Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2018-IR-01

Investigation into multiple alleged unauthorized accesses of health information at Alberta Hospital Edmonton

October 17, 2018

Alberta Health Services

Investigations 006542, 001509, 001591, 001626, 001637, 001790, 001837, 001849, 002016, 002120, 002749, 002752, 004067, 004068, 004129, 004154, 004196, 004235, 004249, 004250, 004292, 004302, 004304, 004420, 004561, 004562, 004563, 004611, 004778, 004883 and 005531

Commissioner's Message

As was the case with Investigation Report H2017-IR-02 (involving the South Health Campus hospital in Calgary), this investigation highlights a significant breach of privacy where the focus of the investigation shifted from an affiliate of the custodian (the Employee), to the custodian itself (Alberta Health Services, or AHS).

Alberta's *Health Information Act* (HIA) ultimately holds custodians accountable for the actions of its affiliates. While the Employee in this case improperly accessed health information, AHS did not meet its duties under HIA. Although AHS had administrative safeguards in place to protect health information, it failed to ensure the Employee was aware of and adhering to them, and to follow up concerns about the Employee's activities in a timely way.

In this case, AHS' proactive monitoring practices failed to detect this breach – the largest AHS has ever experienced in terms of number of affected individuals (over 12,000) and duration of the incident (the unauthorized accesses occurred between 2004-2015). AHS reported that this was in part due to the sheer number of AHS employees and because audit log reviews generate a significant number of potential issues that require individual follow up with each Alberta Netcare (Netcare) user's supervisor.

The investigation found that concerns about the Employee's use of Netcare were raised on four occasions between March 2014 and July 2015, and that AHS failed to take reasonable steps when it did not fully investigate these issues when they arose. Without the persistence of the Employee's former coworkers, who repeatedly brought concerns forward, the Employee's unauthorized use of Netcare might well be ongoing to this day.

This raises troubling concerns about AHS' ability to safeguard health information made available through Netcare. A vast number of authorized custodians/users have access to the system, and this number is growing all the time with the addition of new, authorized custodians. The system is broadly designed to facilitate access for those health care professionals involved in providing care. This can only work when the foundation is in place to detect and prevent abuses – including administrative safeguards, training and awareness, and auditing and monitoring. This investigation, and others before it, suggest the foundation may not be solid for a number of reasons, including the scale of the challenge, technical limitations and a lack of resources.

All in all, the findings from this investigation suggest it is well past time to consider whether the current approach to safeguarding health information made available through Netcare, as implemented by AHS in cooperation with Alberta Health, is adequate. I am now considering next steps, which could include an overall review of Netcare governance and safeguards. I will be following up with AHS and Alberta Health in this regard.

As noted, this was a significant breach given the large number of affected individuals and the time span over which the unauthorized accesses took place. These factors contributed to the time it took for AHS to contain the breach, investigate internally, identify affected individuals, assess the risk of harm, decide on a plan to notify affected individuals and report to the OIPC.

One individual who submitted a complaint to my office expressed concern with how long it took AHS to notify affected individuals. AHS addressed this in its September 2016 public communication about the breach, which said the breach required "in depth review of this former employee's accesses to Netcare

and Netcare Personal Directory for the full period of time between January 2004 and July 2015. This level of review takes significant time and resources to ensure it is done properly. This notification is occurring now because our investigation is now finished."

It is worth noting that, at the time the breach occurred and was discovered, there were no requirements in HIA for AHS to report the breach to me, or to notify affected individuals. Nonetheless, AHS made a decision to notify all affected individuals, including those whose information might have been accessed inadvertently (i.e. the specific individual was not targeted, but his/her name may have shown up in response to a broad search query). The OIPC consulted with AHS at the time and supported AHS' decision to notify all affected individuals.

As of August 31, 2018, amendments to HIA respecting breach reporting and notification are now in force. Under these new provisions, AHS would likely be legally required to report this breach to me, the Minister of Health and the affected individuals.

Further, as is noted in this report, during the course of this investigation I opened a separate, related investigation to consider possible offences under HIA. After a review of the available evidence provided by AHS, and considering when it was provided to my office and the two-year limitation period set out in HIA, I determined it would not be possible to proceed with charges against the Employee.

This situation might be different now, given the recent amendments to HIA which introduce new offences and significant potential penalties. For example, HIA now provides for a fine of not less than $200,000 for a person who fails to take reasonable steps in accordance with HIA regulations to maintain administrative, technical and physical safeguards to protect against reasonably anticipated threats to the security of health information (sections 107(1.1)(a) and 107(7)).

Overall, given the number of affected individuals in this case, the number of complaints submitted to the OIPC and media coverage of this matter, I believe it is in the public interest to publish this report reviewing the circumstances of the breach and the safeguards AHS had in place at Alberta Hospital Edmonton to protect health information. This report should be a wake-up call for custodians, alerting them to the potential consequences if they fail in their duty to implement and maintain reasonable safeguards to protect health information.

Jill Clayton
Information and Privacy Commissioner

Table of Contents

Background

[1] On July 28, 2015, the Office of the Information and Privacy Commissioner (OIPC) received an email from Alberta Health Services (AHS) reporting that it had "received allegations from two AHS Staff Members regarding an unauthorized access of their health information in Alberta Netcare" by an employee (the Employee) at Alberta Hospital Edmonton. The email stated that AHS "continues to investigate this matter and has requested an expanded audit of user [sic] from Alberta Netcare. Notification will be considered upon the conclusion of the investigation."

[2] The Information and Privacy Commissioner (Commissioner) opened a self-reported breach file and assigned a Senior Information and Privacy Manager to follow-up with AHS about the breach. During initial contact between the OIPC and AHS, the OIPC was advised that the breach could involve a large number of individuals and AHS was conducting a thorough investigation.

[3] On December 3, 2015, AHS provided its first detailed report of the breach to the OIPC. The report "concluded the accesses to 24 individuals were unauthorized and not in accordance with the employees [sic] role". The report noted the Employee had been terminated and "The responsible department notified the affected individuals by letter" on August 18, 2015.

[4] In January 2016, the OIPC followed up with AHS to ask if it had reviewed audit logs of accesses by the Employee. The OIPC was advised that AHS' internal audit showed as many as 12,000 unauthorized accesses may have occurred, and AHS would send a revised report of its investigation to the OIPC.

[5] On March 16, 2016, the OIPC received the updated report. The updated report noted that:

> [B]oth the OIPC and our department have received numerous complaints from members of the public who also have concerns about this former employee accessing their health information. Some of these complaints date back to accesses made in 2004.
>
> Because the new complaints stem back to 2004… AHS Privacy ordered a new set of audits. Alberta Health Netcare and Netcare [Person Directory] were requested from January 1, 2004 – July 27, 2015; [Admission Discharge and Transfer] audit log was requested … and an [Alberta Regional Mental Health Information System] audit was requested".
>
> … the findings from the audit review:
>
> Netcare [Person Directory]: 12,861 patients with unauthorized views by the former employee
>
> Netcare: 1,418 patients with unauthorized views by the former employee
>
> Of these, 376 patients are duplicates as they were viewed in both Netcare and Netcare [Person Directory].
>
> Notification to the affected individuals is pending.

[6] To this point, the OIPC had received 11 written complaints from individuals who had been notified by AHS of the breach in August 2015, or who had otherwise requested and received

copies of their audit logs and were concerned about unauthorized access to their health information by the Employee. The complainants were advised that individual investigations of their complaints would be held in abeyance pending the outcome of the OIPC's related investigation.

[7] Following the March 16, 2016 report, AHS continued to communicate with the OIPC about its investigation and the logistics of notifying affected individuals.

[8] Based on information provided by AHS, the Commissioner opened a separate, related offence investigation on September 8, 2016 to consider possible offences under HIA.

[9] On September 26, 2016, AHS issued a news release to inform the public about the breach. The news release said, in part:

> Following the conclusion of a privacy investigation, Alberta Health Services (AHS) is notifying 1,309 Albertans that their health information was inappropriately accessed by a former AHS employee. An additional 11,539 individuals will also be notified that their demographic information was viewed by this same former employee. These notifications will be completed through direct-mailed letters, which will be mailed today, Monday, September 26, 2016.
>
> The inappropriate accesses, which took place between January 2004 and July 2015, occurred in the electronic health record systems, Netcare and Netcare Personal Directory. The accuracy of the breached patient records has not been altered or impacted.

[10] Following the September 26, 2016 news release and letters to affected individuals, the OIPC received an additional 19 written complaints from affected individuals. As with the previous 11 complainants, these individuals were advised that their complaints would be held in abeyance pending the outcome of the OIPC's related investigation. In total, the OIPC received 30 complaints from individuals.

[11] In November 2016, given the available evidence provided by AHS, as well as the two-year statutory limitation period set out in HIA, the Commissioner decided it was not possible to pursue offence charges against the Employee. Instead, the investigation proceeded as an HIA compliance investigation on the Commissioner's own motion under section 84(1)(a) of HIA.

[12] I was assigned to review and collate information collected to this point, to gather additional, relevant information, and to write the investigation report. This report outlines findings and recommendations that resulted from this work.

Jurisdiction

[13] AHS' September 26, 2016 public news release said that it was "…notifying 1,309 Albertans that their **health information** was inappropriately accessed by a former AHS employee. An additional 11,539 individuals will also be notified that their **demographic information** was viewed by this same former employee"(emphasis added).

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

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

[16] 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…

[17] "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…

[18] AHS' news release also said that "…the inappropriate accesses… occurred in the electronic health record systems, Netcare and Netcare Personal Directory."

[19] Alberta Netcare (Netcare) is the provincial electronic health record (EHR). Netcare makes available demographic, prescription, lab test, diagnostic imaging and other information about individuals who receive health services in Alberta. The information made available through Netcare is diagnostic, treatment and care, and registration information and qualifies as health information as defined in sections 1(1)(i) and 1(1)(u) of HIA.

[20] Netcare Person Directory (Person Directory) provides a trusted list of all individuals who have a record in Netcare so that any source system may point to that list and link the right diagnostic, treatment and care information to the right individual's record. Information made available through Person Directory includes name, age, city, date of birth and gender

(see Appendix 1 for a screenshot with fictional data). For the vast majority of affected individuals in this case, and almost all of the individuals who submitted complaints to the OIPC, the information at issue was viewed using Person Directory.This information is registration information as defined in section 1(1)(u) of HIA, and health information as defined in section 1(1)(k) of HIA.

[21] A "custodian" is defined in HIA to include "a regional health authority established under the *Regional Health Authorities Act*" (section 1(1)(f)(iv)). AHS is a regional health authority established under the *Regional Health Authorities Act* on April 1, 2009, and is a custodian under section 1(1)(f)(iv). Prior to April 1, 2009, Alberta Hospital Edmonton was part of the Capital Health regional health authority (Capital Health). Since Capital Health no longer exists, this investigation and report focus only on the period that followed the formation of AHS. Unless otherwise noted, the term "custodian" in this report refers to AHS.

[22] Section 1(1)(a)(i) of HIA defines an "affiliate" as "an individual employed by the custodian". The Employee who accessed the health information at issue was employed by AHS as a Typist/Medical Secretary at the time of these accesses, and is therefore an affiliate of AHS.

[23] Section 28 of HIA states that an affiliate must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian. Under section 62(2) of HIA, any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use or disclosure by the custodian. AHS is therefore responsible for the Employee's access to and use of health information.

Issues

[24] The OIPC received a total of 30 written complaints from individuals affected by this matter. These individuals were generally concerned that their health information had been accessed for unauthorized purposes, and wanted to know why their information had been accessed. A number of complainants also expressed concern that the Employee's actions went undetected for such a long period of time.

[25] Given the above, the following issues were identified for this investigation:

- Did the Employee, as an affiliate of AHS, access and use health information in compliance with section 27 of HIA?
- Did AHS take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information and to protect against any reasonably anticipated unauthorized use or access pursuant to section 60 of HIA?

Methodology

[26] I took the following steps as part of this investigation:

- Interviewed and communicated in writing with current and former employees of Alberta Hospital Edmonton, employees in the AHS Privacy Office, and AHS Human Resources Advisors to collect information relevant to the investigation.
- Interviewed a number of the individuals who submitted complaints to the OIPC after receiving AHS' letter notifying them of the breach.
- Reviewed the following documentation:
    - AHS' reports summarizing its internal investigation of the matter, including notes from interviews with the Employee
    - AHS' response to OIPC questions
    - Partial audit logs of accesses made to the health information
    - AHS training materials and policies and procedures
    - Additional information provided to the OIPC by some of the complainants
- Requested an interview with the former Employee, but she declined to participate.

Analysis and Findings

Issue 1: Did the Employee, as an affiliate of AHS, access and use health information in compliance with section 27 of HIA?

[27] Netcare is the provincial EHR. Netcare makes available demographic, prescription, lab test, diagnostic imaging and other health information about individuals who receive health services in Alberta. This information is made available to authorized users who meet eligibility requirements set by Alberta Health under the authority of the *Alberta Electronic Health Record Regulation* (EHR Regulation).

[28] Netcare includes a subsystem referred to as Person Directory. Information made available through Person Directory includes name, age, city, date of birth and gender. In this case, the Employee accessed individually identifying health information made accessible through Netcare and Person Directory, as evidenced by the audit logs of her use of these systems.

[29] Section 56.5 of HIA says that "an authorized custodian … may use prescribed health information that is accessible via the Alberta EHR for any purpose that is authorized by section 27" of HIA.

[30] Section 27 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.

[31] 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.

[32] As part of its internal investigation of this breach, AHS interviewed the Employee on two occasions to ask about her purposes for accessing certain individuals' records through Netcare information systems.

[33] In the first interview, the Employee denied accessing health information in Netcare for purposes other than performing her work duties. In the second interview, the Employee admitted to accessing the records of about 20 individuals, whose names were read to her, for purposes not related to her work. As a result of the interviews, AHS determined that the Employee accessed information in Netcare for reasons related to her work, but also for other non-work related reasons. The AHS Privacy Office requested the audit log from Alberta Health for all accesses made by the Employee back to 2004 (when Netcare logging commenced), and the subsequent review of audit logs by the AHS Privacy Office found that the Employee accessed the health information of over 12,000 individuals between 2004 and 2015, in contravention of HIA.

[34] I reviewed notes from the two interviews AHS conducted with the Employee, as well as additional information provided by AHS and the Employee's former colleagues and supervisors. The Employee provided a variety of explanations for her accesses to the health information of individuals in Netcare. The various purposes cited by the Employee are discussed below.

Curiosity

[35] In the second interview done by AHS, the Employee admitted to accessing numerous, named individuals for the purpose of confirming their address or date of birth. This included physicians or other employees working at Alberta Hospital Edmonton, their relatives, or the Employee's own relatives. For some of these accesses, the Employee offered explanations related to the individuals' life events, such as their birthdays, their passing or the passing of a family member. For many other accesses, the Employee was able to explain how the individuals she looked up were related to her or to her colleagues at Alberta Hospital Edmonton, but gave no work-related reasons for accessing their information in Netcare.

[36] There is no provision in section 27 of HIA that authorizes the use of health information for "curiosity", and all such accesses by the Employee for this purpose contravened section 27 of HIA.

Don't Know or Can't Recall

[37] The Employee was not able to offer any explanation for accessing the health information of numerous, named individuals, stating she did not recall.

[38] Custodians can only use health information for one or more of the purposes set out in section 27. Section 28 of HIA prohibits an affiliate from using health information in any manner that is not in accordance with the affiliate's duties to the custodian. In my view, it is incumbent on the custodian/affiliate to be able to demonstrate that accesses are for an authorized purpose, as set out in section 27 of the Act. Accesses that cannot be explained cannot be said to be for legitimate, authorized purposes and are therefore in contravention of section 27 of HIA.

Billing Services

[39] I obtained statements from a number of former coworkers of the Employee and reviewed internal AHS correspondence that indicated that for many years the Employee had a second job working as a contractor for an Edmonton area business that provides billing services for physicians. Physician practices established in the community that deliver health services outside of AHS facilities need to bill Alberta Health for these services. In this situation, it is not uncommon for billing submitters to have to confirm patient details, such as name, personal health number or date of birth.

[40] The evidence I reviewed suggests that the Employee had on more than one occasion performed some of this work on AHS or Capital Health time, using resources provided by her employers. In my view, it is likely that some of the unauthorized accesses to registration information in Netcare in this case were related to the Employee's performance of this work.

[41] Under section 27(1)(g), custodians may use health information for the purpose of "obtaining or processing payment for health services". However, section 28 of HIA prohibits an affiliate from using health information in any manner that is not in accordance with the affiliate's duties to the custodian. The use of health information for billing purposes did not fall within the Employee's duties to AHS, or Capital Health before that. Any such access to health information in relation to this contract work was therefore not authorized under section 27 of HIA.

Findings

[42] The Employee's access to and use of individually identifying health information in Netcare was not authorized under section 27 of HIA.

[43] The Employee contravened section 28 of HIA when she accessed and used health information for purposes that were not in accordance with her duties to AHS.

[44] Since AHS is responsible as a custodian for the actions of its affiliates under section 62(2) of HIA, AHS contravened section 27 of HIA when its affiliate accessed and used health information for unauthorized purposes.

Issue 2: Did AHS take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information and to protect against any reasonably anticipated unauthorized use or access pursuant to section 60 of HIA?

[45] A custodian has a duty to protect health information in its custody or under its control. Specifically, 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
>
> (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.
>
> (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

[46] Section 8 of the *Health Information Regulation* sets out additional security requirements including:

> 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.

[47] These sections of HIA and the *Health Information 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 maintain a written record of the safeguards that are implemented.

[48] This investigation concerns the Employee's access to and use of health information available through Netcare. Unlike most other health information systems that AHS employees may use, the responsibility to protect the health information available through Netcare is shared among several stakeholders.

[49] With respect to Netcare (the Alberta EHR), Alberta Health is "… designated the information manager of the Alberta EHR" (section 2 of *Alberta Electronic Health Record Regulation*). As such, Alberta Health has responsibility to implement certain safeguards, and particularly those that are physical and technical. As Alberta Health is not the subject of this investigation, I will focus on AHS' implementation of administrative safeguards which typically include policies and procedures, confidentiality agreements, and training. I also looked at AHS' auditing practices in detail, which are relevant to AHS' duty under section 8(6) of the *Health Information Regulation* to ensure that affiliates "adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information".

Policies and Procedures

[50] Under section 63(1) of HIA, a custodian is required to "establish or adopt policies and procedures that will facilitate the implementation" of HIA and its regulations. Policies and procedures are essential as they provide affiliates with clarity as to the custodian's expectations and guidance on how to protect health information in order to comply with HIA.

[51] I requested that AHS provide me with relevant policies, procedures and documentation, which I reviewed. The following table summarizes the policies AHS had in place.

AHS Policy	Description
Policy #1105: Access to Information	This policy deals with the physical, technical and remote access controls in place for AHS electronic systems. The policy says that the IT and Security Compliance Office shall review user rights, either as part of the regular security review or more frequently (as required), and may revoke or modify privileges when necessary. The policy addresses consistent administrative and technical access controls to safeguard patients and staff, and to protect the security of information technology (IT). It also says that AHS has the right to audit and log access to information to manage the controls.
Policy #1112: Collection, Access, Use & Disclosure of Information	This policy says that only authorized persons can collect, use or disclose information in accordance with the legislation, and that authorized persons must use the information responsibly and appropriately, maintaining the confidentiality, security, integrity, availability and accuracy of information.
Policy #1109: Information Technology Acceptable Use	This policy sets out the responsibilities of users regarding the use of IT. The policy states that users shall: • Be assigned a unique User ID

	• Be responsible for all actions taken by that User ID • Take necessary security precautions • Not allow another individual to use their User ID and/or password The policy also says that users shall only access the minimum information necessary for the performance of their duties with AHS, and references the sign-off on AHS user agreements at appointment stating that the signature constitutes acceptance of compliance responsibilities identified in the agreements.
Policy #1143: Information Security and Privacy Safeguards	This policy says that persons who do not complete the information security and privacy training as required, and whose roles require them to access information, shall not be granted access or may have their access to information suspended until training has been completed.
AHS Code of Conduct	The code applies to everyone who provides care or services or acts on behalf of AHS. The code has five principles. The third principle references upholding AHS policies and procedures. The fifth principle mentions respecting the confidentiality and privacy of health information by only collecting, using, accessing, disclosing and storing the minimum amount of information necessary to meet the purpose.

[52] I reviewed the policies and procedures described above and find that AHS has established these in order to facilitate the implementation of the Act and the regulations, as required by section 63(1) of HIA.

Confidentiality Agreements and Training

[53] As noted above, section 8(6) of the *Health Information 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.

[54] With respect to confidentiality agreements, AHS informed me that the confidentiality agreement the Employee signed dated back to 2001, when the Employee worked at Alberta Hospital Edmonton which was then part of Capital Health.

[55] I asked AHS to provide me with documentation related to any information access and privacy training the Employee received. I received documentation related to annual performance reviews of the Employee; however, this documentation did not provide any evidence that the Employee received privacy training or was reminded of her duty to comply with AHS' privacy policies and procedures.

[56] AHS did inform me that it has developed training materials that its affiliates are expected to review at their computer, and that managers throughout AHS are responsible to ensure that their direct reports review these materials on a regular basis. Based on this, I interviewed two individuals who supervised the Employee from 2008-2014 and from 2014-2015, respectively. I was told that the Employee had not received any privacy training during these time periods. In particular, the Employee's manager from 2008-2014 told me she had not received explicit instructions to have her direct reports review these materials and she therefore assumed it was not necessary for her direct reports to take this privacy training.

[57] The only information I obtained that suggested the Employee may have received privacy training in relation to use of Netcare came from a former employee at Alberta Hospital Edmonton who provided me with a copy of one of her own performance review documents (similar to those I had received concerning the Employee). These documents evidenced that the other employee had attended a training session on December 20, 2004. The other employee explained that, at the time, there had been a significant training effort that coincided with the introduction of NetCARE[1], and that all employees of Alberta Hospital Edmonton were required to attend, including the Employee.

[58] AHS was not able to positively confirm this fact because, as previously noted, Alberta Hospital Edmonton was part of the former Capital Health in 2004, and AHS was not yet formed. AHS did confirm that there was no documented evidence on the Employee's file that would demonstrate she received training about privacy or HIA compliance in relation to her use of Netcare, or even a reminder at any point over the time period in question.

[59] Based on the above, I find that AHS failed to ensure the Employee was made aware of the safeguards put in place to protect health information, in contravention of section 8(6) of the *Health Information Regulation.*

Adherence (Auditing Practices)

[60] Section 60(2)(a) of HIA specifically requires that custodians implement appropriate safeguards to "address the risks associated with electronic health records".

[61] Section 8(6) of the *Health Information Regulation* requires that a custodian "ensure that its affiliates… **adhere to** all of the custodian's administrative, technical and physical safeguards in respect of health information" (emphasis added). Indeed, in order to protect individuals' health information against known risks, safeguards are needed but these are of no value if affiliates do not follow them.

[62] As part of my investigation, I communicated with AHS about how it ensures affiliates are complying with safeguards to protect health information in electronic information systems, including relevant policies and procedures. AHS said that it proactively monitors for unauthorized collection, use, access or disclosure of health information through routine review of monthly audit logs generated by Alberta Health, or has Alberta Health generate audit logs in Netcare for review by AHS when following up on concerns of unauthorized

[1] At the time, "NetCARE" referred to an information system of Capital Health, which had not yet been designated as the Alberta EHR.

activity raised by patients or employees. Both approaches are discussed below in the context of the current matter.

Routine Audit Log Reviews

[63] AHS reported that it had for years been auditing its employees' use of Netcare, as per "Policy #1105: Access to Information" (described in the table above).[2] However, AHS said that the auditing it had done failed to detect the misuse of Netcare by the Employee. AHS explained this was due in part to the sheer number of AHS employees and that audit log reviews generate a significant number of potential issues that require individual follow up with each Netcare user's supervisor. As a result, AHS assesses and samples issues flagged in audit logs to determine which ones will be investigated more closely, and which ones will not. This creates the possibility that some potential contraventions of AHS policy or HIA may not be investigated, and in some cases can continue over long periods of time.

[64] It appears this may be the reason the Employee's unauthorized use of Netcare escaped detection through the review of audit logs.

Responding to Concerns

[65] In addition to routine audit log reviews, AHS may receive concerns or complaints from individuals (e.g. patients, employees) alleging possible unauthorized access to and use of health information.

[66] My investigation found that concerns about the Employee's use of Netcare had been raised on more than one occasion. I reviewed records related to these concerns, and noted that on each occasion, issues were raised by another employee of Alberta Hospital Edmonton, usually in the context of some non-privacy related matter (e.g. general employment related issues). These concerns, and their follow up, are described below.

- **March 2014**: At this time, a concern was raised by one of the Employee's coworkers alleging the Employee was sharing Netcare login credentials with another affiliate. In response, the Employee's Manager met with the Employee to discuss the situation. After the Employee assured the Manager she had not misused Netcare, the issue was not looked into further and was not escalated or reported to anyone else in AHS.

- **July 2014**: On this occasion, a concern was raised anonymously by someone purporting to be an employee of Alberta Hospital Edmonton, alleging that the Employee was using Netcare for the purpose of doing billing for a different organization. The Employee was asked to meet with Human Resources and respond to the concern and other employment-related issues. After the Employee assured those attending the meeting she had not misused Netcare, the issue was not looked into further.

[2] After a reviewing a draft of this report for fact-checking purposes, AHS noted, "AHS reviews all Netcare audits they receive from Alberta Health. AHS Privacy (Office) receives approximately 12-23 (audit logs) per month and all undergo a thorough review. The Employee's access was never audited previous to this investigation nor did AHS receive an audit for review."

I reviewed notes from the meeting – which include the Employee's responses to questions put to her – and note that a Human Resources Advisor specifically asked the Employee about her potential misuse of Netcare, and whether an audit log review of the Employee's use of that system would show unauthorized use. The Employee responded: "No". In the end, the Employee's use of Netcare was not reviewed by AHS at the time and the AHS Privacy Office was not involved.

- **May 2015:** At this time, one of the Employee's coworkers reported the Employee was sharing Netcare account credentials with another AHS affiliate. By this time, the Employee had a new manager, who delegated the handling of the issue to a unit supervisor at Alberta Hospital Edmonton. The unit supervisor discussed the situation with the Employee and advised that the AHS Privacy Office would have to be involved, as the issue fell within that office's expertise and responsibility. When the AHS Privacy Office was notified of a possible contravention, an AHS Privacy Advisor spoke with the Employee about acceptable use of health information systems, and discussed the matter with the individual who had brought up the concern.

  In the course of these exchanges, the AHS Privacy Advisor informed the individual who brought the allegations that the individual could request a Netcare Audit Log, which would show any accesses to the individual's health information in Netcare. [3] However, the AHS Privacy Advisor did not review and did not have the Employee's use of Netcare reviewed at that time.

- **July 2015:** Between May and July 2015, the individual who had raised the May 2015 concern followed the advice of the AHS Privacy Office and obtained a Netcare Audit Log. The Netcare Audit Log showed the Employee had accessed the individual's record in Netcare on more than one occasion. The individual provided a copy of the Netcare Audit Log to the Employee's Manager, as well as to the AHS Privacy Office. Another meeting involving Human Resources was held to ask the Employee to explain her accesses to the individual's record in Netcare. Around the same time, the AHS privacy advisor requested and started to review the audit log of the Employee's use of Netcare.[4]

[67] Overall, in the span of 17 months, AHS had received four separate reports from two individuals alleging the Employee's use of Netcare contravened acceptable use rules. AHS only followed through on the fourth one, and only once it was presented with evidence of unauthorized use. AHS explained to me that a contributing factor to its inaction in the face of these concerns was the fact that they were raised by some of the Employee's coworkers, in the context of tense workplace relationships, along with a change in managers in June 2014. [5]

---

[3] Any individual who has a record in Alberta Netcare may exercise this right. Alberta Health has information available at http://www.albertanetcare.ca/AuditLogs.htm.

[4] After a reviewing a draft of this report for fact-checking purposes, AHS noted that on August 17, 2015, the Employee was terminated from her employment with AHS.

[5] I also reviewed evidence that concerns about the Employee "spending work time doing a home business of doctor's billings" were raised in November 2005, when Alberta Hospital Edmonton was part of Capital Health. It appears the Employee denied using work time to do doctors' billings "except to look up the patients' health care numbers if the doctors did not write it on the form", but was nonetheless advised to "stop this practice".

[68] I interviewed those involved, and reviewed email correspondence and records generated throughout the handling of these concerns. In my view, AHS failed to take reasonable steps when it did not fully investigate the issues raised. In fact, it appears that without the persistence of the Employee's former coworkers, who repeatedly raised the issue, the Employee's unauthorized use of Netcare would not have been detected in July 2015 and may have continued on.

[69] Based on the above, I find that AHS did not meet its duty to comply with section 8(6) of the *Health Information Regulation* by failing to ensure its affiliate (the Employee) adhered to AHS' safeguards to protect health information.

Findings

[70] AHS has established reasonable policies and procedures to facilitate the implementation of the Act and the regulations, as required by section 63(1) of HIA.

[71] AHS failed to ensure the Employee was aware of the safeguards put in place to protect health information, in contravention of section 8(6) of the *Health Information Regulation.*

[72] Over the course of 17 months, AHS received four separate concerns regarding the Employee's alleged misuse of Netcare. By not investigating these concerns fully, AHS contravened section 8(6) of the *Health Information Regulation* which requires custodians to take reasonable steps to ensure its affiliates (the Employee) adhere to administrative, technical and physical safeguards in respect of health information. Without the persistence of the Employee's former coworkers, who repeatedly raised the issue, it appears the Employee's unauthorized use of Netcare would not have been detected in July 2015 and may have continued on.

Recommendations

- AHS should review privacy training provided and implemented at Alberta Hospital Edmonton and across AHS, and ensure that all employees receive regular, updated, documented privacy training.
- With respect to monitoring for compliance with rules and procedures concerning access to and use of health information in Netcare (and other electronic health information systems), I recommend that AHS:
  - Review the adequacy of the process by which potential HIA or policy compliance issues are investigated and escalated.
  - Complete a review of the criteria and approach used to audit employee access to and use of Netcare.
- Considering the number of authorized users of Netcare, the vast amount and sensitivity of health information made available through it, and the process for granting access to the system, the criteria and approach used by AHS to review audit logs for follow up must be examined to ensure they are adequate to detect and prevent unauthorized use of Netcare.

Other Considerations

[73] In addition to the two issues examined above, I examined another topic in the course of my investigation, as it relates to concerns raised by some of the individuals who submitted complaints to the OIPC. My comments and observations concerning Person Directory may help to explain how some of these individuals came to be affected in this matter.

Netcare Person Directory

[74] As has been described above, Netcare is the provincial electronic health record system. Netcare contains demographic, prescription, lab test, diagnostic imaging and other health information about all individuals who receive health services in Alberta. Netcare itself is not an information system that contains health information, but is instead a portal that aggregates the health information of any individual who has received health services in Alberta, from a large number of source information systems.

[75] In order to correctly match diagnostic, treatment and care information available through Netcare to the subject individual, Netcare includes a subsystem referred to as Person Directory. The purpose of Person Directory is to provide a trusted list of all individuals who have a record in Netcare, so that any source system may point to that list and link the right diagnostic, treatment and care information to the right individual's record.

[76] The distinction between Netcare and the Person Directory is critical to individuals affected in this matter, since the Employee accessed some records in Netcare, and some records in Person Directory. When AHS issued its news release on September 26, 2016 to inform the public about the breach, the news release said, in part:

> Following the conclusion of a privacy investigation, Alberta Health Services (AHS) is notifying 1,309 Albertans that their **health information** was inappropriately accessed by a former AHS employee. An additional 11,539 individuals will also be notified that their **demographic information** was viewed by this same former employee. [emphasis added]

[77] My comments here relate to the 11,539 individuals whose demographic information was accessed, as this represents the larger number of individuals affected, and includes almost all of the individuals who submitted complaints to the OIPC.

[78] During my investigation, AHS provided information to explain why this number was so high. Essentially, the Employee used Person Directory to search for individuals' records in Netcare. To do so, she entered information on the search page of Person Directory, which generated a list of results matching the search criteria, with a link to their record on Netcare. Each entry on the list displayed full name, name type, age, city, date of birth and gender (see Appendix 1 for fictional examples illustrating the fields and results that would be displayed).

[79] Based on the design of Netcare, an entry is added to an individual's audit log whenever the individual's information appears in a list of search results. Similarly, the searcher's (user's) audit log will show an entry for every individual whose information was displayed as the result of a search. This largely accounts for the high number of individuals affected by this

matter. A single search, if run on a common last name (such as 'Smith' in the fictional screenshots included in Appendix 1) could produce dozens of results on a single screen, therefore generating a corresponding number of entries in the Employee's audit log, and one entry in the audit log for each individual who appeared on a list of search results.

[80] I have provided this explanation to clarify that the Employee did not have to perform over 12,000 separate searches in order to affect 12,000 individuals. Further, not every affected individual was specifically looked up by the Employee. While it may be of little comfort to affected individuals, I believe this information about the system and the auditing function may help to explain how some individuals came to be affected by the Employee's unauthorized use of Netcare.

Summary of Findings and Recommendation

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

- The Employee's access to and use of individually identifying health information in Netcare was not authorized under section 27 of HIA.
- The Employee contravened section 28 of HIA when she accessed and used health information for purposes that were not in accordance with her duties to AHS.
- Since AHS is responsible as a custodian for the actions of its affiliates under section 62(2) of HIA, AHS contravened section 27 of HIA when its affiliate accessed and used health information for unauthorized purposes.
- AHS has established reasonable policies and procedures to facilitate the implementation of the Act and the regulations, as required by section 63(1) of HIA.
- AHS failed to ensure the Employee was aware of the safeguards put in place to protect health information, in contravention of section 8(6) of the *Health Information Regulation.*
- Over the course of 17 months, AHS received four separate concerns regarding the Employee's alleged misuse of Netcare. By not investigating these concerns fully, AHS contravened section 8(6) of the *Health Information Regulation* which requires custodians to take reasonable steps to ensure its affiliates (the Employee) adhere to administrative, technical and physical safeguards in respect of health information. It appears that without the persistence of the Employee's former coworkers, who repeatedly raised the issue, the Employee's unauthorized use of Netcare would not have been detected in July 2015 and may have continued on.

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

- AHS should review privacy training provided and implemented at Alberta Hospital Edmonton and across AHS, and ensure that all employees receive regular, updated, documented privacy training.

- With respect to monitoring for compliance with rules and procedures concerning access to and use of health information in Netcare (and other electronic health information systems), I recommend that AHS:

  - Review the adequacy of the process by which potential HIA or policy compliance issues are investigated and escalated.

  - Complete a review of the criteria and approach used to audit employee access to and use of Netcare.

- Considering the number of authorized users of Netcare, the vast amount and sensitivity of health information available through it, and the process for granting access to the system, the criteria and approach used by AHS to review audit logs for follow up must be examined to ensure they are adequate to detect and prevent unauthorized use of Netcare.

Closing Comments

[83] This investigation has highlighted significant shortcomings at Alberta Hospital Edmonton, and many discrepancies between the policies and procedures established by AHS and their implementation.

[84] I understand that, after notifying affected individuals of this matter, AHS has taken the following actions:

- Provided a support line for the affected individuals. Approximately 1,300 one-on-one discussions took place.

- Focused on continued privacy and HIA awareness training for AHS employees (in April 2018, AHS indicated 90% of its workforce had been trained, and just over 97% at Alberta Hospital Edmonton). The updated training includes a digital re-sign of the Confidentiality and User Agreement.

- Changed its practices to systematically embed privacy messages in performance appraisals and orientation training for all employees and physicians at AHS.

- Addressed the lapse in documentation about employee training and has ensured employee acknowledgement of policies and procedures is properly recorded and retained. AHS' online privacy training became tracked in AHS' learning management system, which allows managers to pull reports of who has or has not completed requisite training. Reports are also pulled for the executive level to track training numbers and to identify areas where more training is required.

- Established a process whereby AHS requests tailored audit logs from Alberta Health to specifically audit employees who work in addictions and mental health at Alberta Hospital Edmonton. At least four users per month are audited in addition to the usual audit logs Alberta Health provides to AHS for review.

- Conducted an internal audit to review audit processes,[6] and reported that, "Efforts are currently being made by AHS to procure an auditing tool with artificial intelligence…"

- Developed a new "Protection of Privacy and Access Policy" to set expectations for behaviour when handling health, personal and AHS business information.

[85] I would like to thank all the current and former AHS employees with whom I consulted for their cooperation in this investigation.

Chris Stinner
Manager – Special Projects and Investigations

[6] After a reviewing a draft of this report for fact-checking purposes, AHS noted, "In 2016, AHS Privacy (Office) had an internal audit done of our audit processes and no gaps were found. Some enhancements were highlighted and have been included into our organizational plans. The audit process though does not include the maintenance or control of the audit logs or proactive auditing in Netcare as those aspects are still managed by Alberta Health."

Appendix 1: Netcare Person Directory Screenshots

These screenshots illustrate the search feature in Person Directory. These screenshots were provided by AHS, and are from a test system. All search result data are fictional.