



Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 124-2017 and 135-2017

Kelsey Trail Regional Health Authority Dr. A. Lawani

November 1, 2017

Summary:

A library book with records containing personal health information tucked into its pages was returned to the Nipawin Public Library. Kelsey Trail Regional Health Authority (Kelsey) retrieved the records and reported the matter to the Information and Privacy Commissioner (IPC). The IPC found that Dr. A. Lawani is the trustee responsible for the privacy breach. He made a number of recommendations including Kelsey implement a procedure so that it only discloses personal health information that is necessary for billing by physicians. He also recommended that Dr. A. Lawani establish policies and procedure on how to safeguard personal health information.

I BACKGROUND

- [1] A library book with records containing personal health information tucked into its pages was returned to the Nipawin Public Library. An employee at the library noticed the records and reported the matter to Nipawin Hospital of the Kelsey Trail Regional Health Authority (Kelsey). An employee from the hospital retrieved the records from the library.
- [2] Through its own investigation, Kelsey determined that it was Dr. A. Lawani who had borrowed and returned the book to the library. Kelsey reported this matter to my office.

II DISCUSSION OF THE ISSUES

1. Who is the trustee responsible?

[3] Both Kelsey and Dr. A. Lawani qualify as a trustee. Kelsey is a trustee as defined by subsection 2(t)(ii) of *The Health Information Protection Act* (HIPA). Dr. A. Lawani qualifies as a trustee as defined by subsection 2(t)(xiii) of HIPA. In order to determine which trustee is responsible for this particular privacy breach – that is, the unauthorized disclosure of the personal health information to the library - my office must determine who has custody or control over the records.

a. Was it a “use” or a “disclosure” when Kelsey provided a copy of the patient records to Dr. A. Lawani?

[4] The Operating Room Office at the Nipawin Hospital (which is a part of Kelsey) provided the copy of records to Dr. A. Lawani. Determining whether Kelsey’s provision of the patient records to Dr. A. Lawani is a “use” or a “disclosure” is important in finding which trustee has custody or control. If it is a “use”, then the records remain in the custody or control of Kelsey and Kelsey would be the trustee responsible for the privacy breach. If it is a “disclosure”, then the records are in the custody or control of Dr. A. Lawani and she would be the trustee responsible for the privacy breach.

[5] Subsection 2(u) defines “use” as follows:

2 In this Act:

...

(u) “use” includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[6] The definition of disclosure is when a trustee shares personal health information with an entity that is separate from itself. In other words, an entity that is not a division or branch of the trustee.

[7] Based on submissions by both Kelsey and Dr. A. Lawani's solicitor, Dr. A. Lawani is a surgical assistant at the Nipawin Hospital. Dr. A. Lawani is not an employee of Kelsey but she is a physician with practicing privileges within Kelsey. She received a copy of the records containing patient personal health information so she could bill the Ministry of Health for her services. This billing is not on behalf of Kelsey. In other words, when she bills the Ministry of Health, the Ministry of Health pays fees directly to Dr. A. Lawani. I find that Dr. A. Lawani is an entity separate from Kelsey for this purpose.

[8] Since Dr. A. Lawani is an entity separate from Kelsey, I find that Kelsey's provision of a copy of the patient records to Dr. A. Lawani for the purpose of billing is a disclosure. Dr. A. Lawani is the trustee with custody or control of the personal health information. Therefore, I find that Dr. A. Lawani is the trustee responsible for this privacy breach.

b. Is the disclosure by Kelsey authorized by HIPA?

[9] Subsection 27(2)(a) of HIPA provides as follows:

(2) A subject individual is deemed to consent to the disclosure of personal health information:

(a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;

[10] Kelsey collected the patients' personal health information for the purpose of delivering health services (in this case, surgeries) to patients. As mentioned earlier, Kelsey disclosed the personal health information to Dr. A. Lawani for the purpose of billing. Therefore, I must determine if billing is a purpose consistent with the original purpose.

[11] The province of Saskatchewan provides coverage for all medically necessary services provided by physicians. Physicians who provide such services will bill the Ministry of Health for payment. In this case, in order for Kelsey to deliver a medically necessary health service, such as surgery, it must have physicians conduct the surgery. In turn, the physicians bill the Ministry of Health. In order to facilitate billing, it is necessary for

Kelsey to disclose some of the patients' personal health information to physicians so that physicians can bill the Ministry of Health.

[12] Based on the above, physician billing is a purpose consistent with the delivery of medically necessary health service. I find that subsection 27(2)(a) of HIPA authorizes Kelsey to disclose the personal health information that is necessary for Dr. A. Lawani to bill the Ministry of Health. Dr. A. Lawani's solicitor noted that page 26 of the Ministry of Health's Physician Payment Schedule (October 1, 2017) requires physicians to submit the following information to bill:

- a. patient's name in full;
- b. patient's Health Services Number (HSN);
- c. patient's month and year of birth, and sex;
- d. location of service:
 - i. office
 - ii. hospital in-patient
 - iii. hospital out-patient
 - iv. home
 - v. other
- e. three-digit ICD diagnostic code;
- f. where service is provided in Saskatchewan, service code corresponding to procedure or treatment performed;
- g. where service is provided outside Saskatchewan, the service may be submitted to the physician's own provincial plan for direct reimbursement where such arrangements exist. For services received in Quebec, a description of the procedure or treatment provided;
- h. date of each service, except that, with respect to hospital visits, only the dates of the first and last visits and the total number of visits need be shown;
- i. amount charged for each service provided;
- j. additional remarks if nature of service was unusual;
- k. name and signature (not required if claim is submitted by computer) of person providing service;
- l. four-digit referring physician number where applicable.

[13] Therefore, subsection 27(2)(a) of HIPA authorizes the disclosure of the personal health information listed above for the purpose of billing, and not necessarily the entire patient record.

[14] In this case, Kelsey disclosed entire patient records. Dr. A. Lawani's solicitor indicated to my office that the entire patient record was disclosed because Dr. A. Lawani needed the patient records not only for billing but for assessment purposes to meet one of the

conditions of her Provisional with Restrictions License issued by the College of Physicians and Surgeons. The disclosure of personal health information for a purpose beyond that of billing is beyond the scope of this investigation. That is because Kelsey has identified that it discloses personal health information to Dr. A. Lawani for the purpose of billing. It is a separate matter if Dr. A. Lawani requires the entire patient record for assessment purposes. If Dr. A. Lawani requires copies of entire patient records for assessment purposes, she must make a request to Kelsey for a copy of the records and identify her authority for the collection of the personal health information. Then, before it discloses personal health information (such as the entire patient record), Kelsey must be sure of its authority under HIPA to do so.

c. Is the collection of personal health information by Dr. A. Lawani authorized by HIPA?

[15] The term “collect” is defined by subsection 2(b) of HIPA, which provides:

2 In this Act:

...

(b) “collect” means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;

[16] In this case, when Kelsey disclosed the patient records containing personal health information, Dr. A. Lawani collected the patients’ personal health information. Subsection 25(1)(f) of HIPA restricts the collection of personal health information by trustees to only certain circumstances. Subsection 25(1)(f) of HIPA provides:

25(1) Subject to subsection (2), a trustee shall collect personal health information directly from the subject individual, except where:

...

(f) the trustee collects the information by disclosure from another trustee pursuant to section 27, 28 or 29;

[17] As I found earlier, subsection 27(2)(a) of HIPA authorized Kelsey’s disclosure of some personal health information for the purpose of billing in this case. Therefore, I find that subsection 25(1)(f) of HIPA authorizes Dr. A. Lawani to collect some personal health information from Kelsey for the purpose of billing.

d. Was the data minimization principle observed?

[18] The data minimization principle provides that a trustee should collect, use, or disclose the least amount of identifying information necessary for the purpose. The data minimization principle is based on subsection 23(1) of HIPA, which provides:

23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.

[19] As noted earlier, the Ministry of Health's Physician Payment Schedule (October 1, 2017) lists the information that physicians must submit for billing.

[20] Kelsey provided my office with a copy of the records that were involved in the privacy breach. Based on a review of the records, it appears that Dr. A. Lawani received personal health information that was not necessary for billing.

[21] Kelsey disclosed more personal health information than was necessary for billing and Dr. A. Lawani collected more personal health information than was necessary for billing. I find that neither Kelsey nor Dr. A. Lawani complied with the data minimization principle. I recommend that Kelsey implement a procedure so that it only discloses to physicians the information necessary for billing. This may include creating a new form that records only the information necessary for billing instead of providing the physician with the patient record. I recommend that Dr. A. Lawani implement a procedure so she only collects the information necessary for billing.

2. Does Dr. A. Lawani have sufficient safeguards in place?

[22] Section 16 of HIPA requires that trustees establish safeguards to protect personal health information. It provides as follows:

16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

(a) protect the integrity, accuracy and confidentiality of the information;

- (b) protect against any reasonably anticipated:
 - (i) threat or hazard to the security or integrity of the information;
 - (ii) loss of the information; or
 - (iii) unauthorized access to or use, disclosure or modification of the information; and
- (c) otherwise ensure compliance with this Act by its employees.

[23] In order to bill the Ministry of Health for her services, according to her solicitor's submission, Dr. A. Lawani first collects paper records containing patient personal health information from Kelsey. Then, she provides them to a billing clerk who assists her with billing. The billing clerk then shreds the records.

[24] Dr. A. Lawani admitted she does not have any processes in place to safeguard personal health information. She kept records containing personal health information with other work-related documents and resources (which included the library book) until she provided the records to the billing clerk. She is now seeking a secure location within the Nipawin Hospital where she can store records containing personal health information. I find that this is a good first step in establishing appropriate safeguards. Further, Dr. A. Lawani's solicitor has indicated that Dr. A. Lawani is educating herself on privacy protection using resources made available by the Saskatchewan Medical Association (SMA) and the College of Physicians and Surgeons of Saskatchewan (CPSS). I find that this is another good step to take in ensuring she is complying with HIPA.

[25] I recommend that Dr. A. Lawani establish policies and procedures in the following areas:

- Establishing safeguards for secure storage of personal health information,
- Transporting records securely,
- Ensuring proper handling and management of the records by other parties (such as the billing clerk),
- Retention and disposition of records.

[26] Regarding the above, I suggest that as Dr. A. Lawani explores options for storage, she ensures there are appropriate safeguards to protect the personal health information. For example, SMA's reference manual recommends physicians have locked fireproof filing cabinets, restricting office access and alarm systems and protection from environmental

factors. It also says a good rule of thumb is to have three locks protecting personal health information, including a locked building, locked office, and locked filing cabinets.

[27] Also, I recommend that Dr. A. Lawani establish policies and procedures regarding the transportation and handling of patient records. For example, after she obtains records from Kelsey, she may have to physically transport them to the billing clerk. The records should be locked in a storage case (such as briefcase or a storage box) and also locked in the trunk of a vehicle. Unless there are no alternatives, the records should not be left unattended in the trunk while she is elsewhere.

[28] Further, I recommend that Dr. A. Lawani establish formal written agreements with parties assisting her with the billing process (such as the billing clerk) so that the other parties are managing the personal health information confidentially and appropriately.

[29] Finally, I recommend that Dr. A. Lawani establish policies and procedures that consider the retention and destruction of records. I note that the bylaws of CPSS address how long members should be retaining records. I recommend that Dr. A. Lawani consult with CPSS to see how long she must retain records containing the personal health information she needs to bill the Ministry of Health. Then, I recommend she establish a policy or procedure for the retention of records. This policy or procedure should also establish a process for destroying records as well. It should include the method in which records will be destroyed and how she will keep track of which records have been destroyed (to demonstrate records that were destroyed were retained for the full retention period prior to being destroyed).

3. What steps should Dr. A. Lawani take to respond to this privacy breach?

[30] My office suggests that trustees undertake the following five steps when responding to a privacy breach:

- Contain the breach,
- Notify the affected individuals,
- Investigate the breach,
- Prevent similar breaches,

- Write a privacy breach report.

[31] Below is an analysis of each of the above steps:

Containment

[32] To contain the breach is to ensure that personal health information is no longer at risk. This may include recovering the records, revoking access to personal health information, and stopping the unauthorized practice.

[33] The breach was contained when the Nipawin hospital employee retrieved the records from the Nipawin library. I find that this privacy breach has been contained.

Notification

[34] Notifying affected individuals of the privacy breach as soon as possible is important so individuals can determine how they have been impacted and take steps to protect themselves. In this case, the affected individuals have not been notified of this privacy breach yet because my office had to determine which trustee is responsible.

[35] As noted earlier, my office found that Dr. A. Lawani is the trustee responsible for this privacy breach. Dr. A. Lawani indicated she is willing to notify the affected individuals of this privacy breach. However, she does not know who the affected individuals are because she no longer has a copy of the records that were involved in this privacy breach. My office reviewed the records involved in this privacy breach but it does not contain the contact information of the affected individuals. Therefore, even if Dr. A. Lawani had a copy of the records, she would not be able to notify the affected individuals.

[36] I believe a coordinated approach between Kelsey and Dr. A. Lawani is required to notify the affected individuals. Since there are approximately 19 affected individuals, I recommend that Dr. A. Lawani prepare 19 letters notifying the affected individuals. The letters should include the following:

- A description of what happened,
- A detailed description of the personal health information that was involved,
- A description of possible types of harm that may come to them as a result of the privacy breach,
- Steps that the individuals can take to mitigate harm,
- Steps the trustee is taking to prevent similar privacy breaches in the future,
- The contact information of the trustee so she can answer questions and provide further information about the privacy breach,
- A notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner (IPC),
- Recognition of the impacts of the breach on affected individuals and an apology.

[37] Once the 19 letters are prepared, I recommend that Dr. A. Lawani request that Kelsey forward the notification letters to each of the affected individuals.

Investigate the privacy breach

[38] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar breaches in the future.

[39] As noted earlier, Dr. A. Lawani kept records containing personal health information with other work-related documents (which included the library book). This led to the records being tucked into the library book and Dr. A. Lawani made the mistake of returning the book without removing the records.

Prevent similar breaches

[40] Preventing future breaches means to implement measures to prevent similar breaches from occurring.

[41] As noted already, Dr. A. Lawani is seeking a more secure location within the Nipawin Hospital to store records containing personal health information and she is educating herself on privacy protection through resources by the SMA and CPSS.

[42] Further, I recommend that Dr. A. Lawani comply with the recommendations described in paragraphs [21], and [25] to [29] to minimize the likelihood of a similar privacy breach in the future.

Write a privacy breach report

[43] Documenting the privacy breach and the trustee's investigation into the matter is a method to ensure the trustee follows through with plans to prevent similar privacy breaches in the future.

[44] Dr. A. Lawani's solicitor documented the privacy breach in a letter dated July 20, 2017 to my office that includes what Dr. A. Lawani has done and will do to prevent a similar privacy breach in the future.

III FINDINGS

[45] I find that Kelsey's provision of a copy of the patient records to Dr. A. Lawani for the purpose of billing is a disclosure.

[46] I find that Dr. A. Lawani is the trustee responsible for this privacy breach.

[47] I find that subsection 27(2)(a) of HIPA authorizes Kelsey to disclose some personal health information to Dr. A. Lawani for the purpose of billing.

[48] I find that subsection 25(1)(f) of HIPA authorizes Dr. A. Lawani to collect some personal health information for the purpose of billing.

[49] I find that neither Kelsey nor Dr. A. Lawani complied with the data minimization principle.

[50] I find that Dr. A. Lawani does not have sufficient safeguards in place but she is taking steps to establish appropriate safeguards.

[51] I find that this privacy breach has been contained.

[52] I find that the affected individuals have not been notified yet.

[53] I find that Dr. A. Lawani has investigated the privacy breach.

[54] I find that Dr. A. Lawani is taking some appropriate steps to prevent a similar privacy breach in the future.

[55] I find that Dr. A. Lawani's solicitor has documented the privacy breach in a letter.

IV RECOMMENDATIONS

[56] I recommend that Kelsey implement a procedure so that it only discloses to physicians the information necessary for billing. This may include creating a new form that records only the information necessary for billing instead of providing the physician with the patient record.

[57] I recommend that Dr. A. Lawani implement a procedure so she only collects the information necessary for billing.

[58] I recommend that Dr. A. Lawani establish policies and procedures on the following areas:

- Establishing safeguards for secure storage of personal health information,
- Transporting records securely,
- Ensuring proper handling and management of the records by other parties (such as the billing clerk),
- Retention and disposition of records.

[59] I recommend that Kelsey and Dr. A. Lawani undertake the coordinated approach in notifying the affected individuals as described in paragraphs [36] and [37].

Dated at Regina, in the Province of Saskatchewan, this 1st day of November, 2017.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy
Commissioner