INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Report of an investigation concerning misuse of the Alberta Electronic Health Record (Netcare)

November 30, 2011

Covenant Health

Investigation Report H2011-IR-004

(Investigation H3999)

Introduction

[1] On December 30, 2010, the Information and Privacy Commissioner received a complaint from an individual (Complainant 1) alleging that 9 physicians had accessed his health records through Alberta Netcare, in contravention of the *Health Information Act* (HIA). Complainant 1 had obtained a Netcare audit log report from Alberta Health and Wellness (AHW), showing that 9 physicians who were not his care providers had accessed his health records on several occasions. Complainant 1 named another physician and a nurse, not among those shown in the audit logs, that he suspected may have been responsible for these accesses. The nurse (i.e. "the Nurse) is Complainant 1's ex-spouse and the physician (i.e. "the Physician") is the new partner of Complainant 1's ex-spouse. Both the Nurse and the Physician work at a Covenant Health[1] hospital.

[2] Complainant 1's new partner (Complainant 2) and Complainant 1's mother (Complainant 3) also obtained Netcare audit log reports and identified suspicious accesses, some under the accounts of the same physicians identified by Complainant 1, as well as the accounts of 3 additional physicians. These suspicious accesses occurred within the same timeframe as the suspicious accesses to Complainant 1's records, sometimes within seconds.

[1] Covenant Health is Alberta's Catholic healthcare hospital board, active in 12 communities in the province and provides acute care, continuing care, assisted living, hospice, rehabilitation and respite care, and seniors' housing. Covenant Health has 9,434 employees and has extended privileges to 2600 physicians. Source: http://www.covenanthealth.ca/about-us.html.

[3] Because of the repeated and systematic nature of the suspicious accesses in Netcare, the Information and Privacy Commissioner decided to investigate this matter as a possible offense under section 107 of the HIA. The 12 physicians identified in the Netcare audit logs (i.e. "the 12 Physicians"), the Physician and the Nurse were identified as persons of interest.

[4] The Commissioner also opened an investigation under section 84(1)(a) of the HIA to review Covenant Health's role in this matter. Section 84(1)(a) allows the Commissioner to conduct investigations to ensure compliance with any provision of the HIA.

[5] The offence investigation ruled out the Nurse and the 12 physicians identified in the Netcare audit log as perpetrators of the suspicious accesses to the Complainants' records. After reviewing the offence investigation results, the Commissioner decided it was not feasible to pursue an offence in relation to the Physician, due to lack of admissible evidence.

[6] This report outlines the findings and recommendations from my investigation under section 84(1)(a) in relation to Covenant Health.

Background

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

[8] On request from an individual, AHW will provide a report (i.e. a "Netcare audit log") that shows which Alberta Netcare custodians have viewed the individual's records. Responding to an individual's request for their Netcare audit log is required by part 56.6(4) of the HIA and is processed as a formal request for access to health information under Part 2 of the HIA.

[9] Complainant 1 and his ex-spouse (i.e., "the Nurse") were separated at the time of this incident and involved in divorce proceedings. On October 25, 2010, Complainant 1 and the Nurse attended a meeting with their respective legal counsel. At this meeting, the Nurse's lawyer asked a question about Complainant 1's medical history. This line of questioning made Complainant 1 uneasy and he asked AHW for a copy of his Netcare access log the following week, which he received on November 24, 2010. It was at this point Complainant 1 noted the access to his health records by physicians who were not his care providers.

[10] Complainant 2 (Complainant 1's new partner) and Complainant 3 (Complainant 1's mother) also submitted their own access requests for their Netcare audit logs and received results showing suspicious accesses to their records as well. Three further physicians' accesses were identified by the Complainants as suspicious. By combining the three Complainants' audit logs, the following pattern of Netcare access emerged, summarized on Table A, below.

[11] **Table A**

Table Explanation

This table shows the date of Netcare access in the Date column, with the time of access (in 24-hour clock format) relative to the three complainants' records in the corresponding columns to the right of the date. Each access is attributed to the physician responsible for the Netcare account in question. The physicians' names have been anonymized. For example, someone using Dr. D's Netcare account viewed Complainant 1's record on December 8, 2009 at 10:18 am, then immediately went on to view Complainant 2's record between 10:19 and 10:20 am.

Date	Complainant 1	Complainant 2	Complainant 3
05-Aug-09	Dr. A 10:31-10:34		
28-Sep-09	Dr. B 19:00		
26-Oct-09	Dr. C 10:00		
22-Nov-09	Dr. C 10:00-10:12		
08-Dec-09	Dr. D 10:18	Dr. D 10:19-10:20	
26-Dec-09	Dr. E 16:44	Dr. E 16:45	
25-Jan-10	Dr. F 14:08	Dr. F 14:09-14:11	
12-Mar-10	Dr. G 11:51-11:52	Dr. G 11:53	
22-Apr-10	Dr. H 18:39		
02-May-10			Dr. G 12:34
18-May-10	Dr. G 7:37-7:38	Dr. G 7:35	
13-Jun-10		Dr. I 10:21	
29-Aug-10	Dr. J 2:01	Dr. J 2:02	
02-Oct-10		Dr. K 14:57	
09-Oct-10		Dr. L 10:16	

[12] Further investigation of network records revealed that all of the accesses occurred from within or near the emergency department at a single Covenant Health hospital. I confirmed with Covenant Health that the questionable accesses to the Complainants' health information were not related to any health services provided at a Covenant Health facility, nor had the accesses been authorized for any other reason.

[13] The audit logs summarized on Table A could be interpreted two ways: either 12 different physicians chose to put their careers at risk to view health records belonging to individuals they were not treating, or someone else with access to the same work area had used the 12 physicians' accounts to view the records.

[14] The Complainants suspected that Complainant 1's ex-spouse (i.e. "the Nurse") or the Nurse's new partner (i.e. "the Physician") may have been behind these accesses. Complainant 1 said he recognized the names of some of the 12 physicians noted in the Netcare audit logs from social events he had attended with his ex-spouse and therefore knew they were work colleagues. Further, Complainant 1 provided evidence showing that some appointments related to his divorce proceedings and other life events such as travel or illnesses, appeared to coincide with the timing of some (though not all) of the Netcare accesses.

[15] The Commissioner decided to open 14 offence investigations under section 107 of the HIA, one for each of the 12 physicians named in the Netcare audit logs, and one each for the Nurse and the Physician named by the Complainants.

[16] The Commissioner also opened an investigation under section 84(1)(a) of the HIA to review Covenant Health's actions. Initially, the Commissioner opened a second investigation of Alberta Health Services (AHS) under section 84(1)(a) because the implicated physicians and the Nurse also worked at AHS facilities. However, a review of more detailed system audit information showed that all of the suspicious accesses originated from within a single Covenant Health hospital and the AHS investigation was subsequently closed.

Application of HIA

[17] The *Health Information Act* applies to "health information" in the custody or control of "custodians."

[18] Covenant Health is a "custodian" under section 1(1)(f)(i) of the HIA.

[19] The three Complainants' audit logs show that their demographic information, lab test results, operative results, progress notes and diagnostic imaging reports were viewed. This information all falls within the definition of "health information" in section 1(1)(k) of the HIA.

[20] Under section 1(1)(a)(i) an individual employed by a custodian is an "affiliate" of the custodian. The Nurse is an employee of Covenant Health and is therefore an "affiliate" under 1(1)(a)(i) of the HIA.

[21] Under section 1(1)(a)(ii) of the HIA, a person who performs a service for a custodian under a contract or agency relationship as an appointee is considered to be their "affiliate." All of the physicians implicated in this matter have privileges at a Covenant Health hospital. The physicians' privileges were granted through appointments under the Capital Region Medical Staff Bylaws,[2] to which Covenant

[2] The Capital Region Medical Staff Bylaws applied to medical staff at the former Capital Health regional health authority and to medical staff at Covenant Health (formerly known as Caritas Health Group) facilities in the Edmonton area between July 17, 1997 and February 27, 2011. As of February 28, 2011, the Alberta Heath Services Medical Staff Bylaws

Health is a party. Because they are appointees who provide services to Covenant Health under the Medical Staff Bylaws, the 12 physicians are "affiliates" of Covenant Health under section 1(1)(a)(ii) of the HIA. The Physician who was considered a person of interest in the Offence investigation is also a Covenant Health affiliate for the same reason.

[22] 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 collection use or disclosure by the custodian. Therefore, while Covenant Health affiliates may have carried out the Netcare accesses described in this report, Covenant Health remains responsible for any related contraventions of the HIA as custodian.

[23] Alberta Netcare includes information related to health services provided throughout Alberta. This means the information in question was created by many different custodians, not solely by Covenant Health. However, Covenant Health has the ability to control its affiliates' use of Netcare by determining users' access rights based on their need to know, setting policies and monitoring system use. The information in question was accessed at a Covenant Health hospital through Netcare accounts registered to Covenant Health affiliates.

[24] Alberta Netcare is managed by Alberta Health and Wellness. Covenant Health's computers and network are managed by Alberta Health Services. Both AHW and AHS are "custodians" under the HIA. However, neither AHW nor AHS acts as a custodian in the situation under investigation. Alberta Health and Wellness manages Netcare on behalf of participating custodians, such as Covenant Health. In this context, AHW is Covenant Health's "information manager" under section 66 of the HIA.[3] AHW delegates the provision of Netcare in hospitals to Alberta Health Services. AHS also provides information technology services to Covenant Health, such as network and computer infrastructure. AHS is Covenant Health's "information manager" when it provides information technology services to Covenant Health. While the information in question was accessed through systems provided by its information managers, AHW and AHS, Covenant Health remains responsible for compliance with the HIA, pursuant to section 66(6) of the *Act*.

[25] In summary, the health services providers implicated in this breach are all Covenant Health affiliates. The health information in question was accessed through systems and infrastructure provided by Covenant Health's information managers, Alberta Health and Wellness and Alberta Health Services. The HIA applies to this matter because the information in question is health information in the custody or control of a custodian, Covenant Health.

---

came into effect, superseding the Capital Region Medical Staff Bylaws. The new Bylaws are in force at all Alberta Health Services and Covenant Health facilities throughout Alberta.

[3] AHW's role as information manager of Alberta Netcare is explained in more detail in a previous Investigation Report, H2008-IR-001, at paragraphs 39-40, available from http://www.oipc.ab.ca.

Commissioner closes offence investigation files

[26] The HIA establishes offences and penalties under section 107. In particular, section 107(2)(a) and (b) read as follows:

> **107(2)** No person shall knowingly
>
> (a) collect, use, disclose or create health information in contravention of this Act,
>
> (b) gain or attempt to gain access to health information in contravention of this Act,

[27] To charge a person with an offence under section 107 of the HIA, it must be proven beyond a reasonable doubt that the person knowingly contravened the HIA. If the Commissioner obtains clear evidence that a person knowingly contravened the HIA, he will forward that evidence to Alberta Justice and Attorney General (the "Crown") for an opinion about prosecution. Offences are prosecuted by the Crown before a judge of the Provincial Court of Alberta.

[28] Evidence obtained from Covenant Health's records and an interview with the Nurse revealed that the Nurse had been on leave during the period in which the Complainants' health information had been accessed, and that the Nurse had no involvement or knowledge of the Netcare accesses in question. Therefore, the Commissioner closed that offence investigation file.

[29] Evidence obtained from Covenant Health's records revealed that the Physician had worked at the Covenant Health hospital at or around most of the times listed on Table A. The Commissioner decided to interview the Physician.

[30] In an offence investigation, a person of interest is "cautioned" before being interviewed. This means the interviewer informs the person of interest that the person is being interviewed to gather evidence related to the possible prosecution of an offence under section 107 of the HIA, that the person is not obligated to speak with the interviewer, that the interviewer has no power to detain the person, that the person may terminate the interview at any time and that the person may retain legal counsel before being interviewed. The person is also advised that anything they say in the interview may be used against them in the prosecution of the offence. Finally, the interviewer confirms that the person understands this caution. If a person is interviewed when that person has not been cautioned, the record of the interview is not admissible in Court and cannot be used as evidence in prosecuting the offence.

[31] On April 7, 2011, the Physician's legal counsel indicated that the Physician would like to make a statement to clear up the matter, but would not make a statement under caution. Although the un-cautioned statement could not then be used in a prosecution, the Commissioner decided to take the un-cautioned statement to assist with the section 84(1)(a) investigation of Covenant Health, since that statement could possibly lead to identifying who had misused the Complainants' health information and lead to privacy improvements at Covenant Health and in

Netcare. After obtaining the un-cautioned statement from the Physician, the Commissioner closed the remaining offence investigation files.

Investigation of Covenant Health under HIA s. 84(1)(a)

[32] In the April 7, 2011 interview, the Physician admitted to having looked at the three Complainants' health information without authorization in Netcare, in a pattern consistent with the audit logs, within the same timeframe. The Physician confirmed using other physicians' Netcare accounts to perform these unauthorized accesses without their permission or knowledge. Next, the Physician stated that none of this information had been shared with the Nurse (Complainant 1's ex-spouse) and that the Nurse had no knowledge of this Netcare activity while it was underway. The Physician said the timing of the accesses had no correlation with events in Complainant 1's life and that the apparent correspondence between accesses and Complainant 1's divorce and custody proceedings was coincidental.

[33] The Physician made the following statements in the interview:

> "You know that they're going through a divorce and custody hearing… and even though I'm not a part of that, I sit on the outside… It's really been a horribly trying time… It was the only thing I could control in any way…I think it was just the only thing I felt I had some kind of a power over. I know that's wrong and it's a terribly wrong use of that power."

[34] On April 8, 2011 the Physician's counsel confirmed that the admissions outlined above had been presented in writing to Alberta Health Services. This letter was subsequently sent to Covenant Health by the Physician's legal counsel on April 15, 2011. In later meetings, I confirmed with Covenant Health that the admission had been received and was consistent with the information gathered in the interview of April 7, 2011.

Issues

[35] The Physician accessed the three Complainants' health information, but was not involved in providing health services to any of the Complainants. As a custodian, Covenant Health has a duty under the HIA to take reasonable measures to protect health information from threats such as unauthorized access to health information. A custodian's affiliates also have a duty to follow the custodian's direction with regards to information security. Because they allowed their Netcare accounts to be misused, the 12 physicians' actions also need to be considered.

[36] Therefore, I identified the following three issues in this investigation:

A. Did the affiliate (the Physician) use health information in any manner not in accordance with the affiliate's duties to the Custodian, in contravention of Part 4, section 28 of the HIA?

B. Did the custodian fail to protect health information in contravention of section 60 of the HIA?

C. Did the affiliates (the 12 physicians) use health information in any manner not in accordance with the affiliates' duties to the Custodian (Covenant Health) in contravention of Part 4, section 28 of the HIA?

A. The Physician's use of the Complainants' health information

[37] Section 25 of the HIA says,

> **25** No custodian shall use health information except in accordance with this Act.

Further, section 28 of the HIA says,

> **28** 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.

Acceptable uses of health information are listed in section 27 of the HIA. If a custodian or its affiliate accesses health information in Netcare for some reason not listed under section 27 of the HIA, this contravenes section 25 of the HIA. If the custodian's affiliate uses health information in some way that does not align with the affiliate's duties to the custodian, this contravenes section 28 of the HIA.

[38] Covenant Health confirmed that none of the Complainants sought health services at any Covenant Health facility at the time of the Netcare accesses in question. There was no other reason authorized under the HIA for the Physician to have viewed the Complainants' health information. In the interview of April 7, 2011, the Physician admitted that accessing the Complainants' health information was wrong. Clearly, viewing the three Complainants' health information was not in alignment with the Physician's duties to Covenant Health. Therefore, I find the affiliate used health information in contravention of Part 4, section 28 of the HIA.

[39] Because a custodian is responsible for any use of health information by its affiliates under section 62(2) of the HIA, Covenant Health is ultimately responsible for this misuse of health information. Covenant Health had no knowledge of this privacy breach and certainly had no hand in directing the Physician's actions in relation to the breach. However, Covenant Health had a duty to take reasonable measures to protect the health information in question, which is the focus of the next part of this Report.

B. Covenant Health's duty to protect health information

[40] Section 60 of the HIA reads as follows:

> **Duty to protect health information**
>
> **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,
>
> (b) …
>
> (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…

[41] Sections 8(6) and 8(7) of the *Health Information Regulation* are also relevant to this case and read as follows,

> **8(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.
>
> **(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.

[42] These provisions mean that custodians need to identify threats to patient confidentiality and implement reasonable measures to mitigate the risk of unauthorized use of health information. Further, the HIA places particular emphasis on mitigating the risks associated with electronic health records. Subsection 60(1)(c) refers to "reasonably anticipated threats." This means that custodians must take steps to protect health information that a reasonable person, faced with similar circumstances would also take. If a threat to confidentiality is generally well known, it is reasonable to expect a custodian would anticipate it and devise a safeguard to mitigate the threat. Finally, sections 8(6) and 8(7) of the *Health Information Regulation* place duties on custodians to make their affiliates aware of their safeguards and to impose sanctions against affiliates that breach its safeguards. It is only possible for a custodian to verify whether its affiliates are following its safeguards if the custodian is able to determine what its affiliates have

done with health information in its custody or control and be able to hold each affiliate individually accountable for their actions.

[43] In the interview of April 7, 2011, the Physician made the following statements:

> If I need to look something up and Netcare is open and ready to go, I'll often just proceed.
>
> I may have a Netcare session on that computer. I don't look to see who's logged on. I don't do it with an ill intent. It's quick and it's easy. It takes a long time to log on to Netcare. It's not an excuse, but if I need Netcare and it's running, I will use it.
>
> I know from my experience I've gone back onto Netcare and I've looked and think I'm looking into my patient and nothing makes sense and I'll look and it's another patient someone else has done the same thing. If it's there and they need it, it's running, they'll use it.

The above statements imply that it is common practice, at least at this particular emergency department, for staff to simply use whoever's Netcare account is currently logged in and available. The fact that the Physician was able to misuse 12 colleagues' accounts on 15 separate occasions provides further evidence that staff at this emergency department routinely used common Netcare login sessions.

[44] In this case, the Physician admitted to using colleagues' Netcare accounts to access health information for an unauthorized purpose. Therefore, I need to examine whether Covenant Health had reasonable safeguards in place to mitigate this threat. Before beginning this analysis it is important to understand the environment in which these unauthorized accesses took place and the nature of the threat to privacy that a custodian would reasonably anticipate in this environment.

[45] The Physician used other Netcare users' accounts from within an emergency department at a Covenant Health hospital. Emergency departments are busy workplaces, where healthcare workers are frequently called away from working at a computer terminal at a moment's notice. Further, health care workers in emergency departments share common computer terminals to access health information systems. Anytime someone leaves a computer terminal to deal with an urgent matter, it is possible they may forget or not have time to properly log off the health information system they are using.

[46] Therefore, the threat is that a person who is authorized to use Covenant Health systems and authorized to be present in the emergency department may misuse others' sessions in information systems when someone else steps away from a computer terminal without logging off. This threat poses a risk to patient privacy because the perpetrator may misuse health information, but not be held accountable for their actions. This threat also poses a risk to those who step away from the computer terminal without logging off, as they may be held responsible for the misdeeds of a co-worker.

[47] I asked Covenant Health to identify what physical, technical and administrative measures it had in place to prevent someone from using an open health information system login session for which another authorized user is responsible.

Physical Safeguards

[48] Covenant Health employs security guards, controlled areas and photo identity badges, which are all physical controls that protect health information and other assets. The Physician had been issued a photo identity badge, was authorized to be in the emergency department area, was on shift at or around the time of all of the accesses, and was an authorized Netcare user. Therefore, no one would have had any reason to question the Physician's presence in the emergency department, or the Physician's use of Netcare or other health information systems available through the emergency department computer terminals. In my view, physical safeguards would not have prevented the Physician from viewing the Complainants' health information, nor would these safeguards have done anything to prevent the 12 physicians from leaving their Netcare accounts open. I therefore concentrated my investigation on Covenant Health's administrative and technical safeguards.

Administrative Safeguards

[49] To prevent someone from misusing a computer account that is left open and unattended, many custodians establish a policy that requires users to log-off or terminate their session when they step away from a computer terminal. Covenant Health provided copies of the following policies, which I reviewed:

I-G-110 – Security in Information Handling
I-G-120 – Security of Equipment and Digital Storage Media

[50] The above policies contain the following provisions:

- Users must 'lock' computer work station, log-out of applications and/or implement password protected screensavers as appropriate if information processing equipment is left unattended.
- Users are prohibited from sharing unique user IDs and passwords assigned to support authorized access to information systems unless specifically authorized by management and Information Systems to do so.
- Users must exit applications when leaving workstations unattended. Users may be automatically logged off any running application after 15 minutes of inactivity.
- Where two or more users share workstations, each user must access application by using a unique user ID for authentication purposes unless shared user ID is authorized by Information Systems and the manager of the department.

[51] Covenant Health also gave me a copy of an Information Systems Confidentiality Agreement signed by Netcare users. This Agreement, administered by Capital Health (now AHS) and signed by the 12 physicians, contains the following statements to which each user must agree:

A. Computing facilities and services are to be used only for authorized purposes. Activity logs are maintained in order to track usage.
B. Computer user-IDs, passwords or other authorize information provided to individual users must not be shared with others.
C. Users must log-off or lock workstations located in publically accessible areas when leaving them.

[52] The same Information Systems Confidentiality Agreement was signed by the Physician on March 26, 2004.

[53] Covenant Health provided evidence that Capital Health (now AHS) had delivered security training to staff in 2005. This was security awareness training which did not relate specifically to Netcare. The curriculum did include a section that reinforced the policies on sharing computer IDs and logging off workstations, as noted in the above paragraphs. I asked whether the 12 physicians whose Netcare accounts were misused had taken this training. Covenant Health reported it could confirm that 4 of the 12 physicians had taken this training. The Physician who misused Netcare had also completed this training in 2005.

[54] Covenant Health also reported that security training related directly to Netcare was not mandatory for physicians who had hospital privileges. Therefore there were no records of any training on this topic. I find this exemption from training puzzling and worrisome. While I acknowledge that physicians understand patient confidentiality through their professional and ethical standards, this general knowledge does not necessarily translate into an inherent knowledge of technical information security controls that need to be followed in a particular application. All users need to be trained on Netcare security, including physicians.

[55] In summary, Covenant Health had established a policy telling users to log out of applications when leaving a computer terminal unattended. However, there was no evidence to show the 12 physicians whose Netcare accounts were misused had received any training in how to use Netcare securely. Four of these physicians were trained in general privacy and security awareness in 2005, but these incidents occurred in 2009-2010. No refresher training had been delivered. If system users are not trained or only trained infrequently, this creates conditions where users forget policy and, over time, actual practice diverges from written policy. As cited earlier, the HIA not only requires that custodians establish privacy and security policies; the HIA also requires that custodians make their affiliates aware of these policies and take measures to ensure their affiliates are actually following the policies.

Technical Safeguards - Background

[56] Before I review the technical safeguards that Covenant Health had in place, I will describe the kinds of technical controls that may reasonably be expected to prevent unauthorized access to systems by insiders who attempt to misuse their colleagues' computer accounts. To mitigate this risk, custodians typically employ technical controls that include unique authentication and audit logs, reinforced by other technology, such as system timeouts or smart cards. Unique authentication means that each user of an information system is assigned a user identification code and a password which only that person may use. System audit logs create a record of the actions each individual user has performed within an information system, such as creating, viewing, editing or deleting a record. For example, the Netcare audit logs showed the Complainants in this case that 12 physician accounts had been used to access their health records inappropriately. These measures can be used to detect and investigate privacy breaches and also have a deterrent effect on those who are tempted to misuse their privileges. As long as users do not share login credentials or leave their computers unattended, unique authentication combined with system audit logs helps to ensure users are individually accountable for their actions.

[57] Users are normally instructed through policy and training to log off from information systems when not using them. If a user forgets to log off, technical controls serve as a second line of defense. The most common of these technical controls is a timeout mechanism where the system logs the user off or locks the computer screen after a short period of inactivity. Individual applications (for example, Netcare) may have their own timeouts, or a network or computer terminal timeout may be used. In all cases, the user needs to re-enter a username and/or password to re-gain access once the timeout has locked their computer or application.

[58] Relying on timeouts to prevent unauthorized access presumes a scenario where users are trained to log off from applications or to lock their computers when they leave a computer workstation unattended. If the user forgets to do so, the system locks their computer, keeping data safe until the user logs in again. These kinds of controls work reasonably well in an office environment where everyone has their own computer and workspace and people are not called away frequently and suddenly. In such environments, it is more likely that workers will remember to log off and, if they forget, there is only a short period available for someone to attempt to misuse the unattended computer.

[59] Implementing system timeouts in a busy environment, such as an emergency department, presents challenges. In the first place, an application or screensaver timeout is an inconvenience on a shared workstation. When workers need rapid access to a shared terminal they may be tempted to share a password or login session. Second, in this environment, it seems unlikely that a computer will be idle long enough for a timeout to activate. In this situation, relying on a system timeout is an ineffective security control and provides a false sense of security.

[60] Other kinds of technical controls have been implemented in Alberta that take into consideration the unique risks of emergency departments and other busy work areas. For example, a number of physician clinics have informed us through Privacy Impact Assessments (PIAs)[4] that they use a smart card system in their clinic that allows staff to come and go from computer terminals quickly while maintaining unique login information. The user inserts a smart card into a reader attached to a computer terminal and logs in normally with their user name and password. The smart card then stores the user's login information. When the user needs to leave, they simply remove their smart card and the system is locked, preventing others from taking advantage of an open session. The user can then re-insert their card at another terminal and their previous login session is restored. This system makes it easy for users to share a common terminal and quickly take their user credentials with them when they leave. Most importantly from a security perspective, this system enforces individual user accountability. (Of note, this system also includes a system timeout as a third line of defense, in case a user forgets to remove their card when leaving the terminal.)

Technical controls implemented at Covenant Health

[61] Covenant Health reported technical controls were in place, which included unique user login credentials, audit logs and system timeouts. Each Netcare user is assigned a unique username and password. Further, as evidenced in this investigation, Netcare audit logs are in place to track individual users' actions within the application. However, neither of these controls is particularly useful if users are not trained to log-off when leaving a computer terminal, or commonly share their login sessions, as evidenced earlier in this report. Therefore, the only control that may have provided some protection was Covenant Health's system timeout.

[62] Covenant Health advised me that system timeouts are implemented in its emergency department as follows. A screen saver timeout is activated after a 10 minute period of inactivity on a computer. The emergency department has a generic password, which all emergency room workers know that allows staff to access the computer if the timeout has been activated. This means that anyone may de-activate the screensaver with a shared password. This control may protect an open information system session from an outsider, but does nothing to protect against insider misuse or enforce individual accountability because all staff working at the emergency department share the same password.

[63] I also asked about timeouts on the Netcare application. Alberta Health and Wellness responded to this question, advising that each Netcare custodian can set a timeout based on a risk assessment and the environment in which that custodian

[4] A PIA is a due diligence exercise, in which custodians identify and address potential privacy risks. The PIA process requires a thorough analysis of potential impacts to privacy and a consideration of reasonable measures to mitigate these impacts. Under section 64 of the HIA, a custodian must prepare a PIA that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of identifying health information and must submit the PIA to the Commissioner for review and comment before implementing the proposed new practice or system.

uses Netcare. AHW was able to tell me the 12 physicians' current timeout settings, but does not maintain records of previous settings (there is no requirement in the HIA to maintain this information). Therefore, it is not possible to know definitively what settings had been applied when the Netcare misuse took place. However, AHW's records show that all but one of the 12 physicians currently have their timeout set to a time longer than the 10-minute screensaver timeout set in the emergency department. While Covenant Health's 10-minute screensaver will still provide some protection against an outsider (as noted in the previous paragraph), these Netcare timeouts provide no additional protection because they are set for periods longer than 10 minutes.

[64] AHW has allowed physicians to set their own Netcare timeouts. In independent practice, a physician is a custodian in their own right, making them responsible for health information security in their own clinic or office. In such cases it makes sense to allow these kinds of Netcare users to set their own timeouts, based on a risk analysis. However, the 12 physicians in this case were working at a hospital as affiliates of another custodian (Covenant Health) and are not responsible for establishing security measures. In this situation, Covenant Health should have set a timeout policy, based on a risk assessment, taking into consideration the unique environment of an emergency department. Covenant Health says it did not conduct a risk assessment or set a policy on Netcare timeouts and also says it did not know that Netcare users could set their own timeouts.

[65] As stated earlier, the threat to be mitigated in this case is that an insider may misuse a colleague's system account while a computer is left unattended. Covenant Health's policies say that users must log off applications or lock the screens of computers that are left unattended. The policies also state that each user must use only their own user accounts and not share these credentials with others. At least 12 Covenant Health affiliates were not following these policies. Physicians were exempted from Netcare privacy and security training. General privacy and security training was only provided to 5 of the 13 physicians concerned in this investigation. The general training that was provided was delivered in 2005 and may have been forgotten by 2009-2010.

[66] Given that users weren't trained to log off their systems, the only thing protecting health information from misuse by insiders was the emergency department's 10 minute timeout, which any user could de-activate with a shared password. Further, the 12 physicians' Netcare timeouts do not provide any additional protection. Relying solely on these system timeouts to prevent insider abuse of information systems in busy area like an emergency department was not a useful mitigation strategy. Other technical controls need to be considered that will allow users to quickly and easily switch between login sessions while maintaining individual user accountability.

[67] Covenant Health had a policy in place to address the risk of insider abuse of information systems, but medical staff members were not following this policy because they were not consistently trained. Further, Covenant Health's technical

security measures were not implemented in a way to reasonably protect against this risk. Therefore, I find that the Custodian failed to protect health information in contravention of section 60 of the HIA.

C. The 12 physicians' use of health information

[68] I considered whether the 12 physicians whose accounts were misused should be held individually responsible for this breach of privacy. As noted above, Covenant Health did have a policy instructing users to log off computer systems when leaving them unattended. The 12 physicians did not follow this policy direction, which allowed their colleague to misuse health information in Netcare. However, given the 12 physicians' lack of security training related to Netcare and the commonly accepted practice of sharing Netcare logins in the emergency department, it would have been difficult for the 12 physicians to actually understand their duties to Covenant Health relative to Netcare security. Actual practice was in direct conflict with written policy, little or no training had been provided and the policy was not enforced. Therefore, I do not find the 12 physicians contravened Part 4, section 28 of the HIA.

Actions taken by the Custodian

Sanctions against the Physician

[69] Under section 8(7) of the *Health Information Regulation* a custodian must establish sanctions that may be imposed against affiliates who breach the custodian's safeguards. I asked Covenant Health what sanctions may apply to the Physician in this case. Covenant Health responded to this question by providing a copy of the relevant sections from the Caritas Health Group[5] [now Covenant Health] Medical Staff Bylaws, which were effective April 13, 1999, and the Capital Region Medical Staff Bylaws,[6] effective July 17, 1999. The Physician is subject to both of these bylaws.

[70] Under the bylaws, a member of the medical staff may face discipline ranging from a formal reprimand to suspension, up to revocation of appointment and privileges if they are found to be guilty of unprofessional conduct. In Alberta, the College of Physicians and Surgeons of Alberta (CPSA) regulates physicians under the authority of the *Health Professions Act*. Through the *Health Professions Act*, the CPSA has a mandate to investigate complaints of unprofessional conduct against its members, make findings, resolve complaints, provide advice and direction and administer sanctions.

[71] On June 21, 2011, Covenant Health's Chief of Staff sent a letter to the CPSA, reporting the actions of the Physician. The letter stated, "I believe this may constitute unprofessional conduct and therefore report this for further review by

[5] Covenant Health was formerly known as Caritas Health Group until October 7, 2008.
[6] See footnote 1, page 4.

the College." At the same time, Covenant Health wrote a separate formal letter of reprimand to the Physician, advising that the allegation of unprofessional conduct was being referred to the College and setting the expectation that the Physician never repeat this misuse of health information.

[72] The Information and Privacy Commissioner has no jurisdiction over CPSA investigations of unprofessional conduct or the *Health Professions Act*. Therefore, I offer no comment on the CPSA's investigation, which is ongoing at the time of this report's release.

[73] On June 21, 2011 the Physician received a letter of reprimand that was placed on the Physician's file. Further action by Covenant Health may be forthcoming subject to the results of the CPSA investigation. These results may not be known for some time. However, the Information and Privacy Commissioner expects to be advised of any further actions taken by Covenant Health relative to the Physician following the outcome of the CPSA investigation. In the meantime, I am satisfied the matter has been referred to the appropriate body with the legal authority to conduct an investigation into the alleged unprofessional conduct.

Other actions taken by Covenant Health

[74] Covenant Health committed to performing random, on-going audits of both the Physician's use of Netcare and of the three Complainants' health information held in Netcare to identify any unauthorized activity.

[75] Covenant Health's Chief of Staff wrote to each of the 12 physicians whose Netcare accounts had been misused by the Physician. Each of the 12 was informed that their accounts were misused due to their failure to log out of Netcare prior to leaving a workstation. The letters included a reminder that the physician is responsible to ensure that he or she logs out prior to leaving a workstation unattended.

[76] The site leader at the Covenant Health hospital where the breaches took place reminded all emergency department physicians of their obligation to log in and log out of information systems appropriately and to ensure that workstations are not left unattended with a user's log in session open and vulnerable to misuse. Further, a news item relating to the Security of Computer Workstations was published in the Covenant Health electronic staff newsletter, "CompassWEEKLY," to remind all staff of their obligations to protect the privacy of patients' health information by not sharing their user name or passwords and to always ensure that active log in sessions are closed prior to leaving a workstation unattended.

[77] In responding to this breach Covenant Health provided a news article about a pilot project running in Calgary hospitals, initiated by its information manager, Alberta Health Services. This system appears to be similar to the smart card system used in physician offices, described above. I asked the AHS Chief Information Security Officer (CISO) about their smartcard system. The AHS system has been deployed

in four Calgary area emergency departments and the next phase of this project will deploy the smart cards to AHS emergency departments in the Edmonton area. The CISO also advised me there would be no technical impediment to implementing this smart card system at Covenant Health facilities in Edmonton because they use the same clinical applications as AHS. The AHS smart card system may have the potential to address the challenge of allowing multiple users to quickly switch login sessions on a common computer terminal. However, there is currently no plan to implement this technology at Covenant Health facilities. I will return to this point in my recommendations.

[78] Covenant Health cooperated fully and openly with this investigation.

Recommendations

[79] While the actions Covenant Health has taken so far contribute to preventing similar misuse of Netcare in the future, I make the following additional recommendations to Covenant Health:

A. Establish a privacy and security training program that requires all staff, including physicians, to refresh their training at least once every three years. (Both AHS and Covenant Health advise that a three-year training cycle could tie-in with the existing requirement for physicians to review medical staff bylaws every three years). This training program must include general privacy and security awareness and specific training related to information systems used at Covenant Health.

B. Work with its information manager, Alberta Health Services to research and identify potential security control technologies that give staff the ability to rapidly switch between users on shared terminals while still maintaining individual user accountability.

C. Conduct a risk assessment in its facilities to determine where computer account login sharing is prevalent.

D. Work with its information manager, Alberta Health Services, to deploy rapid user-switching security controls in work areas identified through the above risk assessment.

E. Review Alberta Netcare application timeout capabilities with its information manager, Alberta Health and Wellness and establish appropriate Netcare time-out settings for its affiliates, based on risk.

F. Within 50 days of publication of this report, give the Information and Privacy Commissioner a written plan showing Covenant Health's executive-level commitment to comply with recommendations A-E.

[80] Covenant Health noted the technical controls that protect its information technology infrastructure are established by Alberta Health Services. Further, Netcare security controls are set by Alberta Health and Wellness. As explained earlier, AHW and AHS act as Covenant Health's information managers under section 66 of the HIA in this context. Covenant Health remains responsible for directing its information managers to establish reasonable privacy safeguards. However, in reality, Covenant Health may not have the ability or the power to actually direct AHS or AHW. At the same time, Covenant Health will need AHW's and AHS' cooperation and assistance to implement my recommendations. I recognize this places Covenant Health is in a difficult position. Therefore, if Covenant Health is unable to produce a plan in accordance with recommendation F because it has not received the necessary cooperation and assistance from its information managers, I will report this concern to the Information and Privacy Commissioner, who will consider what actions to take relative to AHS and AHW.

[81] I am pleased to report that Covenant Health has agreed to implement the above recommendations. Covenant Health has also agreed to inform the Information and Privacy Commissioner of any further action it decides to take relative to the Physician, following the outcome of the College of Physicians and Surgeons of Alberta investigation into this matter.

[82] I would like to thank Covenant Health for its cooperation in helping to resolve this matter.

Conclusion

[83] This investigation uncovered misuse of Alberta Netcare by an authorized user. A physician used colleagues' Netcare login sessions to view health information for reasons unrelated to patient care, contravening the HIA. This breach of privacy was enabled because strong controls to enforce user accountability in Netcare were not in place. While Covenant Health had policies to address the risk of insider abuse of health information systems, its affiliates were not trained and were not following policy, nor were effective technical controls applied. All custodians should be aware of the risk to patient privacy if they fail to reinforce their written policies with regular training and security controls.

[84] I would like to thank the complainants for bringing this matter to our attention and thank Covenant Health, Alberta Health and Wellness and Alberta Health Services for cooperating with this investigation.

Brian Hamilton
Director, Health Information Act