Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2017-IR-02

Investigation into multiple alleged unauthorized accesses of health information at South Health Campus

November 29, 2017

Alberta Health Services

Investigation 001548

Table of Contents

Introduction

[1] On September 8, 2015, a patient was admitted to the South Health Campus emergency department in Calgary. The South Health Campus is a hospital operated by Alberta Health Services (AHS) that opened in January of 2013, with the emergency department opening later that year in September. The patient was flagged as a "confidential patient". Many staff members were aware of media reports concerning the patient and her daughter. The patient remained in the emergency department until September 11, 2015.

[2] On September 10, 2015, the AHS Information and Privacy Office (AHS Privacy Office) was notified by a South Health Campus emergency department manager of a possible contravention of the *Health Information Act* (HIA) involving a disclosure of the patient's health information. Due to the circumstances of the patient's admission to the emergency department, the AHS Privacy Office decided to complete a proactive audit of all accesses to the health information of the patient, and the patient's daughter, within the Sunrise Clinical Manager electronic medical records system (SCM EMR), and the provincial electronic health record (Netcare).

[3] The audit identified 160 employees of the South Health Campus emergency department who accessed the health information of the patient, or both the patient and her daughter (the health information). The audit reports were distributed to emergency department managers for review to determine if these accesses were authorized. The review confirmed that the majority of the accesses were necessary to provide health services and were authorized; however, accesses made by 75 employees required further investigation.

[4] An investigation team was mobilized, including staff from the AHS Privacy Office, human resources, and management. The team interviewed the 75 employees and determined that 49 of them accessed health information "outside their role" of providing a health service.

[5] AHS disciplined the 49 employees who were found to have accessed the health information without authority; however, a majority of the employees filed grievances pursuant to their respective collective bargaining agreements. Following grievance resolution meetings with the employees and their union representatives, AHS rescinded discipline for 38 of the employees and reduced discipline for the remaining 11.

[6] The alleged unauthorized accesses were reported to the Office of the Information and Privacy Commissioner (OIPC) on September 18, 2015. On October 15, 2015, the Commissioner opened an investigation on her own motion under section 84(1)(a) of the HIA.

[7] The Commissioner assigned an investigator to gather information for the investigation. I was assigned to write the investigation report.

[8] This report outlines findings and recommendations from the investigation. That being said, during the investigation and prior to the release of this report, AHS took steps to address the issues that arose in this investigation, and accordingly, some of the recommendations made have already been addressed. The steps taken by AHS to address issues are highlighted later in the report.

Methodology

[9] The following steps were taken during this investigation:

- The OIPC investigator communicated in writing and met with AHS senior executives and the AHS Privacy Office to collect information for the investigation.
- I reviewed:
  - AHS's report summarizing its internal investigation of the matter, including notes from interviews with affiliates
  - AHS submissions to the OIPC responding to questions posed by the OIPC investigator
  - Audit logs of accesses made to the health information, as well as audit logs for other patients seen at the emergency department between September 6-11, 2015
  - Privacy Impact Assessments (PIAs) previously submitted to the OIPC for the SCM EMR
  - AHS training materials and policies and procedures
  - AHS's rationale for discipline and the subsequent decision to rescind or reduce discipline, including template correspondence to the employees involved

Application of the HIA

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

[11] The information at issue in this case consists of registration information, as well as diagnostic, treatment and care information for two individuals – the patient and her daughter. This information is "health information" as defined in section 1(1)(k) of the HIA.

[12] The HIA defines "custodian" to include "a regional health authority established under the *Regional Health Authorities Act*" (section 1(f)(iv)). AHS is a regional health authority established under the *Regional Health Authorities Act* and is a custodian under section 1(1)(f)(iv).

[13] Audit logs demonstrate that the health information was accessed in the SCM EMR by AHS employees working in the South Health Campus emergency department.

[14] Section 1(1)(a)(i) of the HIA defines an "affiliate" as "an individual employed by the custodian". The employees who accessed the health information of the patient and her daughter are affiliates of AHS.

[15] Section 28 of the 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 the 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 when its affiliates access and use health information.

Issues

[16] The objectives of this investigation were to determine whether health information was accessed and used in accordance with the HIA, to review safeguards and training, and determine whether sanctions for contravening safeguards were in place. The following issues were identified:

1. Did AHS affiliates access and use health information in compliance with sections 27 and 28 of the HIA?

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, access or disclosure pursuant to section 60 of the HIA?

3. Did AHS take reasonable steps to ensure affiliates were aware of and adhered to all of the custodians' administrative, technical and physical safeguards in respect of health information pursuant to section 8(6) of the *Health Information Regulation*?

4. Did AHS establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information, as required by section 8(7) of the *Health Information Regulation*?

Analysis and Findings

Issue 1: Did AHS affiliates access and use health information in compliance with sections 27 and 28 of the HIA?

[17] Section 27 of the HIA lists the purposes for which a custodian may use health information. The relevant portions of section 27 include:

> 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…
> (e) providing for health services provider education…
> (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.

[18] Section 28 of the 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". Any access to or use of health information by an affiliate which is not in accordance with the

affiliate's duties to the custodian is a contravention of section 28 of the HIA. It follows that an affiliate may use health information only for purposes set out in section 27 of the HIA.

[19] As previously noted, the AHS Privacy Office audit and subsequent review found that accesses to the health information at issue by 75 affiliates in the South Health Campus emergency department required additional review to determine if the accesses were authorized.

[20] AHS interviewed the 75 affiliates to ask about their purpose(s) for accessing the health records and their role in providing care to the patient, or both the patient and her daughter. Many accesses were found to be authorized based on the affiliate's role, and for the purposes of providing direct care.

[21] As a result of the interviews, however, AHS determined that 49 of the 75 affiliates "accessed information outside their role" of providing a health service.

[22] The 49 affiliates included AHS Managers, nurses, and non-nursing or clerical staff. I reviewed notes from the interviews AHS conducted with the 49 affiliates who provided a variety of explanations for their accesses to the health information. The most frequently cited purposes are discussed below.

Providing or preparing to provide a health service

[23] Affiliates reported that the accesses were work-related. They believed it was important to "be aware" of all patients in case they were called to cover for another staff, be part of a "code team", perform triage, or act as "float nurse". A number of affiliates also said they were aware that the patient in this case was categorized as "CTAS level 1", and would require increased care.[1]

[24] In some cases, these explanations would appear to be authorized uses under the HIA. However, after consulting with management, the investigation team found that many of the accesses were not authorized for a variety of reasons, such as the affiliates' specific assignment/role on a particular day/shift, or because of the timing of the access (e.g. near the end of a shift).

[25] AHS confirmed that many of the accesses were not required to provide or prepare to provide a health service, saying, for example:

> Typically, nurses working on a team work together and support each other in the assessment and interventions for the patients, or when taking over care for a patient during shift breaks or shift changes.

[1] Emergency department staff use the Canadian Triage and Acuity Scale (CTAS) National Guidelines (http://caep.ca/resources/ctas/implementation-guidelines), which assess patients based on five levels. A patient with threats to life or limb, for example, will be assessed as the highest priority and categorized as a CTAS level 1 patient. These patients usually need to be seen by a physician immediately, 98 percent of the time, according to the CTAS scale. A patient with an acute non-urgent condition would be a lower priority and likely categorized as a CTAS level 5 patient. It is reasonable to expect that a CTAS level 1 patient will have his or her health records accessed more frequently as more health services providers are engaged in providing care, and the care is more continuous.

> The primary nurse is responsible for ensuring that all patient interventions/assessments are carried out. However, other nurses may be required to assist depending on the magnitude of the presenting complaint and other demands for services. Nurses working on the team should access information about their particular grouping of patients only as needed fulfill [sic] their professional role as a nurse on the team. If a nurse is asked to assist another nurse in a different area of the department, the nurse would be able to access the chart for that assigned patient to support carrying out their role. Nurses should only access patient information to cover for a colleague's break at the time of hand-off. All nurses are responsible and accountable to protect and maintain the privacy and confidentiality of the patient's information at all times.

[26] AHS also said "It is not the expectation … to proactively go into the files in anticipation of who you may cover."

Assessment of patient stability, to ensure proper placement, and to facilitate flow and patient movement within the emergency department

[27] During interviews, affiliates reported that it was a normal practice in the ER to look patients up to "promote flow" – for example, "to determine wheatear [sic] there is a patient who is more stable… and can be swapped" or because the affiliate "needed to see what was going on in POD F in the event [of needing] to move a patient there." Another affiliate reported needing "to review patient information to determine which unit is appropriate for them, based on bed availability, acuity and the general condition of the patient."

[28] As noted above, in some circumstances, these explanations would appear to be legitimate, authorized purposes under the HIA. For example, AHS confirmed that "Patient Flow in the ER is essential to the smooth operation of the entire department."

[29] However, after reviewing specific accesses, AHS found in some cases that the affiliate's job duties did not include managing the flow of the unit, or the flow coordinator for a specific pod did not need to access information of patients in other pods. AHS confirmed that "float for a specific pod is only for the patient flow for that pod, no need to access patient files in other pods… Instead the RN should call charge to take care of the patient going to another pod."

Education

[30] A number of affiliates explained their access to the patient's health information by saying that it was for "learning" or "educational purposes", including "to understand the diagnosis even if they are no longer [sic] have direct care with a client", "to put together case studies of cases that would reasonably be a good learning for staff", "determine if debriefs are required after a bad code", or because of the patient's CTAS level.

[31] While "providing for health services provider education" is an authorized purpose under section 27 of the HIA, these accesses were, for example, "determined to be inappropriate as there was no need to access the patient records to do a "debrief", or "access for educational purposes would not be acceptable".

Curiosity

[32] A number of affiliates admitted accessing the health information out of "curiosity". In some cases, they were aware that a "confidential patient' had been admitted, and some mentioned that there had been "talk in the department".

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

Don't know/can't recall

[34] A significant number of affiliates were unable to recall why they accessed the health information when presented with evidence of accesses on specific dates and times.

[35] Custodians can only use health information for one or more of the purposes set out in section 27. Section 28 of the 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.

Findings

AHS contravened the HIA when its affiliates accessed and used health information for purposes that were not authorized under section 27 of the Act. AHS affiliates contravened section 28 of the HIA when they accessed and used health information for purposes that were not in accordance with their duties to AHS (the custodian).

Recommendations

- Complete a review of the access to health records that is necessary to support and manage the provision of care within a team environment at the South Health Campus in a manner that ensures use of health information is limited to what is essential to meet authorized purposes set out in section 27.
- Develop electronic health record access guidelines for South Health Campus, and provide training to all affiliates within the emergency department.

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, access or disclosure pursuant to section 60 of the HIA?

[36] A custodian has a duty to protect health information in its custody or under its control. Specifically, section 60 of the 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

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

> 8(1) A custodian must identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information…
>
> (3) A custodian must periodically assess its administrative, technical and physical safeguards in respect of
>
> (a) the confidentiality of health information that is in tis custody or under its control and the privacy of the individuals who are the subjects of that information,
> (b) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information, and
> (c) any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information.

[38] The HIA requires 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 and use of health information. Further, the Act specifically requires that measures be taken to address the risks associated with electronic health records. A custodian is required to maintain a written record of the safeguards that are implemented, and must periodically assess the implementation of safeguards.

[39] I reviewed the administrative and technical safeguards that AHS had in place to meet these obligations under the HIA. I did not review physical safeguards in this case because all of the AHS affiliates were authorized to be present in the South Health Campus emergency department.

Administrative Safeguards

[40] Section 63 of the HIA requires that a custodian establish or adopt policies and procedures that will facilitate the implementation of the HIA and its regulations. Policies and procedures are essential as they provide affiliates with guidance on how to protect health information and remain in compliance with the HIA.

[41] In order to determine whether AHS has reasonable administrative safeguards in place, AHS was asked to provide relevant policies, procedures and documentation. The following table summarizes the policies AHS has 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.

[42] I reviewed the policies and procedures described above and find that AHS has taken reasonable steps to establish administrative safeguards to protect the confidentiality of health information and to protect against reasonably anticipated risks. Whether AHS policies and procedures were effectively implemented and affiliates were aware of and adhering to them is a separate matter I will address later in this report.

Technical Safeguards

[43] AHS has a policy in place which sets out the acceptable use of IT resources. This is a policy of general application. In this investigation, assessment of relevant safeguards requires consideration of the SCM EMR's technical safeguards, as this system was used to access the health information of the patient and her daughter. In completing this assessment I examined information submitted by AHS and also considered privacy impacts assessments (PIAs) for the SCM EMR that were previously submitted to the Commissioner and accepted by the OIPC.

[44] The issue in this case is whether there is authorized access to and use of electronic health records. 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.

[45] In this case, the audit logs were used by AHS to identify which affiliates had accessed the health information of the patient, or both the patient and her daughter. These measures are effective in detecting and investigating alleged privacy breaches and can also act as a deterrent to accessing another person's records without authority. This is only effective if users do not share login credentials or leave their computers unattended while remaining signed into the system.

[46] OIPC Investigation Report H2011-IR-004[2] discussed the challenges of busy environments, such as an emergency department, when health service providers need immediate access to a shared terminal. The report noted the emerging use of smart card systems that allow staff

[2] Investigation Report H2011-IR-004 is available at https://www.oipc.ab.ca/media/127962/H2011-004IR.pdf.

to quickly come and go from a computer terminal while maintaining unique login information. The SCM EMR in the South Health Campus emergency department uses a smart card system.

[47] I noted above that AHS has previously submitted PIAs for the SCM EMR to the Commissioner, as required by section 64 of the HIA. These PIAs were accepted by the OIPC. PIA acceptance attests that a custodian has undertaken a due diligence assessment of privacy risk and steps that will be taken to mitigate that risk. The PIAs for the SCM EMR outlined administrative, technical and physical safeguards that AHS said would be implemented to mitigate risk, and in particular, to mitigate the risk of unauthorized access to and use of health information.

[48] In reviewing notes from the interviews AHS held with the 49 affiliates, I observed that a number of them indicated that they either left their smart card in the electronic SMR EMR or that it was normal practice for affiliates to leave the smart card in for the whole shift. This practice is a breach of the AHS Information Technology and Acceptable Use Policy and, as noted above, defeats the purpose of smart card technology to quickly ensure unique login access to a system. This practice is also in direct contravention of the safeguards AHS said would be implemented in its PIA submissions.

[49] The HIA requires that reasonable safeguards be implemented to protect the privacy and confidentiality of health information, including protecting against unauthorized access. These safeguards must also take into account the appropriate measures to address the risks associated with electronic health records.

[50] Well known and established best practices to mitigate the risk of unauthorized access by an authorized user (e.g. snooping) include uniquely identifying a user of an electronic health record, maintaining a log of the records that a user accesses, and regular monitoring to ensure a user complies. AHS failed on all three of these best practices.

[51] First, users were uniquely identified, but due to leaving smart cards in the system, unique identification was defeated and the logs that were maintained lost credibility and usefulness for detection and investigatory purposes.

[52] Second, in some cases, AHS could not conclusively say which affiliate accessed what records in the system. AHS was forced to rely on less reliable interviews that were based on recollection of accesses made in the past.

[53] Third, AHS failed to undertake regular monitoring of the implementation of technical safeguards, as required by section 8(3) of the *Health Information Regulation*. Even if AHS was regularly monitoring, it would not have been able to effectively detect unauthorized accesses due to unique identification having been defeated. That said, regular monitoring may have allowed AHS to uncover, prior to this significant breach, that there was an unusual level or pattern of accesses that should be explored for correction and training to be provided, as needed.

[54] I find that AHS did not take reasonable steps to implement technical safeguards within the SCM EMR in the emergency department or to monitor that the safeguards in place were maintained over time.

[55] This is a particularly disappointing finding to make. AHS previously provided a PIA to the Commissioner that outlined mitigation strategies in relation to implementation of the SCM EMR, but then failed to follow through on commitments made in the PIA to mitigate risk.

Findings

AHS has taken reasonable steps to establish administrative safeguards to protect the confidentiality of health information and to protect against reasonably anticipated risks.

AHS did not take reasonable steps to implement technical safeguards within the SCM EMR in the emergency department or to monitor that the safeguards in place were maintained over time, in contravention of sections 60(1) and (2) of the HIA, and section 8(3) of the *Health Information Regulation*.

Recommendations

- Review the SCM EMR 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 South Health Campus. Review all other locations where the SCM EMR is used to confirm that there are no further gaps in safeguards implementation.

- Within 90 days from the date this report is released, inform the Commissioner about the results of the SCM EMR PIA assessment, and implementation of SCM EMR safeguards at South Health Campus. Thereafter, ensure a periodic review is undertaken in compliance with section 8(3) of the *Health Information Regulation*.

Issue 3: Did AHS take reasonable steps to ensure affiliates were aware of and adhered to all of the custodians' administrative, technical and physical safeguards in respect of health information pursuant to section 8(6) of the *Health Information Regulation*?

[56] Section 8(6) of the *Health Information 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.

[57] AHS provided information about its privacy resources and training materials, documentation regarding responsibility for ensuring appropriate access to health information, and pre- and post-incident training documentation for the affiliates who were involved in this incident. This included links to the following "standard privacy training modules and policies":

- Privacy and Security Video
- AHSecure - Collect It Protect It
- Information Privacy and IT Security Awareness which includes the Confidentiality & User Agreement
- HIA Awareness

[58] The training materials offered by AHS provide a basic understanding of privacy legislation and the importance of protecting the confidentiality of health information with regard to the access, collection, use and disclosure by AHS and its affiliates.

[59] In my view, AHS has developed reasonable training resources for its affiliates along with clear policies and procedures.

[60] Despite the above, AHS does not appear to have carried out regular monitoring of affiliates nor does it appear to have enforced its policies. Information provided during this investigation suggests that affiliates were not aware of or did not adhere to administrative, technical and physical safeguards. For example, AHS's Information Security and Privacy Safeguards Policy (1143) states:

> 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.

[61] Despite this, there was no evidence of privacy training for a number of the 49 affiliates involved in the incident. Nonetheless, these affiliates had access privileges to AHS information systems in direct contravention of AHS policies.

[62] Affiliates must also sign the AHS confidentiality and user agreement acknowledging their understanding of the conditions of access and that they are responsible for all actions performed under their user ID; however, as previously noted, several affiliates admitted to leaving their smart card in the system and remaining logged in for the whole shift. This is a contravention of AHS policies. Of equal concern is that many of the 49 affiliates reportedly had NOT signed confidentiality agreements.

[63] AHS also said that "… managers' accountability/responsibilities with regard to AHS affiliates' appropriate access to health information and any relevant training documentation regarding this responsibility is contained within the Manager Position descriptions." However, it is clear from this investigation that management of the South Health Campus emergency department supported practices that conflicted with AHS policies and contravened the HIA. The practices demonstrate that AHS did not take reasonable steps to ensure its affiliates were aware of and adhering to safeguards. Further, the practices demonstrate that technical safeguards were not effectively implemented or maintained by AHS.

[64] Information provided in this investigation suggests there was a lack of awareness due to a culture where practices were accepted over time without proper monitoring and reinforcement of training on appropriate practices that were outlined in policies.

Findings

AHS has clear policies and training in place; however, there is a disconnect with the implementation of policies. While affiliates were required to read and observe the policies, AHS did not take reasonable steps to ensure the policies were known, understood, applied and monitored.

AHS contravened section 8(6) of the *Health Information Regulation* by failing to ensure that its affiliates were aware of and adhering to all of the custodian's administrative, technical and physical safeguards in respect of health information.

Recommendations

- Complete privacy training for all emergency department affiliates, and ensure that user agreements and confidentiality agreements are signed.
- Track privacy training, and sign-off of necessary agreements, and consider building this into yearly performance management processes or some other relevant AHS process that reasonably ensures training is provided and refreshed on a periodic basis.

Issue 4: Did AHS establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information, as required by section 8(7) of the *Health Information Regulation*?

[65] Section 8(7) of the *Health Information Regulation* says:

> (7) A custodian must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information.

[66] The following AHS documents relate to performance management and discipline to address situations where an affiliate has breached, or attempted to breach safeguards, in respect of health information.

Document	Summary
Performance Management Policy 1116-04	These documents both clearly outline the process and responsibilities for applying a sanction. Each policy also includes the following statement: "certain clauses take precedence over this policy when a conflict arises with the procedure (for example applicable collective agreements)."
Progressive Discipline Policy 1116-05	
Just Culture document	This document addresses the AHS commitment to the provision of a safe, trusting and healthy work environment

	along with tools and support to ensure staff is aware of, understand and apply Just Culture Guiding Principles along with the promotion of fairness, respect, transparency, accountability and learning from mistakes to improve safety and performance.
Collective Agreement Discipline Articles and Alberta Union of Provincial Employees (AUPE) GSS Article 9	These articles set out the agreed upon process for discipline, dismissal, termination and notification of unionized affiliates, as well as the timelines for addressing a disciplinary matter.
MOOS [Management and Out of Scope] Terms and Conditions	This document sets out the senior leadership and management terms and conditions of employment, briefly outlining a manager's responsibilities regarding performance management. Under performance management, the document says, "In accordance with the AHS performance management process, managers are responsible for annually evaluating and reviewing their direct reports performance" (p. 7). This policy identifies a manager's responsibilities regarding an affiliate's performance.

[67] AHS policies establish sanctions that may be imposed if an affiliate breaches or attempts to breach safeguards. The sanctions, and process for applying them, were followed by AHS upon completion of its internal investigation, wherein AHS disciplined the 49 employees who were found to have accessed health information without authority. The process was followed when the employees filed grievances of the discipline imposed by AHS, as per their collective bargaining agreements. As noted previously, the grievance resolution process led to AHS rescinding discipline for 38 employees and reducing discipline for the remaining 11.

[68] I asked AHS to explain why different levels of discipline were administered, and why they were reduced or rescinded. AHS said:

> Common practices were evident of monitoring patients within the department for a variety of operational and educational reasons, including: assisting Triage with patient movement, being prepared to cover breaks, helping colleagues provide care, checking to see if patients are being triaged properly, and viewing unique cases to prepare for similar future cases. These common practices were cited by many of those disciplined as the reason for their access to the patient information. These practices had been condoned by department management, and education related to appropriate practices had been unclear.

[69] AHS also said:

> A consistent theme arising from these…[interviews] was that many employees believed their access to patient information was appropriate within the SHC ED which encourages a team based approach to providing health care to patients. Employees expressed their belief that their access to patients' health information was necessary to ensure safe and efficient patient care. The employees stated that they were following well-established practices which were known to the management of the SHC ED. The grievance resolution meetings brought to light that the ED environment and practices require review of AHS policies regarding accessing patient health information on a "need to know" basis only. Additional audits were subsequently requested for several users. These audits confirmed that employee practices were consistent with the practices of other staff members in the department. AHS concluded that the vast majority of staff

had accessed the patients' information in good faith and because they believed access was appropriate and necessary, not with any malicious intent.

[70] AHS said that the grievance resolution meetings found that affiliates believed their accesses were appropriate; broad access was encouraged within a team-based approach and they were following well established practices known and supported by management within the South Health Campus emergency department. Viewed in this light, and considering management responsibilities and related policies such as the Just Culture document, AHS found it was appropriate to reduce or rescind discipline.

[71] The HIA does not dictate what discipline should be applied or the process to determine what discipline is fair. The HIA requires custodians to establish sanctions that can be levied, when appropriate. A custodian should have related policies and processes to guide when and how to apply a sanction to ensure it can fairly administer sanctions, when necessary, but the way in which a custodian chooses to do this is left to the discretion of the custodian, related policies and, when relevant, collective bargaining agreements.

Findings

AHS has established sanctions that may be imposed if an affiliate breaches or attempts to breach safeguards, in compliance with Section 8(7) of the *Health Information Regulation.*

Summary of Findings

Access and Use

[72] AHS contravened the HIA when its affiliates accessed and used health information for purposes that were not authorized under section 27 of the Act. AHS affiliates contravened section 28 of the HIA when they accessed and used health information for purposes that were not in accordance with their duties to AHS (the custodian).

Safeguards

[73] AHS has taken reasonable steps to establish administrative safeguards to protect the confidentiality of health information and to protect against reasonably anticipated risks.

[74] AHS did not take reasonable steps to implement technical safeguards within the SCM EMR in the emergency department or to monitor that the safeguards in place were maintained over time, in contravention of sections 60(1) and (2) of the HIA, and section 8(3) of the *Health Information Regulation*.

Training and Awareness

[75] AHS has clear policies and training in place; however, there is a disconnect with the implementation of policies. While affiliates were required to read and observe the policies, AHS did not take reasonable steps to ensure the policies were known, understood, applied and monitored.

[76] AHS contravened section 8(6) of the *Health Information Regulation* by failing to ensure that its affiliates were aware of and adhering to all of the custodian's administrative, technical and physical safeguards in respect of health information.

Sanctions

[77] AHS has established sanctions that may be imposed if an affiliate breaches or attempts to breach safeguards, in compliance with Section 8(7) of the *Health Information Regulation.*

Summary of Recommendations

[78] The following recommendations were made:

1. Complete a review of the access to health records that is necessary to support and manage the provision of care within a team environment at the South Health Campus in a manner that ensures use of health information is limited to what is essential to meet authorized purposes set out in section 27.

2. Develop electronic health record access guidelines for South Health Campus, and provide training to all affiliates within the emergency department.

3. Review the SCM EMR 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 South Health Campus. Review all other locations where the SCM EMR is used to confirm that there are no further gaps in safeguard implementation.

4. Within 90 days from the date this report is released, inform the Commissioner about the results of the SCM EMR PIA assessment, and implementation of SCM EMR safeguards at South Health Campus. Thereafter, ensure a periodic review is undertaken in compliance with section 8(3) of the *Health Information Regulation*.

5. Complete privacy training for all South Health Campus emergency department affiliates, and ensure that user agreements and confidentiality agreements are signed.

6. Track privacy training, and sign-off of necessary agreements, and consider building this into yearly performance management processes or some other relevant AHS process that reasonably ensures training is provided and refreshed on a periodic basis.

Follow-up Actions Taken by AHS

[79] While this investigation was underway, AHS immediately began a review of relevant policies and applied an educational approach to address the culture and practices within the South Health Campus emergency department that do not align with AHS policy or the HIA. AHS reported the following activities were implemented, or were in the process of being implemented:

- Education sessions on the Health Information Act provided throughout the site to staff and physicians.
- A town hall with a panel of experts was held for staff, physicians and volunteers.
- Each Unit and Program at SHC has developed an action plan regarding Privacy and access to information. These actions are tracked and reported quarterly to site Leadership, Privacy & HR.
- Leadership within the Emergency Department has met with each individual staff member to ensure understanding of appropriate access to patient information within the scope of their role and designation.
- Managers at the site are to ensure all staff have taken the Annual Continuing Education (ACE) AHSecure Collect IT, Protect IT training within 3 months. Note the ACE training module now includes the AHS Confidentiality & User Agreement.
- Managers have added Privacy & Security awareness as a topic for discussion in staff meetings as a standing item.
- Leadership, Privacy, Communications, Human Resources, and Information Risk Management have created a series of FAQs to assist staff in determining appropriate access to patient information. These FAQs were provided to staff by the site Leadership and posted on AHS Insite.
- A working group was established with representatives from the SHC Leadership, HR, and Privacy to ensure that privacy and appropriate access to information is integrated in unit education and orientation helping to more clearly outline the practice in departments regarding appropriate access to information. This was initiated with focus group meetings with management to determine needs.
- AHS Privacy has worked with the SCM training team to embed additional material into the SCM training manual about users accessing only the information necessary to perform their role, which includes a specific focus on how to handle “Private” or confidential patients.
- Any user identified to have inappropriately accessed health information is subject to a follow up audit for all accesses by the user. These audits will begin 6 months after the investigation completion (estimating to take about months to complete for all staff). The audits will be requested by Privacy and sent to the Responsible Manager for further review.

[80] In addition, the AHS Executive approved new mandatory completion of privacy and security training and the signing of the AHS Confidentiality and User Agreement by all AHS staff once every three years. A mandatory Privacy and Security Working Group will track and report on training.

[81] AHS also confirmed that all affiliates involved in this matter completed privacy training and signed the AHS Confidentiality and User Agreement.

Conclusion

[82] This case highlights a significant breach of privacy where the focus of the investigation shifted from the affiliates to the custodian. While the affiliates improperly accessed health information, the custodian had not met its duties to implement safeguards and ensure affiliates were aware of them. In addition, the custodian had not conducted periodic monitoring to ensure compliance.

[83] AHS did have privacy policies in place and had completed PIAs on the SCM EMR, but the significant gap in this case was the failure to ensure policies and safeguards were implemented and put into practice by affiliates.

[84] There were 49 AHS affiliates disciplined for unauthorized access to health records. Discipline was reduced or rescinded. In my view, a contributing factor in the need to reduce or rescind discipline for the unauthorized access that occurred was due to the significant gaps by AHS in ensuring its affiliates were aware of their responsibilities and in the failure to implement related safeguards.

[85] The HIA ultimately holds custodians accountable for the actions of its affiliates. An affiliate must only use health information in accordance with the affiliate's duties to the custodian, but can only be held responsible to the extent the custodian has made him or her aware of the established privacy policies and implemented safeguards.

[86] This report highlights the differences between AHS policies and PIA commitments and the actual practices within the South Health Campus emergency department. It is clear that management and affiliates did not understand the requirements of the HIA to access and use health information for authorized purposes only, and some key commitments to safeguard privacy were not effectively implemented or practiced.

[87] The emergency department staff who reported this matter and the AHS Privacy Office that quickly responded to it should be commended for shining a light on this compliance issue and taking steps to address it during the course of this investigation. The actions taken by the AHS Privacy Office allowed for a thorough review and consideration of the steps that need to be taken to address the compliance issues uncovered.

[88] AHS has taken a number of steps to address this matter. Our office will follow up with AHS to confirm progress on all recommendations.

LeRoy Brower
Assistant Commissioner