INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Report of an investigation of a malicious software outbreak affecting health information

August 19, 2011

Dr. Cathy MacLean

Investigation Report H2011-IR-003

(Investigations H3317, H3425, H3427 and H3976)

Introduction

[1] On January 28, 2010, the Information and Privacy Commissioner received a report from the University of Calgary ("the University" or "U of C") that a computer server at the University of Calgary Medical Clinics' Sunridge location (UCMC Sunridge) had been affected by virus software.

[2] The University issued a public news release on March 17, 2010 to notify the public about this incident, stating that approximately 5000 UCMC Sunridge patients' records had been affected and that it had sent letters to notify those patients on March 15, 2010. The news release concluded that "the viruses may have allowed unauthorized third parties to access this information remotely."

[3] The Commissioner assigned me to conduct an investigation of this matter under section 84(a) of the *Health Information Act* (HIA), which allows the Commissioner to investigate compliance with any provisions of the HIA. This Investigation Report outlines findings and recommendations from my investigation.

Background

[4] The University of Calgary Medical Clinics are family medicine clinics run by the University of Calgary in partnership with Alberta Health Services. UCMC provide general medical services, train residents from the University of Calgary's Family Medicine Program and conduct research. At the time of the incident, UCMC included two locations, UCMC Sunridge and UCMC North Hill.

[5] On March 15, 2010, the University sent written notices to the approximately 5000 affected individuals. Three of these individuals registered formal complaints with the Commissioner (our files H3425, H3427 and H3976). One of the complainants had been affected by a previous breach at UCMC Sunridge in 2008, which I also

investigated in our file H2318. As it is relevant to the current investigation, I will refer to the 2008 case later in this Investigation Report.

[6] The University of Calgary Faculty of Medicine's information technology department is known as the Health Innovation and Information Technology Centre, or HiiTec. HiiTec provided an Incident Report and an Incident Risk Analysis. According to HiiTec's Incident Report, the computer server at UCMC Sunridge was infected by nine different Trojan horse programs.

[7] According to the Information Systems Audit and Control Association's (ISACA) *Glossary of Terms*[1], Trojan horse programs are, "Purposefully hidden malicious or damaging code within an authorized computer program." Trojan horse programs often create a "back door" that allows an external party to take control of and/or steal data from the affected computer.

Application of HIA

[8] Amendments to the HIA were proclaimed in force on September 1, 2010, through the *Health Information Amendment Act*. In this Investigation Report, I refer to the wording of the HIA in force at the time the computer virus outbreak was reported to our Office in January 2010, rather than the amended version of the HIA.

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

[10] Each of the physicians practicing at UCMC-Sunridge is a health services provider who is paid under the Alberta Health Care Insurance Plan to provide health services. Therefore the UCMC-Sunridge physicians fall under the definition of "custodian" set out in section 1(1)(f)(ix) of the HIA.

[11] Dr. Cathy MacLean is the Head of the Department of Family Medicine in the Faculty of Medicine at the University of Calgary and is responsible for UCMC. Dr. MacLean is a custodian under the HIA as described in the previous paragraph and has agreed to respond to this investigation on behalf of all of the custodians at UCMC-Sunridge. When I refer to "the custodian" in this report, I refer to Dr. MacLean on behalf of the other custodians at UCMC-Sunridge.

[12] The compromised information included patient demographics, patient referrals, health insurance, billing codes and Alberta Health Care numbers (i.e. "Personal Health Numbers," or "PHNs"). This information all falls within the definition of "health information" in section 1(1)(k) of the HIA.

---

[1] *ISACA Glossary of Terms*, Information Systems Audit and Control Association, 2011, page 81, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

[13] Because the physicians at UCMC are "custodians" and the information in question is "health information," the HIA applies to this investigation.

[14] Based on information provided to our office in a Privacy Impact Assessment[2], the University of Calgary provides information technology services to the UCMC Sunridge clinic under a memorandum of understanding. Therefore, the University of Calgary is an "information manager" as defined in HIA section 66(1). The University acts as an information manager for each of the custodians at the UCMC Sunridge Clinic. Under section 66(6) of the HIA, custodians are responsible for the actions of their information managers.

[15] Section 60 of the HIA places a duty on custodians to take reasonable steps to maintain safeguards that protect the confidentiality of health information and to protect against reasonably anticipated threats to security, integrity, and unauthorized disclosure or access to health information.

Issue

[16] Did the custodian fail to safeguard health information in contravention of section 60 of the *Health Information Act*?

Analysis and findings

[17] According to the custodian, the compromised computer server was used for the following purposes:

- To back-up copies of faxes and scans
- To back-up billing submissions
- To allow a UCMC Sunridge employee to work on UCMC North Hill billing data while the North Hill employee was on vacation (one time event)
- To store draft copies of letters typed by UCMC staff for physicians.

The custodian noted that, aside from backing up billing submissions data, none of the above information should have been retained on the server.

[18] The custodian did not have a record of the decision that led to the above data being stored on this server. The custodian advised, "Current staff indicate that this is simply the way things were done."

[19] I asked the custodian when the decision was made to store data on this server. The custodian could only speculate that the decision was probably made in 2003, when the server was first installed.

[2] Under HIA s. 64 custodians must submit a PIA to the Commissioner for review and comment prior to implementing a new information system or administrative practice. The UCMC PIA was reviewed and accepted on November 19, 2004 (OIPC file H0453).

[20] I reviewed an Incident Report and a UCMC Risk Analysis, issued by HiiTeC. These reports provide a very thorough analysis of the incident and outline a number of security controls that were not properly implemented. In summary, the report observed that the Trojan horse outbreak had a number of different causes, namely:

- The server was running an older operating system with a number of known security issues.
- The server was not running updated anti-malware software with proactive scanning.
- The server was not using the University's vulnerability assessment program, where servers are scanned and critical vulnerabilities are assigned to support teams for remediation.
- HiiTeC identified 21 administrator accounts on the system. Many of the individuals using the system did not need this type of access. (Malware spreads through user accounts with elevated, or administrator privileges.)

[21] 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, and

[22] The *Health Information Regulation* also establishes a requirement to review safeguards. In particular, section 8(3) says,

> **8(3)** A custodian must periodically assess its administrative, technical and physical safeguards in respect of
>
> (a) 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) 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.

[23] These provisions mean that custodians need to identify threats to patient confidentiality and implement reasonable measures to mitigate the risk presented by these threats. 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 way to mitigate the threat. Finally, section 8(3) of the *Health Information Regulation* says that custodians must review their safeguards periodically to ensure they remain effective.

[24] On December 9, 2009, the Information and Privacy Commissioner issued a report on a Trojan horse outbreak at Alberta Health Services (AHS) (H2009-IR-007)[3]. At paragraphs 33-36, this report established that custodians must take reasonable steps to protect against malicious software. These measures include maintaining an up-to-date anti-malware system.

[25] The server at UCMC was running anti-malware software. However, the HiiTeC report revealed that the anti-virus software was an older version, which had not been supported by the vendor since 2005. Further, this anti-malware software was not performing regular scans of the system, rendering it virtually useless.

[26] Paragraph 49 of H2009-IR-007 also noted that allowing unnecessary administrator accounts on a system can lead to increased vulnerability to malware. Administrator computer accounts are needed by some users to make changes to systems. Malware needs to reach a computer account with elevated or administrative permissions in order to spread. A typical computer account with non-administrator privileges would not allow malicious programs to execute and would thus prevent their spread. Administrator accounts should only be granted to staff needing this type of access to perform their jobs. The HiiTeC report concluded that many of the 21 users at UCMC did not need this type of access.

[27] Investigation Report H2009-IR-007 did not address maintaining up-to-date operating systems as it was not identified as an issue in that case. There are two factors to consider in analyzing security practices related to server maintenance at UCMC Sunridge. First, I will consider the issue of technical maintenance of the server's operating system. Second, I will review the custodian's apparent failure to consider the risks of storing identifiable health information on the server.

[3] Investigation Report H2009-IR-007, http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2514

Server operating system

[28] The server at the root of this breach was running an older operating system. Periodically, software vendors will release updates to fix known security vulnerabilities and other problems in their operating systems. These updates are known as "patches." It is a good practice to run servers with up-to-date operating systems and to apply system patches in a timely manner, after appropriate testing. As vendors release entirely new operating systems and concentrate on patching their newer versions, older operating systems become more and more vulnerable to malware and other attacks over time. In this case, the server operating system was 10 years old and had known vulnerabilities for which the vendor had not made new patches available. As the HiiTeC report said, this server was not included the University's vulnerability assessment program.

Risk of storing health information on server

[29] In 2008 our office investigated a privacy breach at UCMC that is germane to the current investigation (our file H2318). On July 15, 2008 a staff member at UCMC Sunridge uploaded patient information to the protected area of the family medicine website, to allow a physician to retrieve the data. After this transfer, the data were not removed from the site, as had been planned. The staff member thought the site was secure, but did not know that information from this site was routinely copied to another computer server, which was accessible to the public over the internet.

[30] A patient searched their own name on Google and was able to view their own health information as well as that of other UCMC Sunridge patients. The information for each patient included name, gender, date of birth, personal health number and the patient's regular physician. A total of 1,234 patients were affected by this breach. The patient informed the Faculty of Medicine of this problem and the Faculty removed the patient data from their servers on October 27, 2008. UCMC informed all of the affected individuals and cooperated fully with our office's investigation. UCMC also agreed to conduct risk assessments in cooperation with the University to evaluate whether future proposed data storage locations have appropriate security and privacy controls.

[31] As mentioned earlier, one of the individuals affected by the 2008 breach was also affected by the current incident and was, understandably, concerned that their information may not be reasonably protected by UCMC.

[32] As noted at paragraph 22, custodians have a duty to periodically assess their safeguards. I asked UCMC whether it had conducted any inventories of its systems and whether this inventory would identify versions of operating systems, anti-malware and other software. UCMC reported that HiiTeC had conducted an inventory in 2009, which included the server that caused the current breach. However at the time, HiiTeC understood this server did not house any health information. UCMC says this misunderstanding may have been due to the fact that the clinic's main electronic medical record was stored elsewhere and it was not clear that the server at the root of the breach also contained health information. In any

case, the server was not scheduled for an immediate risk review.

[33] While the 2008 and 2010 incidents were not identical, the root cause appears to be the same. The custodian was not aware of what information was being stored on its servers and, because of this, did not (and could not) assess the risks associated with storing the information on those servers. The first step in assessing privacy risk is to identify all health information in a custodian's custody or control. Only then can a custodian assess whether it has implemented reasonable safeguards to protect that health information.

Finding

[34] In summary, the custodian did not maintain up-to-date anti-virus software, allowed unnecessary administrator accounts, ran an older operating system with known vulnerabilities and had not assessed the risks of storing health information on the server at the root of this breach. Therefore, I find the custodian failed to safeguard health information in contravention of section 60 of the *Health Information Act*.

Actions taken by the custodian and information manager

[35] Once the infected server was discovered, the University's HiiTeC group worked to contain and mitigate the damage caused by the Trojan horse programs. Heath information was removed and an attempt was made to continue using the server for other purposes to allow the clinic to maintain normal operations. Unfortunately, it became apparent the server was still infected and it was taken offline on January 14, 2010. As a result, the custodian was forced to operate with paper files until alternative arrangements were made.

[36] The custodian was able to identify the patients who were affected by this breach and notified them of the incident by mail. Similar to Alberta Health Services in the previously investigated malware outbreak (H2009-IR-007), the custodian decided to notify the affected patients. In my opinion, notification is a responsible and prudent response to this kind of breach. As stated in H2009-IR-007 at paragraph 29, "…health information is inherently sensitive. People deserve to know that their health information may have been exposed."

[37] The custodian's information manager, HiiTeC, made 10 short-term and 8 long-term recommendations to the custodian to prevent similar incidents from recurring. Not all of the recommendations focused directly on the root causes of incident, so I will not outline all of them here, However, I agree that the full combination of administrative and technical controls proposed by HiiTeC would help to mitigate similar incidents in the future and improve the custodian's overall privacy protection. Between January 14, 2010 and March 17, 2010, the custodian, through HiiTeC, implemented and improved administrative and technical controls which included:

- Up to date virus scanning was confirmed in place
- Server administrator accounts were reduced to HiiTeC technical staff only
- Personnel received training in server management best practices
- Policies and standards were communicated to clinic personnel regarding management of health information within clinic business processes.

[38] While the custodian was implementing the above remediation strategies, the custodian also made a decision to transfer its information technology infrastructure to a new information manager, Alberta Health Services (AHS). As a result, responsibility for completing the remediation recommendations resulting from this breach was transferred to AHS on March 17, 2010. The custodian confirmed that all recommendations made by HiiTeC have been addressed by AHS and that AHS is now managing the following services for the custodian:

- central file storage and secure network file access
- electronic faxing, user access and secure storage of faxes
- user accounts and security training
- desktop management, antivirus and software patching, software installation and support
- internet service access
- network access and management
- review and approval of electronic medical record implementation plans.

Further Issue

[39] As noted above, the custodian transferred its information technology infrastructure to AHS on March 17, 2010. Section 66 of the HIA requires custodians making such disclosures to have an information manager agreement in place.

[40] The pertinent sections of the HIA read as follows:

> **Power to enter agreement with information manager**
>
> **66(1)** In this section, "information manager" means a person or body that
>
> (a) processes, stores, retrieves or disposes of health information,
>
> (b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or
>
> (c) provides information management or information technology services.
>
> **(2)** A custodian must enter into a written agreement with an information manager in accordance with the regulations for the provision of any or all of the services described in subsection (1).

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

[41] An "information manager" provides information technology services to custodians. Section 66 of the HIA says that a custodian may enter into an agreement with an "information manager." A custodian may disclose health information to its information manager without patient consent, but only if an agreement pursuant to section 66(2) of the HIA is in place.

[42] Section 31 of the HIA reads as follows:

> **Prohibition re disclosure of health information**
>
> **31** No custodian shall disclose health information except in accordance with this Act.

[43] The above passage means that custodians may only disclose health information if there is authority under the HIA to do so. In the absence of an information manager agreement, I could see no other authority under the HIA to authorize UCMC's disclosure of health information to AHS.

[44] I asked the custodian whether an information manager agreement was in place with AHS. On December 17, 2010, the custodian reported that it was still working on an information manager agreement with AHS and would forward it when available. I followed-up with the custodian on this question on February 18, 2011, advising that the custodian was at risk of being found in contravention of sections 31 and 66 of the HIA. Subsequently, I received a draft information manager agreement signed by the custodian on March 21, 2011. However, the agreement had not been signed by AHS and remained unsigned when I followed up again on April 5, 2011 and again on July 12, 2011.

[45] On July 19, 2011, I gave the custodian and AHS one last opportunity to resolve this matter. On July 20, 2011, AHS and the custodian reported they had signed an appropriate agreement under 66(2) of the HIA and sent me a copy of the executed agreement. I reviewed the agreement and it meets the requirements of the HIA.

Recommendations

[46] The custodian agreed to implement the following recommendations:

- Perform an annual privacy review of its information systems, including both hardware and software, in cooperation with its information manager. The objective of this review is to identify all information systems that collect, use or disclose health information and ensure that this health information is reasonably protected and that the administrative, technical and physical privacy controls in place remain effective.

- Perform an annual review of its information management agreement with AHS to ensure that the privacy controls in the agreement remain effective.

- Renew its commitment from investigation H2318 to conduct a risk assessment before installing any new equipment or software on its information systems infrastructure.

- Provide annual privacy awareness training to staff that includes guidance on how to properly implement new technology or equipment, following a managed change process.

[47] In my opinion, the above recommendations, plus the already implemented remediation measures (see paragraph 37) are reasonable safeguards to protect against computer virus outbreaks. However, until UCMC established a contractual agreement with its information manager, UCMC's ability to ensure these safeguards were implemented was questionable. In response to questions raised in this investigation the custodian and AHS eventually did sign an appropriate information manager agreement, as outlined above. Therefore, I am now satisfied this matter has been settled.

[48] I would like to thank Dr. MacLean for her full and open cooperation with my investigation.

Conclusion

[49] Anyone who runs out-of-date computer operating systems and anti-virus software, along with unneeded administrator accounts is vulnerable to malware and hackers. Both the custodian and the information manager in this case were aware of these risks. However, they did not realize they had a time-bomb sitting on their network: an unmanaged computer containing health information that was not included in regular vulnerability scans. This investigation highlights the need for custodians to be aware of their information technology environment and to work with their information managers to conduct periodic reviews of the controls that protect health information privacy. Formal agreements with information managers are mandatory under the HIA and these agreements help to assure custodians that appropriate privacy controls are in place. While a custodian may delegate an information manager to run its information technology infrastructure, the custodian remains responsible for any failures to protect health information.

Brian Hamilton
Director, Health Information Act
Office of the Information and Privacy Commissioner of Alberta