INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Investigation Report Concerning Disclosure and Protection of Health Information

Investigation Report H2009-IR-006

October 20, 2009

Dr. Johan Myburgh

(Investigation H2732)

Introduction

[1] On May 11, 2009, the Information and Privacy Commissioner (the "Commissioner") received a complaint from an individual (the "Complainant") in which he alleged that his health information had been disclosed by an employee of Dr. Johan Myburgh (the "Custodian") in contravention of the *Health Information Act* (HIA).

[2] The Complainant wrote to the Commissioner after receiving an email from his ex-wife. The Complainant alleges that his ex-wife was given information about his medications by a specific employee (the employee) of the medical clinic where his doctor works. The Complainant advised the Commissioner that the clinic uses an electronic medical record (EMR) system, and alleged that the employee recently accessed his health information in the EMR for the purpose of disclosing information to his ex-wife for use in a matter currently before Family Court.

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

[4] This report lays out the findings and recommendations resulting from my investigation.

Background

[5] The Complainant currently receives health services from Dr. Johan Myburgh. Dr. Myburgh is one of four physicians practicing at the Fairview Medical Clinic (FMC or "the clinic"). Prior to beginning to receive health services from Dr. Myburgh in early 2006, the Complainant saw other physicians at the clinic. The physicians at the FMC share responsibility for the administration of the clinic and hire staff to assist them in this regard.

[6] The physicians practicing at FMC have used an electronic medical record (EMR) system to store and manage health information since 2004. The employee had full access to the EMR system that stored the Complainant's health information.

[7] On March 27, 2009, the Complainant received an email from his ex-wife stating that the Complainant "should go back on [his] med's". The Complainant believes that the employee provided his ex-wife with information about his decision to stop a particular medication in early 2006. He alleges that the employee obtained this information by reviewing his medication profile in the clinic's EMR system. Specifically, he states in his letter to the Commissioner:

"I believe because of this possibility (that the employee accessed his health information through the EMR), that is why my ex-wife asked me… about me starting to take my medication again, because how does she know that possibly I was not still taking it, we have been apart for almost 6 years now and my last prescription for XX was in the spring of 2006."

[8] The Complainant provided the email of March 27, 2009, from his ex-wife in support of his allegations.

Application of the HIA

[9] The *Health Information Act* (HIA) applies to "health information" in the custody or under the control of a "custodian".

[10] "Health information" is defined in section 1(1)(k) of the HIA to include "diagnostic treatment and care information", "health services provider information" and "registration information"[1]. I attended the FMC during the course of my investigation and reviewed the Complainant's record in the EMR system. This record contains a mixture of diagnostic treatment and care information, health services provider information and registration information. I have reviewed the information at issue in this case and confirm that it is health information.

[11] The term "custodian" is defined in section 1(1)(f) of the HIA, and includes:

(f) "custodian" means

…

(ix) a health services provider who is paid under the Alberta Health Care Insurance Plan to provide health services;

[12] Dr. Myburgh is a health service provider that was paid under the Alberta Health Care Insurance Plan to provide health services to the Complainant. Dr. Myburgh is not the only physician at the FMC to have provided health services to the Complainant; however, he is the physician that the Complainant has been seeing since 2006 and is the physician named in the complaint.

[13] As the information in question is health information and Dr. Myburgh is a custodian, I find that the *Health Information Act* (HIA) applies to the alleged disclosure of the Complainant's health information.

Issues

[14] The issues to be considered in this investigation are:

1. Did Dr. Myburgh disclose health information in contravention of the HIA?

2. Did the custodians practicing at the FMC take reasonable steps to protect health information against loss as required by section 60 of the HIA?

---

[1] These terms are further defined in sections 1(1)(i), 1(1)(o) and 1(1)(u) of the *Health Information Act* and section 3 of the *Health Information Regulation.*

Analysis

Issue 1 - Did Dr. Myburgh disclose health information in contravention of the HIA?

[15] The Complainant alleges that the employee reviewed his health information in the clinic's EMR system and disclosed information about his medications to his ex-wife.

[16] The Complainant contacted me early in this investigation and stated that he did not want Dr. Myburgh to be investigated in relation to his complaint. The Complainant stated he specifically wanted the complaint to be made against the employee.

[17] The individual against whom the specific allegation has been made is an employee of the FMC. As such, she is Dr. Myburgh's employee. Section 1(1)(a)(i) of the HIA defines "affiliate" to be an individual employed by a custodian. The employee is Dr. Myburgh's affiliate under the terms of the HIA.

[18] Section 62(3) of the HIA specifies that any collection, use or disclosure of health information by an affiliate is considered to be a collection, use or disclosure by the custodian. As such, any alleged privacy breach on the part of Dr. Myburgh's affiliate is considered to be an allegation raised against Dr. Myburgh. I advised the Complainant that I could not investigate the affiliate in isolation of an investigation of the custodian and provided an opportunity for the Complainant to withdraw his complaint. He did not, therefore the investigation against Dr. Myburgh proceeded.

[19] In order to determine whether a disclosure of health information occurred, I must first examine who may have had access to the information that is alleged to have been disclosed. When I have confirmed who had access to the health information at issue, I can then consider whether or not there is sufficient evidence before me to determine that a disclosure of health information took place. I am only able to consider whether or not a disclosure of health information was in accordance with the provisions of the HIA after confirming that a disclosure took place.

[20] The FMC used a Rise/Purkinje EMR from 2004 to January 2006. A Med-Access EMR has been in use in the clinic since January 2006. These systems are designed to record each access to a patient's EMR record. Review of such a log allows someone to determine what health information was accessed by a particular user along with when the access took place.

[21] I asked Dr. Myburgh to obtain an audit log for the Complainant's EMR record. While initially advised by Med-Access that such a log could only be produced for one year prior to the request, Dr. Myburgh was eventually able to secure an audit log for the period of January 2006 to the present.

[22] The audit log indicated that the employee accessed the Complainant's health information on several occasions between March 2006 and June 2006. The employee has not accessed any portion of the Complainant's EMR record since June 2006. Dr. Myburgh reviewed the audit log in detail and concluded that each of the accesses followed an interaction the Complainant had with the clinic, and where the employee was required to follow-up on the visit. For example, several of the accesses relate to billing Alberta Health Care for a visit. Dr. Myburgh stated that it would be reasonable for the employee to review the physician's notes in the EMR in order to bill AHCIP as she routinely performed that function for the clinic. In other instances, Dr. Myburgh ordered tests or additional follow-up for the Complainant and the employee was charged with that follow-up. Dr. Myburgh states he is confident that each access to the Complainant's EMR record was related to the provision of a health service, or the administrative services

that must run along with the provision of health services. I reviewed the system audit logs and agree with Dr. Myburgh – it appears to me that the Complainant's health records were accessed by staff at the FMC for purposes related to their employment with the FMC.

[23] In addition to reviewing the audit logs, I also interviewed both Dr. Myburgh and the employee. During that interview, the employee stated that she never accessed the Complainant's EMR record for non-job related purposes. She also stated that she has not disclosed information about the Complainant that came to her knowledge through her employment with the FMC to the Complainant's ex-wife. I also discussed the FMC's privacy training program with the employee and am satisfied that she was aware that accessing health information in the clinic's EMR for personal purposes is in contravention of the HIA and office policy.

[24] Dr. Myburgh told me during this interview that the Complainant made his concerns about the potential for the employee to access his health information through the EMR known to him in April of this year. Dr. Myburgh immediately "masked" the patient encounter in the EMR. When health information is masked in an EMR system, it can only be accessed by the user who created the health information unless another user with sufficient permission overrides the mask. This is referred to as "unmasking" the record. As with all other accesses of health information in the EMR, the system logs an unmasking event. My review of the audit logs indicated that no user has unmasked the information that Dr. Myburgh masked at the request of the Complainant. I must note, though, that Dr. Myburgh masked only those encounters where he had provided treatment to the Complainant. Dr. Myburgh stated he was not aware of the ability to mask the entire patient record in the EMR.

[25] The Complainant's allegation is that the employee accessed his health information in the EMR and disclosed information about his discontinuation of a medication in early 2006 to his ex-wife. The employee has not accessed the Complainant's health information in over three years. While it is true that the EMR record at the time when the Complainant last accessed it contained information about the Complainant's prescriptions for the medication in question, it does not contain reference to the discontinuation of the medication that took place in early 2006. All the employee would have been able to see when she last accessed the Complainant's EMR record was that the Complainant had been prescribed this medication, and that the prescription had been refilled twice. The employee has not accessed the Complainant's EMR record since the last refill of the prescription in question expired and was not renewed. She has no way of knowing, based on her access to the record, that the Complainant was no longer taking the medication in question.

[26] In support of his allegation, the Complainant provided an email from his ex-wife stating her opinion that the Complainant "should go back on [his] med's". His position is that his ex-wife would only know of him discontinuing a particular medication if that information had been provided by the employee. That being said, I note that the Complainant states elsewhere in his letter of complaint that maintaining this particular drug therapy had been a topic of discussion with his ex-wife. It is far more plausible to me that the Complainant's ex-wife knows about his medications through their relationship than through the disclosure of that information by an employee of his doctor.

[27] The evidence provided by the Complainant is speculative. The email does not prove that the ex-wife had access to information related to discontinuation of drug therapy for a known condition. The email proves that his ex-wife, whom the Complainant acknowledges had previous knowledge of his prescription for this particular medication,

stated her opinion that he had stopped taking the medication and should resume. The email certainly does not prove that information about the discontinuation of the medication was obtained from Dr. Myburgh or one of his employees.

[28] There is no evidence before me to indicate that the employee accessed the Complainant's medication profile for any purpose other than to perform the job functions assigned to her as a staff member of the FMC. The audit logs demonstrate that the employee accessed the Complainant's EMR record only when required to complete a task that had been assigned to her by Dr. Myburgh. The employee has not accessed the Complainant's EMR record in over three years. At the time that the employee last accessed the EMR, the EMR indicated that the Complainant had been prescribed several refills of the medication in question.

[29] There is no evidence before me to support the allegation that Dr. Myburgh's staff disclosed health information to the Complainant's ex-wife. To the contrary, the evidence that was provided to refute the allegation leads me to believe that such access and disclosure did not take place.

[30] I find that Dr. Myburgh did not disclose the Complainant's health information in contravention of the HIA. As the Complainant specifically raised this allegation against one employee, I wish to offer additional clarity to the Complainant on this point - in finding that Dr. Myburgh did not disclose health information in contravention of the HIA, my finding is also that the employee did not disclose his health information to his ex-wife.

Issue 2 - Did the custodians practicing at the FMC take reasonable steps to protect health information against loss as required by section 60 of the HIA?

[31] I have previously established that an EMR has been in use at the FMC since 2004 but that Dr. Myburgh was only able to secure an audit log for the period of January 2006 to the present. While this does not alter my findings in relation to whether or not Dr. Myburgh disclosed health information in contravention of the HIA, it gives rise to a secondary question related to whether or not health information has been adequately protected by the custodians practicing at the FMC[2].

[32] As required by section 64 of the HIA, the custodians practicing at the FMC completed a privacy impact assessment (PIA) when they decided to implement an EMR system and submitted it to the Commissioner for his review and comment. I have reviewed this PIA as it relates to the safeguards that have been developed to protect health information in the EMR. The FMC made the following statements in its PIA:

- That it had implemented an EMR system that fully conformed with the Vendor Conformance and Usability Requirements (VCUR) generated by the Physician Office System Program (POSP)[3], including requirements related to the content and storage of audit logs

---

2 Dr. Myburgh joined the FMC in early 2006. Dr. Myburgh was not directly involved in the decision to discontinue the use of one EMR and begin use of another.

3 POSP assists physicians to purchase computers and medical software in support of improved patient care. In order to receive POSP funding, physicians must choose an EMR system that has been demonstrated to have met the "Vendor Conformance and Usability Requirements" (VCUR). VCUR was originally published in 2003 for 2004 adoption and was updated in 2006. The Rise/Purkinje EMR discussed in this report conformed to VCUR 2004. The Med-Access EMR in use at FMC today conforms to VCUR 2006 standards. Both VCUR 2004 and 2006 contain requirements that an EMR log information about which users accessed the EMR, what they looked at or did within the EMR and when that action took place.

- That access to the EMR would be based on unique user ID, and that all access to the EMR would be logged
- That designated staff, with assistance from Med-Access, would monitor the system for unauthorized access and use
- That staff would be trained on privacy and confidentiality matters and would execute an oath of confidentiality
- That staff would maintain a log of all disclosures of health information

[33] Audit logs are an essential safeguard in electronic health records systems, including EMRs. These logs, when properly implemented, can allow a custodian to determine who has accessed and viewed health information within their EMR with a very high level of certainty. They also play a critical role in maintaining the reliability and integrity of data, as changes to information are also logged. Poorly implemented audit logging functionality renders the control ineffectual.

[34] As part of my investigation, I asked Dr. Myburgh to produce an audit log that would demonstrate which staff members viewed the Complainant's health information in the EMR. Dr. Myburgh asked his EMR vendor, Med-Access, for assistance with this task. Med-Access advised Dr. Myburgh twice that the audit log was only retained for a period of one year. I then requested that the complete audit log for the Complainant's EMR record be provided directly to me.

[35] Med-Access advised me that it was unable to generate an audit log for the period of 2004 to January 2006 as the FMC has used two EMR systems since automating in 2004. The FMC used a Rise/Purkinje EMR between 2004 and January 2006. In January 2006, the FMC decided to begin using the Med-Access EMR. Med-Access advised me that they extracted some demographic and clinical data from the Rise/Purkinje EMR in January 2006 and imported it into the Med-Access EMR that was to be used in the clinic. The process is termed "data migration". Med-Access did not migrate all health information from the Rise/Purkinje EMR into the Med-Access EMR. Med-Access told me that it migrates data that the physician presumes to be sufficient to maintain "continuity of care" and that it relied on direction from POSP in determining what information would meet this standard[4]. Med-Access also told me that it generally advises physicians to retain the health information that is not migrated so as to be able to meet medico-legal requirements. Med-Access was not able to provide documentation to prove that it advised Dr. Myburgh and his colleagues that the data migration was partial in this case and that they should retain the health information that had not been migrated from the old EMR.

[36] When the FMC migrated from a Rise/Purkinje EMR to a Med-Access EMR, only select information was extracted from the old EMR and imported into the new EMR. The information that was excluded from migration included some diagnostic treatment and care information and metadata[5] including all audit logs. The custodians at the FMC did not retain a copy of the health information from the Rise/Purkinje EMR when that system was decommissioned. The result is that no audit log of access to and disclosure

---

4 The Health Information Standards Committee for Alberta adopted the draft "POSP Medical Summary for Transfer of Patient Data (ToPD)" on July 18, 2005. This specification was developed to ensure that physicians moving from one EMR to another could extract core health information from their old EMR and import it into their new EMR. The ToPD specification does not contemplate the export and import of all health information – ToPD is intended to address the need for "summary data" to move from EMR to EMR.

5 Metadata is broadly defined as "information about information". In this case, the audit logs are metadata as they are information about who looked at health information within the EMR system

of health information can be produced for the period from system implementation sometime in 2004 to January 2006.

[37] Section 60(1)(c) of the HIA says:

> *60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will*
>
> *…*
>
> *(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, …*

[38] The HIA does not specify the length of time for which health information must be retained, although it does state that a log of what information has been accessed or disclosed must be maintained for a period of ten years[6]. It stands to reason that if information about the disclosure of health information must be maintained for ten years after the point of disclosure, that the health information itself should be maintained for at least that same length of time. This interpretation generally aligns with the College of Physicians and Surgeon's policy on Physicians' Office Medical Records ("the CPSA policy"), which states:

> *"A physician shall retain for a minimum period of ten years, or in the case of minor patients, until two years after the age of majority or for ten years, whichever is longer, by electronic means or storage of hard copy, the entire interpretive report and a segment of continuous physiologic recordings, whether abnormal or not, sufficient to support the interpretation made.[7]"*

[39] The physicians at the FMC migrated some health information from the old EMR into the new EMR, but did not migrate all of the health information. Selective data migration requires a custodian to take steps to protect the non-migrated data against permanent loss. The options available to physicians in this regard range from maintaining a copy of the decommissioned EMR through to retaining the health information in a format which could be retrieved for the period of time specified by the CPSA policy.

[40] Dr. Myburgh advised me, on behalf of the custodians currently practicing at the FMC, that none of the health information in the Rise/Purkinje EMR has been retained. When the system was decommissioned, it was decommissioned in its entirety. The only information that was in the Rise/Purkinje EMR that currently exists in any format is the information that was migrated into the Med-Access EMR. The consequence of the decisions to engage in partial data migration and not retain an archive of the health information in the Rise/Purkinje EMR is that almost two years of health information on the patients of the FMC is incomplete and has been permanently lost.

[41] Dr. Myburgh states that the decision to engage in partial data migration was based on advice and direction they received from their new EMR vendor, Med-Access. Med-Access states that the advice they gave aligned with the specifications POSP had developed for the transfer and conversion of patient data. While I appreciate that the custodians relied upon the advice provided by others when contemplating data migration,

---

6 Sections 41(1), 41(1.1) and 42(1) of the HIA

7 Colleges of Physicians' and Surgeons of Alberta Policy on Physicians' Office Medical Records, revised August 2005. Accessed at http://uat-cpsa.softworksgroup.com/Libraries/Policies_and_Guidelines/Physicians_Office_Medical_Records.sflb.ashx on September 15, 2009.

the custodians ultimately remain accountable for the loss of health information in this case. It appears to me that the privacy and security risks associated with data migration were poorly understood by the custodians at the FMC. It is only during the course of this investigation that they became aware of the selective data migration process, and the fact that two years worth of their patients' health information has been permanently lost.

[42] In my opinion, the risk of loss of health information when migrating from one EMR to another is a threat that can be reasonably anticipated and that must be mitigated against under the HIA. The custodians at the FMC were required to take reasonable steps to protect the health information in their custody and under their control from loss during the data migration process. The decision to selectively migrate data without taking steps to preserve the health information that was not migrated renders the custodians unable to discharge their duty under the HIA to have maintained safeguards to protect health information against the reasonably anticipated threat of loss.

[43] I therefore find the custodians practicing at the FMC in contravention of section 60 of the HIA as it relates to their failure to retain the health information contained in a decommissioned EMR.

Recommendations

[44] I make the following recommendations to the custodians practicing at the FMC:

1. Review the policies and procedures provided in your privacy impact assessment and provide the Information and Privacy Commissioner with an implementation plan for audit log reviews within 30 days of the release of this report.
2. Consider whether or not to mask the Complainant's EMR record in its entirety to offer an additional level of privacy protection and advise the Complainant of your decision[8].

[45] Med-Access is the custodian's information manager and, under section 66(5) of the HIA is bound to follow the Act. As an information manager under the HIA, I make the following recommendations to Med-Access:

1. Provide Dr. Myburgh with a detailed description of the masking functionality available in their EMR solution, including a description of the resulting functional limitations when a mask has been applied.
2. Immediately train all staff on the availability of audit logs in secondary storage and the process through which a requesting custodian could obtain these logs.

[46] Dr. Myburgh and Med-Access have accepted these recommendations for immediate implementation.

Conclusion

[47] The Complainant alleged that a particular employee at his doctor's office looked at his medication profile in the EMR system and disclosed that information to his ex-wife. I

---

8 This recommendation, while peripheral to the Investigation Report, constitutes a method through which the Clinic can address the Complainant's privacy concerns on an ongoing basis. Masking the record would restrict the record from access from any staff member other than the user who created that particular entry unless the mask was overridden. The Complainant specifically requested this consideration during the investigation.

was unable to substantiate that allegation after a detailed review of the EMR audit logs and formal interview of the employee and physician. In the absence of evidence to the contrary, I found that no disclosure of health information took place.

[48] During the course of conducting this investigation, it came to my attention that a potentially significant amount of health information had not been migrated from the custodians' previous EMR system into the new EMR. This information has been permanently lost as the health information in the old EMR system has not been retained in any format. This is a serious contravention of the HIA, and places the physicians involved in potential contravention of other professional guidelines and standards of practice.

[49] The Office of the Information and Privacy Commissioner (OIPC) is aware that a significant number of physicians are facing the decommissioning of their EMR solutions within the next three years due to changes within the Physician Office System Program. We have been advised that these changes will involve selective data migration for many physicians. It is imperative that these legacy EMR systems be decommissioned in such a way as to retain the health information stored within them and preserve a physician's ability to meet legal challenges to his or her care.

[50] The obligation to address the risks associated with data migration rests on physicians, but they cannot effectively manage it without assistance from their EMR vendor and meaningful guidance from POSP. I have met with POSP throughout this investigation to discuss the general circumstances of this case and reinforce the emergent need for a comprehensive strategy that will assist custodians in managing the risks associated with EMR to EMR data migration. On October 13, 2009, POSP advised me that it is working towards development of a health information archiving solution. POSP anticipates that this solution will be finalized by December of this year and will include input from stakeholders including the College of Physicians and Surgeons and the OIPC. Pending the implementation of this strategy, POSP has stated that it will recommend that all physicians decommissioning EMR systems retain a full, read-only copy of the old EMR.

Submitted by

Leahann McElveen
Portfolio Officer, Health Information Act