagnostic, treatment and care information" as well as "registration information".

[19] Section 1(1)(i) of HIA defines "diagnostic, treatment and care information" as follows:

> (i) "diagnostic, treatment and care information" means information about any of the following:
>
> (i) the physical and mental health of an individual;
>
> (ii) a health service provided to an individual…

[20] "Registration information" is defined in section 1(1)(u) of HIA as follows:

> (u) "registration information" means information relating to an individual that falls within the following general categories and is more specifically described in the regulations:
>
> (i) demographic information, including the individual's personal health number;
>
> (ii) location information;
>
> (iii) telecommunications information;
>
> (iv) residency information;
>
> (v) health service eligibility information;
>
> (vi) billing information…

[21] The information at issue in this matter is maintained in the Clinic's electronic medical record (EMR), and includes the name, personal health number and contact details of patients who received health services at the Clinic, as well as diagnostic, treatment and care information about health services provided by physicians at the Clinic. I have reviewed records provided to me by the Physician and the Society and confirmed that this information is health information as defined in sections 1(1)(i) and 1(1)(u) of HIA.

[22] A "custodian" is defined in HIA to include a "health services provider who is designated in the regulations as a custodian…". Section 2(2)(i) of the *Health Information Regulation* (the Regulation) designates regulated members of the College of Physicians and Surgeons of Alberta as custodians.

[23] The Physician is a regulated member of the College of Physicians and Surgeons of Alberta and is therefore a custodian subject to HIA.

[24] The Consort and District Medical Society (the Society) is incorporated under Alberta's *Societies Act*. The Society's bylaws say:

> 1. The Society will be a joint committee of the Village of Consort (Province of Alberta) and the Special Areas Board representing the Minister of Municipal Affairs for the Province of Alberta hereafter referred to as the Parties.
>
> 2. The parties agree to form a joint committee known as the Consort and District Medical Centre Board to:
>
> - Operate and manage the Medical Clinic located in Consort, Alberta.
> - Operate and manage the rental housing provided for medical personnel
> - Represent the parties in the Committee responsible for recruitment and retention of doctors
> - Lobby and advocate for the delivery of health care services on behalf of the citizens within the boundaries. [my emphasis]

[25] As such, the Society is the legal entity that operates and manages the Clinic.

[26] According to the Society, the Physician "commenced full-time employment at [the Clinic] on November 9, 2015". An announcement at the time said that he had "signed a four year contract to provide services to Consort and area."

[27] The Society also confirmed that the Employees in this case were employed at the Clinic.

[28] Employee A commenced employment in or around September 2002. At the time of the incident, Employee A was the Office Manager. The Society provided me with the "Office Manager – Position Profile", which says that the Office Manager has "primary responsibility for all clinic operations and financial management".[1] The document details the Office Manager's specific duties which include, but are not limited to:

> - Analyze and balance staff workload and deploying staff to effectively support physicians…
> - Ensure clinic policies and procedures manual is documented, regularly updated, and distributed to all staff and physicians…
> - Ensure process documentation for all major clinic processes is documented, regularly updated and kept on file…
> - Ensure staff are trained and clinic is in compliance with the Health Information Act…
> - Ensure all information agreements are signed and current

[1] The lawyer for Employee A commented that "There was no 'Office Manager – position profile' in effect at the relevant time period – the information you've been given has come into effect since these issues". I have no way to verify this, but I note that Employee A's responsibilities related to ensuring compliance with HIA were also laid out in the privacy impact assessment that Employee A helped prepare, as discussed in paragraphs [93] to [97] of this report. The responsibilities set out above are similar to those in the privacy impact assessment.

[29] Employee B commenced employment with the Clinic in or around February 2008. Employee B's specific duties are outlined in the Clinic's "Reception Duties and Responsibilities" document which was provided to me by the Society. These duties and responsibilities include, but are not limited to:

- Importing electronic lab results and faxes…
- Greeting and interviewing patients to obtain medical information and correct demographics…
- Scheduling appointments and giving patients an appointment card when necessary..
- Taking vitals … and recording appropriately in the patient's chart…
- Checking EMR on an ongoing basis for instructions from the physician…
- Booking appointments for physician, PCN Nurse, PCN Dietician, and PCN Wellness Co-ordinator...
- Filing all faxes and scanned documents to patients charts…
- Charting relevant data into patients charts in the EMR (recording faxes sent, appointments received or booked, notifying patient of appointments, etc.)…
- Ensuring we have the patient's written consent when there's a request for releasing medical information, and scanning a copy to the patient's chart…
- Preparing chart transfers and insurance forms, and billing accordingly...
- Rescheduling appointments when the schedule is changed or the physician is called away for an emergency…
- Recalling patients and booking follow-up appointments at the physician's request…

[30] Section (1)(1)(a) of HIA defines an "affiliate" as "an individual employed by the custodian" or "a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian" [my emphasis].

[31] The Society has a contract relationship with the Physician, who is a custodian as defined in HIA. The Society operates and manages the Clinic and employed the Employees to provide services to support physicians practicing at the Clinic, including the Physician.

[32] I find the Society is an affiliate of the Physician who was employed (contracted) by the Society to practice at the Clinic. The Society employed the Employees to provide services to the Physician and therefore the Employees are also affiliates under the contractual relationship between the Society and the Physician.

[33] I note that the Society 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 HIA to which HIA applies, PIPA does not apply in this case.

Issues

[34] A number of issues were brought to my attention during the course of my investigation of this matter. My investigation, however, was confined to those matters that were raised in the original breach report submitted by the Physician to the OIPC. As such, my investigation concerns the following issues:

- Issue 1: Did Employee A and Employee B access and use health information on January 19, 2016, and if so was this access and use in compliance with sections 27 and 28 of HIA?
- Issue 2: Did Employee A access and use health information on January 21, 2016, and if so was this access and use in compliance with sections 27 and 28 of HIA?
- Issue 3: Did Employee A access, use, and/or disclose health information from the Clinic on February 10 and 11, 2016, and if so was this in compliance with sections 27 and 28, and Part 5 of HIA?
- Issue 4: Did the custodian (the Physician) take reasonable steps to maintain administrative, technical and physical safeguards to protect health information as required by sections 60 and 63 of HIA, and Section 8 of the *Health Information Regulation*?

Methodology

[35] I took the following steps during the course of this investigation:

- Sent written questions to lawyers representing the Physician and the Society, and reviewed their responses;
- Requested and reviewed copies of Clinic records, including EMR audit logs;
- Requested and reviewed Netcare audit logs;
- Reviewed the privacy impact assessment submitted, by physicians practicing at the Clinic, to the OIPC in November 2013; and
- Interviewed the Employees, as well as two other former employees of the Clinic.

Analysis and Findings

Issue 1: Did Employee A and Employee B access and use health information on January 19, 2016, and if so was this access and use in compliance with sections 27 and 28 of HIA?

[36] The breach report submitted by the Physician to the OIPC said:

> On January 19, 2016 between approximately 22:30 to 23:10, [Employee A] (who was on… leave at the time) and [Employee B] gained access to the Clinic with keys and accessed the electronic medical records database known as Wolf using [Employee B's] access code. Medical records were accessed and may have been printed.

[37] The report also said that:

> There are five patients confirmed to have had their medical records improperly accessed and reproduced by the Employees on January 19, 2016. They have no relationship with the Employees based on our understanding. … [Employee B] has confirmed in writing that she made copies of the medical records for a mediation with Dr. Idahosa and had redacted the patient names. Further, the patient records were not actually used, produced, or referenced at the mediation. According to [Employee B], the records were left with her legal counsel since the mediation.

[38] The Physician reported that the accesses were confirmed by a review of the Clinic's EMR audit logs. The Society confirmed this review was conducted by a Society Board Member and the Secretary to the Board (now Privacy Officer). I asked the Society to describe its review and explain on what basis it concluded that accesses to certain records were not authorized. The Society provided me with:

- EMR audit logs (which detail employees' use of the EMR, including the time and date information was viewed in patient records in the system);
- Clinic daysheets (a condensed list of patients to be seen, procedures, or tasks to be performed on a given day);
- Daysheets for the Big Country Primary Care Network (PCN);[2] and
- Messages and communications between Clinic staff and health care providers.

[39] The Society explained that it compared the EMR audit logs under each employee's user name with the Clinic and PCN daysheets. An access to the EMR was considered to be unauthorized if on the date of the access the patient did not have an appointment at the Clinic, or did not call, attend, receive lab results, was not referred to another health care provider, did not have messages or other communication with Clinic staff, or there was no other reasonable explanation for the access.

[2] At the time of the incident report by the Physician, the Clinic was part of the Big Country Primary Care Network, which accounted for certain patient consultations at the Clinic.

[40] The Physician said that, on January 19, 2016, Employee A was on leave from the Clinic. The Society provided a copy of an email dated January 17, 2016 and sent from Employee A to Society Board members advising that Employee A would be taking an "immediate 2-week" leave. Another email sent from Employee A to Society Board members advises that Employee A was authorized to return to work on February 3, 2016.

[41] In response to my questions, the Society reported that:

> To the Society's knowledge, during her… leave, [Employee A's] access to the Telus Wolf EMR was deactivated by [the Physician].

The Employees

[42] I conducted separate interviews with Employee A and Employee B.

[43] Employee A said the "Clinic Board" had requested a mediator be assigned to assist with resolving a conflict between employees and the Physician. Employee A had an appointment with the mediator on January 20, but was on leave from the Clinic (as of January 18) and out of town for the day on January 19. Employee A said she went to the Clinic at 10:30 p.m. on January 19 to access and retrieve messages that the Physician had sent to her from the EMR message system, in order to prepare for her meeting with the mediator the next day.

[44] When Employee A attempted to log in to the EMR the night of January 19, she found she was locked out. She said she called Employee B who came to the Clinic. Employee A reported that Employee B logged in to the computer with her user name and password, and then Employee A printed off messages. Employee A said that "quite often" the relevant messages were linked to a patient's file in the EMR, so Employee A "cut out all the patient names from the sheets and shredded them".

[45] Employee A said that she was at the Clinic for 45 minutes to an hour.

[46] Employee B said that, after a meeting with Board staff and the Physician that took place on January 13, 2016, "it was mentioned that maybe we should have a mediator". Over "the next few days we were notified we were getting a mediator come in [sic]". Employee B said that "we wanted to gather up our information so we could go to mediation prepared to show how we were being treated". On January 19, Employee A called her and said she couldn't get on to the computer to log in. Employee B went to the Clinic and "printed off our messages". She said "we cut out the patient names and photocopied and then shredded the original that had the cutout". Employee B confirmed she was at the Clinic for 45 minutes to an hour.

Analysis

[47] Section 27(1) of HIA sets out the purposes for which a custodian may use health information:

> 27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:

(a) providing health services;

(b) determining or verifying the eligibility of an individual to receive a health service;

(c) conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;

(d) conducting research or performing data matching or other services to facilitate another person's research…

(e) providing for health services provider education;

(f) carrying out any purpose authorized by an enactment of Alberta or Canada;

(g) for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

[48] Section 28 of HIA states that, "An affiliate of a custodian must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian". It follows that an affiliate may use health information only for purposes set out in section 27 of HIA.

[49] HIA defines "use" to mean to apply health information for a purpose and includes reproducing the information, but does not include disclosing the information" (section 1(1)(w)).

[50] I reviewed a copy of the audit logs from the Clinic's EMR and confirmed that patient records were accessed in the EMR using Employee B's login credentials, after 10 pm on January 19, 2016.

[51] The Employees also confirmed they accessed the Clinic after hours on January 19, 2016. Employee A was on leave from the Clinic at the time, and her credentials to access the EMR had been suspended. Employee B logged on to the system, and both Employees said they printed patient information and redacted individually identifying health information prior to removing documents from the Clinic. This was done for the purpose of preparing for a meeting with a mediator the next day as part of dispute resolution proceedings.

[52] Section 27 of HIA does not authorize accessing and using patient health information for purposes of preparing for a meeting with a mediator as part of dispute resolution proceedings. This access and use of health information was also not in accordance with the Employees' duties to the Physician. At the time, Employee A was on leave from the Clinic and her login credentials had been revoked. As such, there could be no accesses by Employee A to health information that would be in accordance with her duties to the Physician.

[53] I find that Employee A and Employee B accessed and used health information in the Clinic's EMR on January 19, 2016 in contravention of sections 27 and 28 of HIA.

Issue 2: Did Employee A access and use health information on January 21, 2016, and if so was this access and use in compliance with sections 27 and 28 of HIA?

[54] The breach report submitted by the Physician to the OIPC said, "On January 21, 2016, [Employee A] was still on… leave but visited the clinic during office hours and may have accessed a number of electronic medical records with [Employee B's] access codes."

[55] I asked Employee A about the alleged accesses on January 21, 2016. She said that she went to the Clinic after attending a meeting with the mediator on that day. She said that the Physician had added a Saturday to his work schedule and she was "the only one who knows how to open up the scheduler". She said that she was still locked out of the EMR so she "sat down at the receptionist's desk to set it up quickly". When asked if the Physician had requested that she come in to do this work, Employee A said "that's just the kind of person I am… constantly thinking about work. He wouldn't have been able to book any appointments for his Saturday clinic".

Analysis

[56] As noted previously, a custodian may only use health information for purposes authorized under section 27 of HIA. An affiliate must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian (section 28). It follows that an affiliate may use health information only for purposes set out in section 27 of HIA.

[57] Section 27(1) authorizes a custodian to use health information for various purposes, including "providing health services" and "internal management purposes". HIA contemplates that there are times when health information needs to be accessed and used to manage a medical clinic, which would include patient scheduling.

[58] At the time of the alleged unauthorized access (January 21, 2016), however, Employee A was on leave and her login credentials had been revoked. Employee A confirmed that she nonetheless attended the Clinic on that day and accessed the EMR using the computer at the reception desk. As Employee A's credentials had been revoked, there could be no accesses by Employee A to health information in the EMR that would be in accordance with her duties to the Physician. Further, she confirmed the Physician did not ask her to do this work.

[59] During this investigation, the Clinic provided me with Employee B's EMR audit logs, which I reviewed to attempt to ascertain whether Employee A accessed health information on January 21, 2016 when she used Employee B's EMR account to "open up the scheduler". These audit logs show many accesses to health information for the morning of the day in question.[3] However, since Employee A's use of the EMR that morning is undistinguishable from Employee B's, I am unable to determine which patients' health information, if any, was accessed by Employee A when she used Employee B's EMR account. Therefore, my review of audit logs is inconclusive.

[3] The lawyer for Employee A commented that, "On January 21, employee A accessed the EMR to access the Scheduler only – no patient records were accessed this day".

[60] I find that, to the extent that Employee A accessed or used health information in the Clinic's EMR on January 21, 2016, she contravened sections 27 and 28 of HIA.

Issue 3: Did Employee A access, use and/or disclose health information from the Clinic on February 10 and 11, 2016, and if so was this in compliance with sections 27 and 28, and Part 5 of HIA?

[61] The breach report submitted by the Physician to the OIPC said:

> On February 10 and 11, 2016, while still an employee of the Clinic, [Employee A] accessed and may have printed electronic medical records of her friends and family members. This was subsequently discovered following an internal investigation and audit of the Clinic's electronic medical record system.

[62] More specifically, the Physician reported:

> We have also confirmed that 16 patients had their records accessed and possibly reproduced by [Employee A] on February 10 and 11, 2016. At approximately 2:30 pm on February 10, 2016, [Employee A] was advised that February 11, 2016 would be her last day at the Clinic. The 16 patient files that we confirm were accessed improperly all belonged to [Employee A's] friends (including [Employee B]) and families, and [Employee B]'s family members, which were confirmed through Wolf by the Physician to not have received treatment on those days. While we cannot determine with any certainty [Employee A's] intentions, we find it likely that [Employee A] was attempting to facilitate the transfer [sic] all of her family and friends who were patients of the Clinic to another medical clinic and family physician that she currently works at.

[63] The report also said that another staff member observed Employee A…

> …making multiple visits to the file room and making copies, as well as shredding paper on February 10 and 11, and subsequently leaving the clinic with concealed envelopes. However, we do not know what documents [Employee A] was copying and do not know what physical medical records, if any, were copied by [Employee A].

[64] In summary, the Physician reported that on February 10 and 11, 2016, after Employee A returned from leave and her login credentials were restored, she "accessed and may have printed medical records of her friends and family members". The Society confirmed these accesses occurred by examining the EMR audit logs (using the process described previously in this report). The breach report also suggested the Employees may have been motivated to facilitate the transfer of these patients' care to another medical clinic.

[65] During this investigation, in response to my questions, the Society described its practices for file transfers as follows: [4]

> (a) A heath [sic] care provider requests a patient's chart transfer of specific result via fax (with the patient name and consent). Alternatively, a patient requests transfer of his or her chart.
>
> (b) The patient reviews and signs the consent to disclosure form…
>
> (c) The patient's signed consent disclosure form is reviewed and signed by the physician.

[4] On March 19, 2019, the lawyer for Employee A stated that the file transfer process described by the Society "was not in effect at the relevant time – there were no guidelines or written process in place for staff to follow."

(d) The patient is notified that he or she will be charged… for the chart transfer.

(e) The patient's chart is printed from the Telus Wolf EMR.

(f) The physician reviews the patient's chart to ensure it is complete.

(g) Once payment for the chart transfer is received, the patient's chart is transferred within 30 days.

(h) The patient's chart is transferred via:

I. Inter Hospital: if it is within the range of service

II. Fax: if it is outside the range of service for Inter Hospital

III. Xpress Post with signature: if it is outside the range of service for Inter Hospital and is too large to be faxed.

[66] The Society reported that, "The treatment and medical care of patients, including file transfers, was overseen by the physicians in the [Clinic]. To the Society's knowledge, [Employee A] did not have delegated authority to transfer files prior to the arrival of [the Physician]" and "… did not transfer files prior to the arrival of [the Physician]". Further, "To the Society's knowledge, [Employee A] did not have delegated authority to transfer files during [the Physician's] tenure at the [Clinic]" [my emphasis].

[67] In later correspondence, the Society confirmed…

> … that it was not standard practice in the Clinic for an employee to use a physician's letterhead without the physician's authorization or for an employee to sign on a physician's behalf when corresponding with an insurance company without the physician's authorization. For insurance reasons, all file transfers had to be discussed and approved by the attending physician.

[68] I asked Employee A about the allegations and her activities at the Clinic on February 10 and 11. She said that a number of patients had requested that their medical records be transferred to another health care provider, and there was a backlog of transfer requests that she executed. She said that "every single one of them had signed a patient transfer form that they wanted their records…".

[69] Employee A described the transfer process, saying that "we would … have them come in and sign a consent form to release information". I asked if the physician signed off on the transfer, and was told, "No, no they didn't need to sign off".

[70] With respect to accesses to patient information in the EMR that the Physician and Society had determined to be unauthorized, Employee A expressed concern about the process used to determine that such accesses were "breaches" by noting that, "If patients weren't on the schedule they considered it a breach". She explained that often she would "be doing things for a patient on a given day, even if they didn't attend". She gave examples of referral letters, patients calling to change contact information, scanning documents, receiving CT scans and ultrasounds. All of these activities might result in changes to a patient's EMR

record, and an entry on the system's audit log, despite the fact the patient did not attend at the Clinic on a particular day.

[71] I also asked Employee B about the activities at the Clinic on February 11, noting the allegation that a number of patient chart transfers on that day involved Employee B's relatives and friends. Employee B confirmed that February 11 was Employee A's last day in the Clinic and that once Employee A left, there would be "no staff left to do transfers. If a person wanted a chart transferred, it was then…". Employee B described the process as a "patient would call in asking" for a transfer. When I asked, "Does the doctor sign off?" Employee B responded, "No, he didn't".

[72] Similar to Employee A, Employee B also expressed concerns about the process the Physician and Society used to determine that accesses to patient information in the EMR were unauthorized, explaining that there were a variety of circumstances that would result in changes to a patient's record in the EMR, despite the patient not attending at the Clinic on a particular day. These examples included importing lab test or ultrasound results, CT scans, MRIs, standing requisitions for blood sugar levels, or patients calling in asking for a telephone number of a specialist. With respect to this last example, she noted that it "wasn't possible" to go into the chart and document every time such a request was made.

[73] The other former Clinic employees I interviewed confirmed that Employee A was responsible to respond to requests for transfer of patient charts, but were not aware of the exact process to be followed.

Analysis

[74] Under section 27(1) of HIA, a custodian may use health information for various authorized purposes, including "providing health services" (section 27(1)(a)) and "carrying out any purpose authorized by an enactment of Alberta or Canada" (section 27(1)(f)). An affiliate must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian (section 28). It follows that an affiliate may use health information only for purposes set out in section 27 of HIA.

[75] Transferring a patient's file to another health care provider qualifies as a disclosure of health information under HIA. Part 5 of HIA deals with the disclosure of health information. Section 34(1) of HIA authorizes disclosure with consent, and says:

> 34(1) Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure.
>
> (2) A consent referred to in subsection (1) must be provided in writing or electronically and must include
>
> (a) an authorization for the custodian to disclose the health information specified in the consent,
>
> (b) the purpose for which the health information may be disclosed,

(c) the identity of the person to whom the health information may be disclosed,

(d) an acknowledgement that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent,

(e) the date the consent is effective and the date, if any, on which the consent expires, and

(f) a statement that the consent may be revoked at any time by the individual providing it.

[76] Health information may also be disclosed without consent in a number of circumstances, including "to another custodian for any or all of the purposes listed in section 27(1)" of HIA (section 35(1)(a)).

[77] Section 41(1) of HIA requires a custodian to keep a record of any disclosures made under section 35(1) as follows:

> 41(1) Subject to subsection (1.1), a custodian that discloses a record containing individually identifying diagnostic, treatment and care information under section 35(1), (4) or (5) must make a note of the following information:
>
> (a) the name of the person to whom the custodian discloses the information;
>
> (b) the date and purpose of the disclosure;
>
> (c) a description of the information disclosed.

[78] Similarly to section 28, section 43 of HIA says that an affiliate of a custodian must not disclose health information in any manner that is not in accordance with the affiliate's duties to the custodian.

[79] The above noted provisions authorize the disclosure of health information when a patient has requested that their health record be transferred (disclosed) to another health care provider. A custodian may also remain the primary health care provider, but nevertheless disclose health information to another custodian who is supporting the provision of care or providing specialist services. Under HIA, however, all such disclosures must be documented.

[80] In order to respond to requests for transfers of health records, Employee A would have had to access certain health records for the purpose of reproducing them and prepare these copies for disclosure to the respective individuals who requested them. This would be a "use" of health information as defined in section 1(1)(w), and this use would have been authorized under section 27(1)(f) as it would have been for a purpose authorized under HIA. It is possible that the accesses reported by the Clinic on February 10 and 11, 2016 are reasonably explained by patient requests to have their medical records transferred to other health care providers. It is also possible that other accesses to patient information in the EMR on those days were related to informal requests for disclosure of health information made by patients or other custodians.

[81] In the course of this investigation, I obtained evidence suggesting that at least some patients had requested the transfer of their charts and provided consent for the related disclosure of

their health information. As far as the process to be followed in response to these requests, I received different information from every party I interviewed.

[82] During this investigation, the Clinic also provided me with both completed and blank copies of consent forms in use during the Physician's tenure at the Clinic. Upon examining these, I noted that they fail to include some of the elements listed under section 34(2).

[83] On March 20, 2019, the Physician's lawyer commented that: "[The Physician] has advised that at all relevant times while he was at the Clinic, he used a form that he received from the Alberta Medical Association that was HIA compliant." During the investigation, I sought to obtain evidence from the Physician in relation to file transfers, which he did not provide at the time. He has provided only an unsupported statement now. Furthermore, that statement would not assist the Physician when non-compliant forms are received from other custodians.

[84] Given that the consent forms relied upon by the Clinic do not conform to the requirements listed under section 34(2) of HIA, disclosures of health information based on these completed consent forms would not comply with Part 5 of HIA. However, disclosures to other custodians could still be compliant with Part 5 of HIA, if the disclosures of health information were necessary to support the provision of health services, since section 35(1)(a) does not require an individual's consent. Therefore, in order for any of Employee A's disclosures to comply with Part 5 of HIA, they would have to have been made to other custodians providing health services to the individuals whose health information she used and disclosed.

[85] I find that to the extent that Employee A disclosed copies of health records of patients of the Clinic to other custodians to support their provision of health services to these patients, Employee A's accesses to these individuals' health information were authorized under sections 27 and 28 of HIA, and the disclosure of this health information was authorized under section 35(1)(a). In order for the disclosures to comply with Part 5 of HIA, Employee A would have had to file the documentation supporting these disclosures of health information to each individual's chart in the Clinic or in a centralized disclosure log in order to comply with section 41(1).

[86] I also find that to the extent that Employee A disclosed copies of health records from patients of the Clinic to non-custodians, or to custodians for purposes unrelated to the provision of health services to these patients, then the disclosure of this health information was not authorized under section 35(1)(a) of HIA, and the related accesses were not authorized under sections 27 and 28. In such cases, Employee A's accesses to these individuals' health information contravened sections 27 and 28, and the disclosure was in contravention of Part 5 of HIA.

Issue 4: Did the custodian (the Physician) take reasonable steps to maintain administrative, technical and physical safeguards to protect health information as required by sections 60 and 63 of HIA, and Section 8 of the *Health Information Regulation*?

[87] Custodians have a duty to protect health information in their custody or under their control. Section 60 of HIA 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…
>
> (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
>
> (2) The safeguards to be maintained under subsection (1) must include appropriate measures
>
> (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records…

[88] Section 62 of HIA says:

> 62(1) Each custodian must identify its affiliates who are responsible for ensuring that this Act, the regulations and the policies and procedures established or adopted under section 63 are complied with.
>
> (2) Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

[89] Section 63(1) of HIA says:

> 63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

[90] Section 8 of the the Regulation states:

> 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…
>
> (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.

[91] These sections of HIA and the Regulation require that custodians identify threats to patient privacy and confidentiality and take reasonable steps to maintain administrative, technical and physical safeguards that will mitigate identified risks, including the risks of unauthorized access to and use of health information. Further, HIA specifically requires that measures be

taken to address the risks associated with electronic health records. Custodians are required to establish or adopt policies and procedures, and maintain a written record of the administrative, technical and physical safeguards that are implemented. Custodians must ensure their affiliates are aware of and adhere to administrative, technical and physical safeguards that have been implemented. Finally, any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

[92] I considered the safeguards that the custodians practicing at the Clinic, and the Physician, had in place to meet these obligations under HIA. Given the specific matters at issue in this investigation, I focused on administrative and technical safeguards.

Policies and Procedures

[93] In November 2013, the Clinic submitted a privacy impact assessment (PIA) to the OIPC as it was installing and implementing its Wolf EMR system. The PIA was signed by two physicians practicing at the Clinic at the time. Employee A was identified as the Clinic Privacy Officer, and it was her information that was provided to the OIPC as a contact should the OIPC have questions about the PIA. The Physician did not sign the PIA, as he had not yet commenced employment at the Clinic.

[94] The PIA included an extensive suite of policies and procedures to address the collection, use, disclosure and safeguarding of health information, including:

Privacy Charter

Health Information Privacy Practices

Policy#1	Right of Access
Procedure:	Release of Information & Disclosure Log
Policy #2	Correction or Amendment of Health Information
Policy#3	Collection, Use, and Disclosure of Health Information
Policy#4	Research
Policy#5	Information Handling
Policy #6	Information Security in Contracting
Policy#7	Wireless Networking and Remote Access
Policy#8	Privacy and Security Risks and Mitigation
Policy#9	Information Flow Diagram and Legal Authority Table, Workflow diagram
Procedure:	Privacy Breach Management
Procedure:	Quality Assurance Document Imaging (Scanning) to EMR
Attachment:	Employee Confidentiality and Security Checklist
Attachment:	EMR and Data Quality Assurance
Attachment:	Password Guidelines
Attachment:	Facsimile Transmission Guidelines
Attachment:	EMR Access Request

[95] Each of these policy documents said it was “Approved By” Employee A.

[96] The "Health Information Privacy Practices" document included with the PIA sets out the responsibilities of the Clinic's Privacy Officer. It says:

> 5.2 [Employee A] is designated as the Responsible Affiliate for the purposes of the HIA and given the title of clinic Privacy Officer.

[97] The responsibilities of the Clinic Privacy Officer include but are not limited to:

- "Ensuring that clinic health privacy and security policies and procedures are developed and maintained as necessary"
- "Ensuring that clinic staff and contractors are aware of their responsibilities and duties under HIA"
- "Ensuring the clinic obtains required consent with respect to the disclosure of health information where required"
- "Ensuring the overall security and protection of health information in the custody or control of the clinic per (HIA)…"
- "Ensuring that clinic staff or other affiliates sign a Confidentiality Oath and review clinic privacy & security policies and procedures at time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident/breach at the clinic"

[98] I also made a direct request to the Society for the Clinic's policies and procedures. The Society told me that a member of its Board had received a text message on February 11, 2016 from a Clinic employee saying that Employee A "really cleaned house today. A lot went in the shredder bin". Members of the Society went to the Clinic that day and found that "[Clinic] property had been removed or destroyed".

[99] The Society reported that the property that was allegedly removed or destroyed included, but was not limited to, operational manuals, confidentiality agreements, PIA documentation, emails, referral lists, employee records, and billing information.[5]

[100] I asked the Physician about Clinic policies and procedures. Legal counsel for the Physician advised me that the Physician "…has no documentation regarding privacy training provided to former employees nor does he have any information regarding privacy policies and procedures in effect at the Clinic at the time of the incident. [The Physician] was not the Clinic's Privacy Officer and was not in charge of privacy training". As previously noted, the PIA was signed by two physicians practicing at the Clinic at the time. The Physician did not sign the PIA as he was not employed at the Clinic in November 2013. I have no evidence that the Physician adopted these policies.

[5] In the course of commenting on the factual accuracy of this report, Employee A's lawyer stated that with regards to billing information, this was "not something [Employee A] was responsible for, never had possession of this material", even though that directly contradicted information contained in the above mentioned November 2013 PIA, as well as a statement made to me by Employee A in a recorded interview about her work duties at the Clinic. However, billing information is not relevant to this investigation.

[101] In my interview with Employee A, she confirmed that policies and procedures had been in place in the Clinic, saying "We did those up in 2006 … they were in the binder with the PIA". She did not mention updated policies from 2013, but said that the PIA binder (with policies and procedures) was "never opened". When I asked her about the allegation that she destroyed this documentation, she said, "No, I did not. I left it in my cupboard. The PIA document and all policies and procedures were in a binder in my cupboard and also on a disk in my drawer".

[102] Employee B did not recall ever being given a copy of the Clinic's policies and procedures although "there may have been one to review". She did not know if there were any policies and procedures in place or written down.

Confidentiality Agreements

[103] As noted above, section 8(6) of the Regulation states that, "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." This typically includes having employees sign confidentiality agreements, and ensuring they receive privacy awareness training with regular updates.

[104] The policies and procedures that the Clinic submitted to the OIPC in November 2013 include a template Confidentiality Oath, and a Privacy Charter that specifically says that the Clinic has implemented safeguards to protect health information, including "having employees sign oaths of confidentiality". Employee A's responsibilities as Privacy Officer include "ensuring that clinic staff or other affiliates sign a Confidentiality Oath" (Health Information Privacy Practices).

[105] The breach report originally submitted by the Physician to the OIPC says…

> …all employees of the Clinic are required to sign a confidentiality agreement as a privacy protection measure. The Employees both signed confidentiality agreements which were placed in a physical binder at the Clinic. We suspect that when [Employee A] left the Clinic, she either took the binder with her or otherwise destroyed the binder.

[106] When I asked Employee A if she had ever signed a confidentiality agreement she said "no" and also said that she "was pretty sure" that no employees at the Clinic ever signed such an agreement. She then clarified that in January 2016, the Physician asked her to draft a confidentiality agreement for Clinic staff, and he had her hand it out to the staff in the Clinic. She reported that "a number of them had signed" and that "all those confidentiality agreements should have been in my cupboard".

[107] She confirmed that she destroyed her own confidentiality agreement, and Employee B's "at [Employee B's] request". When I asked why she had destroyed the two confidentiality agreements, she said that she "didn't feel comfortable leaving it there" and she "didn't trust" the Physician.

[108] Employee B told me that when she started at the Clinic in 2008 "there was a form that [she] filled out" with a "small little excerpt in there about confidentiality". She also said that in January 2016, Employee A had given her a confidentiality agreement which Employee B read

and signed. Employee B gave the agreement to Employee A but asked her not to give it to the Physician and to shred it instead. I asked her why she asked Employee A to get rid of the document and was told that she "had no trust in [the Physician]" and she "didn't feel comfortable with him having a signed document of mine".

Privacy Awareness Training

[109] With respect to privacy awareness training, the Privacy Charter included in the PIA documentation submitted by the Clinic to the OIPC in November 2013 says, "We have educated our employees about our Privacy Policy and their role in protecting your privacy". Employee A, as Privacy Officer, was responsible for "ensuring that clinic staff and contractors are aware of their responsibilities and duties under HIA" and for ensuring that clinic staff or other affiliates "review clinic privacy & security policies and procedures at time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident/breach at the clinic". The Clinic's "Policy #5: Information Handling" also says that "confidentiality and security of information shall be addressed as part of the conditions of employment for all clinic staff, beginning with the recruitment stage, and included as part of job descriptions and contracts".

[110] The Clinic's "Section B: Organizational Privacy Management" document says that the Clinic has "Developed an ongoing personnel awareness and training program relevant to the protection and confidentiality of health information in accordance with the HIA". Further, "Our physicians, office administrator, and receptionists have participated in the development, review, and identification of potential privacy and security issues". The document lists the policies and procedures in place at the Clinic, and says "These polices are reviewed on a regular basis, and any changes are communicated to our clinic physicians and staff by the Clinic Privacy Officer. Our clinic staff also review the policies during their orientation and annually thereafter".

[111] I asked Employee A if she had received any privacy training at the clinic. She said "No actual privacy, confidentiality training whatsoever". Although, she also said that the "Telus Wolf guys… came out and showed us how to use the system".

[112] I noted that she was the Office Manager and asked if she had delivered training to staff. She responded "No" and also said that the policy and procedure binder was never shared with staff.

[113] Employee B said that when she started she did not receive any privacy training. She did not recall ever being given a copy of the Clinic's policies and procedures although "there may have been one to review". She didn't know if there were any policies and procedures in place or written down. I asked Employee B about her knowledge of the rules for collecting, using and disclosing health information and she confirmed that confidentiality "was strictly enforced". For example, she knew to "talk quietly on the phone" and not to leave "papers sitting on the desk as you walked away".

[114] When I spoke with other former employees of the Clinic, they confirmed the Employees' statements with regards to Clinic employee privacy training.

Technical Safeguards

[115] To a large extent, this investigation is concerned with unauthorized access to and use of electronic health records. Section 60(2) of HIA specifically requires custodians to maintain appropriate measures that address the risks associated with electronic health records.

[116] As set out in the OIPC's Investigation Report H2011-IR-004, reasonable technical controls include unique authentication and audit logs. Unique authentication means that each user is assigned an identification code and password that only that user can use. Audit logs are a record of the actions each uniquely identified user performs within a system.

[117] The PIA documentation submitted by the Clinic to the OIPC in November 2013 describes the Clinic's technical safeguards (Policy #5: Information Handling):

> 2.1 Information systems users are assigned a unique identifier (User ID) that restricts access to each data and application systems to that information required for the administration of their duties. Use of user IDs other than that assigned to an individual is prohibited. (Netcare pORA Requirement)…
>
> 2.3 Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes…
>
> 2.10 Each user should have a unique user login and password to access the computer network. User rights and accounts will be assigned and maintained by [Employee A]…

[118] In this case, the Clinic's EMR audit logs were used to confirm certain accesses to patient health information. As a safeguard, however, unique authentication is only effective if users do not share login credentials.

[119] The breach report submitted by the Physician to the OIPC alleged that Employee A and Employee B shared login credentials in order to access patient information in the EMR.

[120] Employee A confirmed that, on the evening of January 19 2016, while she was on leave, she attended at the Clinic and found that her login credentials had been revoked. She called Employee B, who came to the Clinic and logged on to the EMR. Both Employee A and Employee B then accessed and printed patient records using Employee B's credentials.

[121] Employee A also said that there were two computers at the reception desk, and "it wasn't uncommon for one receptionist to take a patient back and do their vitals and the other would jump up and sit down at the other computer and log in… The Dr. would often come in and sit down and look at a lab". Employee A explained that it was "not efficient to log off and log in".

[122] When I asked Employee B if she had ever shared her password or computer with colleagues, she told me, "No. My password is strictly mine". She added that no one else had ever shared their password with her. Nonetheless, Employee B confirmed that, on the night of January 19, 2016, she received a call from Employee A, who was at the Clinic but unable to log in to the EMR. Employee B went to the Clinic and "printed off our messages for the mediator. Just messages that [the Physician] had sent to us."

[123] Employee B also confirmed that the reception desk computers were "left open". She explained that the staff "trusted each other" and that they "didn't have time" to log on and off. Employee B said that the physicians in the Clinic would use the reception desk computers, and the physicians would, for example, "sit down at our computers and quickly do up a prescription".

Analysis

[124] When I requested that the Society provide me with policies and procedures for my investigation, I was told the documentation was not available as it had been destroyed by Employee A. Employee A denied doing so. Employee A and Employee B, however, both made statements indicating that policies and procedures were in place at the Clinic.

[125] Custodians previously practicing at the Clinic submitted a PIA to the OIPC in November 2013, which included detailed policies and procedures concerning the collection, use and disclosure of health information at the Clinic. The OIPC accepted the PIA at the time, indicating that the policies and procedures were adequate to meet the requirements of HIA and safeguard against risks to privacy. I reviewed these policies and procedures, and find that they document reasonable administrative, technical and physical safeguards for protecting health information.

[126] Despite the fact there were adequate policies and procedures in place in November 2013, there is no evidence that the Physician ever adopted them when he commenced employment with the Clinic in November 2015.

[127] As previously noted, during this investigation, the Physician's lawyer stated that he "…has no documentation regarding privacy training provided to former employees nor does he have any information regarding privacy policies and procedures in effect at the Clinic at the time of the incident".

[128] Despite this, after receiving a draft of this report, the Physician's lawyer commented that "[The Physician] was required to sign the Privacy Impact Assessment ('PIA') at the time that he started at the Clinic in November 2015 in order to gain access to the Clinic's Telus EMR".[6]

[129] The Physician, through his lawyer, provided differing statements with regards to his efforts to implement or adopt policies and procedures during his time at the Clinic. I note that the Physician's late statements in that regard were not supported by any evidence from him and were not supported by the other evidence I received and reviewed during this investigation.

[130] Given this, I find that the Physician was in contravention of section 63(1) of HIA which requires custodians to "establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations".

[6] Despite that statement, the requirement under section 64 of HIA is that a custodian must prepare and submit a PIA to our office for review, which the Physician did not do.

[131] With respect to privacy training and awareness, my interviews with the Employees and other employees of the Clinic indicate that there was no real training program to ensure staff awareness of the Clinic's policies and procedures:

- During the investigation, the Physician said he "…was not the Clinic's Privacy Officer and was not in charge of privacy training".

- On March 20, 2019, the Physician's lawyer commented that, "[The Physician] reached out to the Alberta Medical Association ('AMA') for assistance... Subsequently on January 20, 2016… AMA Practice Management Program attended at the Clinic to conduct training of office staff, which included training on the importance of confidentiality and handling of health information."

[132] Although the Physician, through his lawyer, stated during the investigation he was not in charge of privacy training, he later offered a contrary statement. Furthermore, the other evidence received during the investigation did not corroborate his statement that the Clinic employees received privacy training on January 20, 2016.

[133] The PIA documents submitted to the OIPC included template confidentiality agreements that purportedly all staff in the Clinic were required to sign. Employee B's responses to my questions suggest that she had, at some point during her employment, signed an agreement that addressed confidentiality. Both Employee A and Employee B confirmed that they had signed confidentiality agreements in January 2016, as initiated by the Physician, but had subsequently destroyed them. Other employees said that they could not remember with certainty signing a confidentiality oath when they started working at the Clinic, but that the Physician asked them to sign one in January 2016.

[134] I acknowledge that the Physician made some efforts in January 2016 to ensure that Clinic staff signed confidentiality agreements; however, overall, there is little evidence that employees received regular privacy training and awareness, or had any knowledge of the Clinic's privacy policies and procedures. Therefore, I find the Physician failed to ensure that Clinic employees were made aware of and adhering to the safeguards put in place to protect health information, in contravention of section 8(6) of the Regulation.

[135] With respect to technical safeguards to protect health information in the EMR from unauthorized access, the Employees said that unique credentials were assigned to all staff. Both also confirmed that, on the night of January 19, while Employee A was on leave and her credentials revoked, the Employees attended the Clinic and accessed patient information in the EMR using Employee B's credentials.

[136] The Employees also confirmed that it was common practice for many staff, including the physician custodians, to use the reception desk computers without any one user logging off or on. Sharing credentials in this manner completely defeats the purpose of implementing a unique log in access to a system.

[137] In her March 20, 2019 letter, the Physician's lawyer stated that "[The Physician] made reasonable efforts to ensure appropriate safeguards were in place at the Clinic to meet his obligations under the *Health Information Act*." However, this statement is not evidence.

Despite multiple opportunities to provide evidence both now and at the commencement of the investigation when the Physician was still at the Clinic, he did not provide any evidence.

[138] I find that reasonable steps were not taken to ensure that technical safeguards implemented in the Clinic were adhered to. It appears that this may have been a long-standing practice at the Clinic. Nonetheless, HIA requires custodians (including the Physician) to implement such safeguards. Section 8(6) of the Regulation specifically requires custodians to ensure that their affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information, and section 62(2) says that, "Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian".

[139] I find that the Physician contravened section 60 of HIA and section 8(6) of the Regulation when he failed to ensure that the Employees, and other Clinic staff, adhered to technical safeguards.

[140] Overall, these are disappointing findings to make. The custodians practicing at the Clinic, as well as Clinic staff, clearly made a significant effort to ensure that a reasonable privacy management framework was developed for the Clinic. However, the Physician failed to adopt this privacy management framework, and, along with previous custodians practicing at the Clinic, failed to follow through on commitments made in the PIA.

Summary of Findings and Recommendation

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

- Employee A and Employee B accessed and used health information in the Clinic's EMR on January 19, 2016 in contravention of sections 27 and 28 of HIA.

- To the extent that Employee A accessed or used health information in the Clinic's EMR on January 21, 2016, she contravened sections 27 and 28 of HIA.

- To the extent that Employee A disclosed copies of health records of patients of the Clinic to other custodians to support their provision of health services to these patients, Employee A's accesses to these individuals' health information were authorized under sections 27 and 28 of HIA, and the disclosure of this health information authorized under section 35(1)(a). In order for the disclosures to comply with Part 5 of HIA, Employee A would have had to file the documentation supporting these disclosures of health information to each individual's chart in the Clinic or in a centralized disclosure log in order to comply with section 41(1).

- To the extent that Employee A disclosed copies of health records from patients of the Clinic to non-custodians, or to custodians for purposes unrelated to the provision of health services to these patients, then the disclosure of this health information was not authorized under section 35(1)(a) of HIA, and the related accesses were not authorized under sections 27 and 28. In such cases, Employee A's accesses to these individuals' health information contravened sections 27 and 28, and the disclosure was in contravention of Part 5 of HIA.

- The Physician was in contravention of section 63(1) of HIA which requires custodians to "establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations".

- The Physician contravened section 60 of HIA and section 8(6) of the Regulation when he failed to ensure that the Employees, and other Clinic staff, adhered to technical safeguards.

[142] Based on these findings, I make the following recommendations:

- Develop/reinstate privacy and security policies and procedures and ensure all physicians practicing at the Clinic adopt them, and all staff, including physicians, receive regular updated, documented privacy training.

- Ensure that all affiliates sign confidentiality oaths, and maintain a copy of the oaths in a secure location.

- Review the Clinic's PIA and complete a comprehensive assessment of whether all of the safeguards to mitigate risk that are outlined in the PIA have been implemented and are currently being practiced at the Clinic. Ensure that all custodians practicing at the Clinic sign off on the PIA commitments.

- Complete a 12-month review of the implementation of safeguards at the Clinic and report back to the Commissioner on the review's findings. Thereafter, ensure a periodic review is undertaken in compliance with section 8(3) of the Regulation.

Closing Comments

[143] This was a complex investigation that progressed through a number of phases. It was complicated by the ongoing dispute between the Employees and the Physician. My investigation, however, is only concerned with those matters related to compliance with HIA, and the specific allegations made in the original breach report submitted to the OIPC.

[144] Overall, the custodians practicing at the Clinic, as well as Clinic staff, clearly made a significant effort to ensure that a reasonable privacy management framework was developed for the Clinic. However, it is particularly disappointing to see that the Physician did not adopt this framework, and the Employees and other staff at the Clinic failed to adhere to the safeguards that were described.

[145] Custodians are ultimately responsible for their affiliates' compliance with HIA. This investigation report should serve as a reminder to custodians that they have a responsibility to ensure that reasonable policies and procedures are in place and followed, wherever it may be that they are practicing.

Chris Stinner
Manager – Special Projects and Investigations