INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Report of an investigation concerning the possible disclosure of health information in response to an employer's request

November 24, 2009

Dr. James Kozan

Investigation Report H2009-IR-005

(Investigation H2487)

Introduction

[1] In February 2009, the complainant wrote to the Information and Privacy Commissioner, claiming that a staff person at the Bigelow Fowler Clinic ("the Clinic") in Lethbridge disclosed his health information to his employer about recent appointments. Allegedly, the complainant's employer had called the Clinic to inquire about a day off he had taken for illness.

[2] The Commissioner authorized me to conduct an investigation under section 85(e) of the *Health Information Act* (HIA, or "the *Act*"). Section 85(e) allows the Commissioner to conduct investigations to attempt to resolve complaints that health information has been collected, used, or disclosed by a custodian in contravention of the HIA.

Background

[3] The complainant received a letter from his employer regarding recent absences from work, dated November 27, 2008. The complainant gave me a copy of this letter. In this letter, the employer states the complainant had claimed sick pay for October 21, 2008. The employer asked the complainant for a doctor's note regarding the absence. The complainant provided a note, dated November 8, 2008 from the Bigelow Fowler Clinic. The employer goes on to say in his letter,

> I called Bigelow Fowler Southside office at 8:35am on November 13, 2008 for confirmation of [complainant's] visit to any of their three affiliated clinics during the October 21 time period. I spoke with a nurse that had seen [complainant] on November 8 and she gave me the following information:
>
> - [Complainant] seen Dr. Lohrenz on October 9, 2008 at the Southside clinic.
> - [Complainant] had a scheduled appointment on November 15 (his first day off) to see Dr. Longair at the Westside Clinic but never showed up.
> - [Complainant] seen Dr. Meller on November 8 to obtain the doctors note that claims [complainant] was off on October 21, 08 for [diagnosis].

> The nurse confirmed in her database that [complainant] had not visited any of their clinics from October 10 through November 7, 2008. Any visit to any of their clinics would show up in their database.

[4] The complainant claims he was disciplined as a result of information revealed in this possible disclosure by the Clinic.

[5] The complainant contacted the Clinic in November 2008 to report the above letter from his employer. In response, the Clinic performed an internal investigation, but was not able to determine whether any of its employees may have accessed or disclosed the complainant's information. The complainant was not satisfied with these results and asked the Information and Privacy Commissioner to conduct an investigation under the HIA.

[6] The Bigelow Fowler Clinic is composed of three clinics in Lethbridge: Bigelow Fowler East (also known as the "Superstore clinic"), Bigelow Fowler West and Bigelow Fowler South. Twenty-three physicians practice at these clinics and patients may attend any one of the three locations. The employer's letter says he obtained the complainant's health information by calling the South location.

[7] Bigelow Fowler's patient records are kept in an electronic medical record (EMR) system. An EMR is a record of patient encounters maintained in an electronic information system. The Clinic has set up its EMR as a centralized system, making patient records accessible by staff from computer terminals at all three Bigelow Fowler locations. Bigelow Fowler implemented an EMR from National Medical Solutions (NMS) in 2005, known as NMS Clinic. NMS is no longer in business and the NMS Clinic EMR is now owned by Optimed Software Corporation.

[8] The Bigelow Fowler EMR is designed to record each access to a patient's record in a log. A clinic staff member with proper authority should be able to review this system log to determine what health information was accessed by a particular user, along with the time of access.

Application of HIA

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

[10] The complainant named the Bigelow Fowler Clinic in his complaint. The Bigelow Fowler Clinic is not a custodian as defined in the HIA. However, each of the three physicians named in the employer's letter from November 27, 2008 is a health services provider who is paid under the Alberta Health Care Insurance Plan to provide health services. Doctors Lohrenz, Longair and Meller therefore fall under the definition of "custodian" set out in section 1(1)(f)(ix) of the HIA.

[11] Dr. Kozan is President of the Bigelow Fowler Clinic and agreed to respond to this investigation on behalf of the above-named custodians. Dr. Kozan is also a custodian under the HIA as described in the previous paragraph. When I refer to "the custodian" in this report, I refer to Dr. Kozan, on behalf of the other custodians at the Clinic.

[12] The employer's letter of November 27, 2008 includes information about the complainant's attendance at various appointments at the Clinic and provides information about his diagnosis in reference to the appointment with Dr. Meller. Consequently, this information falls under the definition of "health information" set out in section 1(1)(k) of the HIA.

[13] Clinic staff who may have responded to the employer's request for information about the complainant's appointments are individuals employed by the custodians at the Clinic and are therefore "affiliates" under s. 1(1)(a)(i) of the HIA. Under the HIA, a custodian is responsible for the actions of its affiliates.

Issues

[14] Did the Custodian disclose the complainant's health information in contravention of Part 5 of the *Health Information Act*?

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

Analysis and findings

Disclosure

[16] I reviewed the results of the Clinic's internal investigation and interviewed the Clinic Manager, who serves as its privacy officer. I asked if the Clinic could confirm whether a staff member had, in fact, disclosed the complainant's health information as described in the employer's letter. After conducting internal interviews and meetings, the clinic found no staff member willing to claim responsibility for disclosing the complainant's health information. Based on my review of the clinic's internal investigation, I am satisfied that the Clinic conducted its interviews and meetings thoroughly and I believe there is little to gain in re-conducting similar interviews and meetings with staff myself. I therefore moved my focus to consider whether the Clinic's EMR contained any evidence that would point to the possible disclosure.

[17] The employer's letter implies that whoever provided the information about the complainant's visits referred to a clinic EMR, where it says, "The nurse confirmed in her database that [complainant] had not visited any of their clinics from October 10 through November 7, 2008." The EMR's system logs should be able to identify whether a staff member viewed the complainant's records within the timeframe the employer says it gathered the information about the complainant's visits to Bigelow Fowler Clinics.

[18] Unfortunately, the custodian advises there are no system logs that would identify whether an employee may have accessed the complainant's health information in the clinic EMR. The Clinic's internal investigation revealed that its previous EMR vendor, NMS, had turned off the logging feature to improve system performance at the time the EMR was installed. Neither the custodian nor the clinic's current EMR vendor, Optimed was aware the system logs were turned off until the clinic

began its internal investigation. This means it is impossible to gather any evidence from the EMR about whether or not any staff member may have viewed the complainant's record while in conversation with the complainant's employer. I will return to this issue later in my report.

[19] The custodian raises some doubts about the accuracy of the employer's letter. For example, the custodian points out the patient missed an appointment on October 15, rather than November 15, as noted in the employer's letter. The custodian also notes that both the East and South locations reported receiving calls on November 13 from a male and a female, asking for the complainant's health information. In both cases, Clinic employees say they did not provide any information to the callers. Finally, the custodian says it is possible that the complainant sought care at another clinic, and that some of the information may have come from that clinic, or even from the employee himself.

[20] I find it difficult to believe the employer could have discovered such specific references to the complainant's visits to Bigelow Fowler Clinics from another source. However, in fairness, there is no evidence other than the employer's note to indicate that a Clinic staff member disclosed the information. The complainant has not asked the Commissioner to investigate the actions of his employer, which could perhaps shed some light on this question.

[21] No one at the Clinic came forward to claim responsibility for this alleged disclosure and, because system logs were not kept, there is no record of anyone accessing the complainant's information at the time in question. Therefore, due to lack of evidence, I cannot find that the custodian disclosed the complainant's health information in contravention of Part 5 of the *Health Information Act*.

Safeguards

[22] I will now consider whether the custodian had implemented reasonable safeguards to protect health information.

[23] Section 60 of the HIA says that custodians must implement physical, administrative and technical safeguards to protect health information from unauthorized disclosure. The following sub-sections are particularly relevant to this case:

> ***60 (1)*** *A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will*
>
> > *(a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,*
> >
> > *...*
> >
> > *(c) protect against any reasonably anticipated*
> >
> > > *...*
> > >
> > > *(ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,*
> >
> > *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,

[24] The *Health Information Regulation* ("the Regulation") provides further guidance in the following subsections of section 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.*

[25] To summarize the above sections of the HIA and the Regulation, custodians need to implement reasonable measures to ensure that their affiliates (employees) comply with the *Act* and protect patient confidentiality. The safeguards must include measures that specifically address the risks associated with electronic health record systems. The custodian must establish sanctions that may be imposed against affiliates that breach these safeguards. Therefore, it stands to reason that the custodian needs to monitor compliance and to be able to identify anyone who has broken the rules within electronic health record systems.

[26] I reviewed Bigelow Fowler's administrative controls and technical safeguards that allow the custodian to ensure HIA compliance and to identify affiliates who may have contravened the *Act*.

Administrative safeguards

[27] I asked the custodian to provide a copy of the policies governing access and disclosure of health information by employees. The custodian provided a confidentiality policy and an oath of confidentiality that all employees sign on hire.

[28] I also reviewed a Privacy Impact Assessment (PIA) the custodian provided to our Office for review in January 2006, when the Clinic implemented its EMR.[1] The PIA includes privacy and security policies that provide clear direction to employees on accessing and making disclosures of health information in compliance with the HIA.

[29] Prior to the incident under investigation, the Clinic did not conduct regular training for its staff regarding privacy or the HIA. After the incident, the Clinic Manager met with staff at all three Bigelow Fowler locations to review privacy and confidentiality requirements. The Clinic Manager advises that regular HIA and privacy awareness training will be provided to all staff from now on.

[1] 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 Bigelow Fowler Clinic PIA was reviewed and accepted on February 22, 2007 (OIPC file H1103).

[30] It is also worth noting that Clinic employees reported receiving calls from unknown individuals asking for the complainant's health information (see paragraph 19) and refused to provide it. This indicates to me there was general awareness among staff that this kind of disclosure would not be appropriate.

[31] In my opinion, with the addition of regular training, the custodian has implemented reasonable administrative safeguards to protect health information from unauthorized disclosure.

Technical safeguards

[32] The employer's letter says the Clinic employee "verified in her database" that the complainant had not visited any Bigelow Fowler site within a date range. This implies that whoever may have disclosed the complainant's health information was using an EMR while speaking with the employer.

[33] Section 60(1)(d) of the HIA says that custodians must monitor their affiliates' compliance with the HIA. A good way to monitor compliance in an EMR is to conduct periodic checks of employee actions by reviewing system logs to confirm that all uses of health information are related to affiliates' work responsibilities, based on a need to know. As stated at paragraph 18, the Clinic had not implemented the system log in its EMR.

[34] The Clinic policies submitted to our Office in January 2006 include a section on technical safeguards for its EMR. This section includes the following policies:

> 4.1 All Bigelow Fowler Clinic information systems users are assigned a unique identifier (User ID) that restricts access to data and application systems to that information required for the administration of their duties.
>
> 4.2. Bigelow Fowler staff members shall only access and use information systems under their assigned User ID. The use of another person's User ID is prohibited.
>
> 4.5 To detect unauthorized access and prevent modification or misuse of user data in applications, systems should be monitored to ensure conformity to access policies and standards. Appropriate security controls, such as audit trails, should be designed, implemented and reviewed every 6 months.

[35] The Clinic worked with the Physician Office System Program (POSP)[2] to implement its EMR. EMR system requirements are set by the Physician Office System Program Committee and are known as Vendor Conformance and Usability Requirements[3] (VCUR). VCUR (2006) says EMRs must be capable of capturing and recording logs of records that were viewed or printed by user identity and patient identification number. The Requirements also state the

---

[2] The Physician Office System Program (POSP) is a tripartite arrangement between Alberta Health and Wellness, the Alberta Medical Association, and Alberta Health Services (formerly Alberta's Health Regions). POSP provides funding and information technology services to physicians to implement clinic electronic health records. Its stated role is "to enable the use of electronic medical records by physicians ...to improve patient care and support best practice care delivery within Alberta's electronic health environment." See www.posp.ab.ca for more information.

[3] The Office of the Information and Privacy Commissioner has advised POSP since 2001 in its efforts to develop EMR system requirements that comply with the HIA by participating on POSP's Technical, Security and Privacy Working Group as an ex-officio member. This Working Group advises the Physician Office System Committee, which formally sets system requirements.

EMR vendor must advise the custodian in developing procedures to review the audit trail that tracks access to patient data by date and time.[4] Bigelow Fowler's EMR, NMS Clinic, does have these system logging capabilities; however, this feature of the EMR was not activated.

[36] All of the physicians at the Clinic, including those named in this report, signed a form indicating they reviewed VCUR requirements and had discussed them with their EMR vendor. This form, known as the "Vendor/Physician sign off on Advice" form, was sent to our Office as part of the custodian's January 2006 PIA submission. This form is actually a cover sheet for a detailed appendix, showing the custodian's consideration of each of the VCUR requirements (including system logging), which is to be sent to the POSP Program Office. The Office of the Information and Privacy Commissioner does not routinely review the appendices. However, our Office does rely on the sign-off forms as evidence that custodians have considered and implemented reasonable technical security measures in their EMR.

[37] I asked the POSP Program Office to produce their copy of the detailed appendix from the Vendor/Physician sign-off process. I wanted to see what specific advice (if any) the Clinic's EMR vendor, NMS, had given to the custodian regarding system logs, or whether the custodian had signed-off on any deviations to the system logging requirement. POSP officials were unable to locate this appendix. The Clinic did not have a copy of this document either. Our Office will be following up with POSP to determine whether this is an isolated incident, or whether this represents a systemic problem.

[38] Based on the Clinic policies and the EMR system capabilities outlined above, the custodian should have been able to identify whether an employee accessed the patient's data on the date indicated by the employer, November 13, 2008. Being able to identify a specific employee would have allowed the custodian to follow-up with the employee and thoroughly investigate whether they disclosed the complainant's health information to his employer. Alternatively, the EMR system log could have revealed that no one accessed the complainant's records at that time. Finally, I note that if the custodian had followed its own stated policy of monitoring system use every six months, it would have discovered that system logs had not been implemented well before the current incident under investigation.

[39] By failing to implement system logs in the Clinic EMR, I find that the custodian failed to safeguard health information in contravention of section 60 of the *Health Information Act*.

Actions taken by the custodian and EMR vendor

[40] After hearing from the complainant about the letter from his employer, the custodian conducted an internal investigation and interviewed staff members to attempt determine the source of the information. The Clinic Manager met with the complainant to review the results of the internal investigation.

---

[4] Vendor Conformance and Usability Requirements (VCUR) 2006, Physician Office System Program, http://www.posp.ab.ca/vendorinfo/vcur.aspx

[41] Following the complaint and internal investigation, the Clinic Manager met with staff at all three Bigelow Fowler locations to review privacy and confidentiality requirements.

[42] Optimed, the vendor who now owns the NMS Clinic EMR product, [5] worked with Bigelow Fowler to test and implement system logging. Once alerted to the failure of NMS to turn on audit logging at Bigelow Fowler, Optimed investigated other implementations of NMS Clinic in Alberta and identified that only 30% of these clinics have the system logging feature turned on. Optimed informed me that it has contacted all of its customers currently using NMS Clinic and advised them to turn on the system logging feature, offering instructions and technical assistance. To avoid confusion, I note that the shortfall in system logging identified in this report refers only to the EMR system known as NMS Clinic, not Optimed's other EMR product, Accuro.

Recommendations

[43] The custodian has agreed to implement the following recommendations:

- Formalize regular HIA and privacy awareness training for all Clinic staff with a yearly review of confidentiality requirements.
- Implement system logging in the Clinic electronic medical record.
- Develop and carry out a plan to review electronic medical record use by clinic staff every six months to ensure compliance with the HIA.

[44] I make two further recommendations to all custodians subject to the HIA who have implemented an electronic medical record:

- Ensure your EMR system logs are operational and that you know how to review and interpret them.
- To be in compliance with the HIA, you need to review your EMR system logs periodically to ensure your affiliates are accessing health information appropriately.

Conclusion

[45] This investigation was not able to determine whether the custodian disclosed health information in contravention of the *Health Information Act*. By failing to have a system log that would reveal who accessed data in its electronic medical record, the custodian failed to meet the requirement to ensure its affiliates were complying with the *Act*. I would like to thank the custodian and Optimed for their full and open cooperation with my investigation.

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

[5] See paragraph 7.