



## INVESTIGATION REPORT 071-2019

### Saskatchewan Health Authority

September 9, 2019

#### Summary:

A first aid and cardiopulmonary resuscitation (CPR) instructor was teaching a CPR re-certification class for St. John's Ambulance. This instructor was also a volunteer medical first responder with the Saskatchewan Health Authority (SHA). While teaching, the SHA issued an alert notifying its medical first responders to a cardiac arrest at a private home. The instructor brought the students in attendance at her class to the private home. A complaint was made to the Saskatchewan College of Paramedics (SCoP), who then reported this matter to the Information and Privacy Commissioner (IPC). The IPC found that a privacy breach occurred. A root cause of the breach was the medical first responder's disregard of expectations set out in a signed Memorandum of Understanding and Confidentiality Pledge with the SHA. The medical first responder also disregarded her professional responsibilities under the Code of Professional Conduct set out for licensed members of SCoP. He made a couple of recommendations including that the SHA treat volunteers the same as employees by requiring volunteers to take the mandatory privacy course.

#### I BACKGROUND

[1] On March 18, 2018, Saskatchewan Health Authority's (SHA) Regina Regional Communication Centre (RRCC) issued an alert notifying its medical first responders to a cardiac arrest at a private home.

[2] At the time of the call, a first aid and cardiopulmonary resuscitation (CPR) instructor was teaching a CPR re-certification class for St. John's Ambulance to three adult students. The instructor is also a volunteer with the SHA as a medical first responder and was registered as a non-practicing Emergency Medical Responder (EMR) with the Saskatchewan College

of Paramedics (SCoP). For the remainder of this Report, the instructor/medical first responder will be referred to as the Medical First Responder.

- [3] During the class noted above, the Medical First Responder received the call. According to SCoP's investigation report, the Medical First Responder indicated that her "immediate reaction was to take the students with her so they could experience the call and perhaps undertake CPR. She grabbed the [automated external defibrillator] and they left immediately".
- [4] My office was advised that the Medical First Responder and the three adult students arrived at the private home before other medical first responders and paramedics. The Medical First Responder, with the assistance of a student, moved the patient from the bed to the floor. However, it was determined that resuscitation was not possible. Soon after, two other medical first responders and two paramedics arrived on scene. A paramedic pronounced the patient dead at the scene.
- [5] The Professional Conduct Committee (PCC) at SCoP received a complaint regarding the Medical First Responder bringing the three adult students to the scene of a cardiac arrest. PCC investigated the complaint. The PCC found there is "sufficient evidence to believe that the incidents as alleged constitute professional misconduct as defined in section 25 of *The Paramedics Act*" and there is "sufficient evidence to find that the incidences establish a violation of the Code of Professional Conduct", which includes the expected standard of conduct to protect and maintain the patient's safety, dignity and privacy.
- [6] A Consensual Complaint Resolution Agreement was signed between the Medical First Responder and the PCC on December 13, 2018. In the Consensual Complaint Resolution Agreement, the Medical First Responder acknowledged that a privacy breach occurred and understood that this matter would be reported to my office. In a letter dated January 11, 2019, SCoP reported this matter to my office.
- [7] On March 6, 2019, my office notified SHA that it would be undertaking an investigation.

## II DISCUSSION OF THE ISSUES

### 1. **Is *The Health Information Protection Act* (HIPA) engaged and do I have the authority to investigate this matter?**

[8] HIPA is engaged when three elements are present: 1) personal health information, 2) a trustee, and 3) the trustee has custody or control over the personal health information. Below is an analysis to determine if these three elements are present.

#### Personal health information

2 In this Act:

...

(m) “personal health information” means, with respect to an individual, whether living or deceased:

- (i) information with respect to the physical or mental health of the individual;
- (ii) information with respect to any health service provided to the individual;
- (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- (iv) information that is collected:
  - (A) in the course of providing health services to the individual; or
  - (B) incidentally to the provision of health services to the individual; or
- (v) registration information;

[9] Information about the patient conveyed through the alert issued by the RRCC as well as information that may have been communicated or observed about the patient at the private home, including cardiac arrest and the pronouncement of the patient’s death, qualifies as personal health information as defined above.

#### Trustee

[10] Subsection 2(t)(ii) of HIPA defines “trustee” as follows:

2 In this Act:

...

(t) “trustee” means any of the following that have custody or control of personal health information:

...  
(ii) the provincial health authority or a health care organization;

[11] Based on subsection 2(t)(ii) of HIPA, I find that the SHA is a trustee.

Custody or control

[12] It should be noted that the SHA also qualifies as a “local authority” as defined by subsection 2(f)(xiii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), which provides:

2 In this Act:

...  
(f) “local authority” means:

...  
(xiii) the provincial health authority or an affiliate, as defined in *The Provincial Health Authority Act*;

[13] Subsection 2(b.1) of LA FOIP defines “employee” as follows:

2 In this Act:

...  
(b.1) “employee” means an individual employed by a local authority and includes an individual retained under a contract to perform services for the local authority;

[14] *Black’s Law Dictionary* (11<sup>th</sup> edition) defines “employ” as: “1. To make use of. 2. To hire. 3. To use as an agent or substitute in transacting business. 4. To commission and entrust with the performance of certain acts or functions or with the management of one’s affairs.”

[15] Further, *Black’s Law Dictionary* (11<sup>th</sup> edition) defines “contract” as “an agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law.”

[16] A Memorandum of Understanding (MOU) between the Medical First Responder and the former Regina Qu’Appelle Regional Health Authority (RQRHA) (which is now a part of the SHA) was signed on September 16, 2005. This MOU outlines the roles and responsibilities of the Medical First Responder, including providing medical aid within the

scope of the Medical First Responder's level of training. It also provides that medical first responders are to maintain strict patient confidentiality. The MOU provides:

It is the responsibility of all responders to maintain strict patient confidentiality. At no time will a patient's name or medical condition be communicated to any unauthorized person or member of the media. Any breach [sic] of patient confidentiality will result in the offending member or group being removed from their responsibilities as a First Responder.

[17] Furthermore, the MOU provides that a part of the role of the [name of Town] First Responders is that they are to respond at the direction of the RQRHA. This suggests that first responders are acting on behalf of the SHA:

[Name of Town] First Responders respond at the direction of the RQHR-EMS Communications Centre and provide medical aid within the scope of the responder's level of training.

[18] The MOU acts as an agreement, or a "contract", signed between the Medical First Responder and the former RQRHA. I find that the Medical First Responder qualifies as an "employee" of the SHA as defined by subsection 2(b.1) of LA FOIP. As an employee of the SHA, the Medical First Responder manages personal health information on behalf of the SHA. I find that the SHA has custody or control of the personal health information in this case.

[19] My office did not receive any information or evidence that suggests that any of the three students were employees of the SHA.

[20] I find that HIPA is engaged.

[21] I find that subsection 52(d) of HIPA provides my office with the authority to investigate this matter.

## **2. Did a privacy breach occur?**

[22] HIPA provides trustees with the authority to collect, use, and/or disclose personal health information in specific circumstances. A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA.

[23] The need-to-know principle is enshrined in section 23 of HIPA. Subsection 23(1) of HIPA provides as follows:

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.

[24] A disclosure occurs when personal health information is exposed to an entity or individuals separate from that of a trustee organization. In this case, the Medical First Responder disclosed the patient's personal health information to the three adult students by bringing the three students to the private home. The students saw and heard the patient's personal health information. The students, enrolled in a CPR recertification course at St. John's Ambulance, did not have a need-to-know the patient's personal health information. There was no authority for the Medical First Responder, or the SHA, to have disclosed the patient's personal health information to the three students. Accordingly, I find that a privacy breach occurred.

### **3. Has the SHA responded to the privacy breach appropriately?**

[25] My office suggests that the following five best practice steps be taken by a trustee organization when a privacy breach has occurred:

1. Contain the breach;
2. Notify affected individuals;
3. Investigate the breach;
4. Plan for prevention; and
5. Write an investigation report.

[26] Below is an analysis of these five steps.

#### ***Contain the breach***

- [27] Upon learning that a privacy breach has occurred, a trustee organization should immediately take steps to contain the breach. Depending on the nature of the breach, this can include stopping the unauthorized practice, recovering the records, shutting down the system that has been breached, revoking access privileges, or correcting weaknesses in physical security.
- [28] In this case, the SHA removed the Medical First Responder from the activation or call-out list four days after this incident. SHA will not be re-instating the Medical First Responder.
- [29] I should also note that according to the Consensual Complaint Resolution Agreement between the PCC and the Medical First Responder, the Medical First Responder agreed to not re-register as a medical first responder.
- [30] I find that the SHA has taken appropriate steps to contain the privacy breach.
- [31] Since the three adult students observed the patient's personal health information, I recommend that the SHA make efforts to contact the students and request that they not disclose the personal health information any further. This could include requesting St. John's Ambulance's assistance in contacting the students and relaying the request.

***Notify the affected individual***

- [32] Notifying an individual that their personal information or personal health information was involved in a privacy breach is important. This is so that the affected individual can take measures to protect themselves from potential harm resulting from the breach.
- [33] Since the affected individual is deceased, the SHA contacted the affected individual's family to notify them of the privacy breach. It should be noted that some members of the affected individual's family were present in the private home at the time of the privacy breach, so they were already aware of the privacy breach.

*Investigate the breach*

- [34] To investigate a privacy breach is to understand what happened that led to the privacy breach. As part of this investigation, the trustee organization should undertake a root cause analysis. Understanding the root causes will assist in the next step of managing a privacy breach, which is to implement a plan to prevent similar privacy breaches from occurring.
- [35] The former RQRHA established its expectation that the Medical First Responder would maintain patient confidentiality with the Medical First Responder through a MOU and through a Confidentiality Pledge.
- [36] First, as noted earlier, there is a MOU signed by the Medical First Responder and the former RQRHA. That MOU features a confidentiality clause that was quoted earlier.
- [37] Second, the Medical First Responder signed a RQRHA Confidentiality Pledge on October 20, 2004. This Confidentiality Pledge provides as follows:

The confidentiality of its client's personal health information is a key concern of the Regina Qu'Appelle Regional Health Authority (the "RQRHA") and accordingly the RQRHA has policies, procedures and practices in place to protect the confidentiality of its client's personal health information. One way to protect the confidentiality of personal health information is to require independent contractors and volunteers to sign a Confidentiality Pledge. Therefore, based on the above, I the undersigned agree as follows:

- (a) That I will only access personal health information on a need-to-know basis for performing services on behalf of the RQRHA;
- (b) That I will keep all personal health information in my possession in the strictest of confidence and only use such information for the purposes of performing services on behalf of the RQRHA;
- (c) That upon no longer requiring the personal health information for the purposes of providing services on behalf of the RQRHA, I will return or destroy all copies of the personal health information in my possession as instructed by RQRHA;
- (d) That I will follow all applicable RQRHA security and confidentiality policies, procedures and practices;



(e) I acknowledge that I have read this Confidentiality Pledge and understand that a breach of it may be in contravention of the *Health Information Protection Act* or other applicable laws.

[38] However, in spite of signing the MOU and the Confidentiality Pledge, the Medical First Responder still brought the three adult students to the private home.

[39] Furthermore, the Medical First Responder had a practicing and non-practicing EMR license with SCoP. In order to become licensed with SCoP, applicants must pass an exam. According to SCoP's website, a portion of this exam is on professional responsibility. Since the Medical First Responder was licensed, she would have been aware of the SCoP's Code of Professional Conduct, which includes the responsibility to protect and maintain the patient's safety, dignity and privacy. According to SCoP's investigation report, the Medical First Responder admitted she made a "huge mistake" and "knows that she broke her Code of Professional Conduct".

[40] Based on the information provided to my office by the SHA and SCoP, the Medical First Responder provided different reasons for why she brought the three adults students to the private home.

[41] According to SHA's investigation report, the Medical First Responder brought the three adult students because having a "rotation of trained individuals for CPR" could be beneficial to the patient. The SHA indicated that there is a practice of medical first responders requesting the assistance of private citizens already on scene in overwhelming circumstances. However, I note that the Medical First Responder deviated from this practice by bringing individuals to the scene rather than requesting the assistance of private citizens or family members already on scene.

[42] As well, the Medical First Responder had indicated to SCoP that she brought the students with her so the students could experience the call and perhaps undertake CPR. According to the Consensual Complaint Resolution Agreement signed by the Medical First Responder and the PCC, the Medical First Responder "brought the three students she was instructing with her to the scene of the cardiac arrest with the intent of allowing them to practice CPR

on a real human.” Further, the agreement also provides that the Medical First Responder told one of the paramedics that, “she was teaching a First Aid/CPR class when she got the call and thought there was no better opportunity for her three students than to attend the call and learn.”

- [43] Regardless of the reasons why the Medical First Responder brought the three adult students to the private home, the Medical First Responder’s actions are directly against the expectations set out in the MOU and the Confidentiality Pledge, as well as her professional responsibilities as a licensed member of SCoP. I find that a root cause of this privacy breach is the Medical First Responder’s disregard of the MOU, the Confidentiality Pledge, and the Code of Professional Conduct set out for licensed members of SCoP.

*Plan for prevention*

- [44] Prevention is perhaps the most important step in responding to a privacy breach. While a privacy breach cannot be undone, a trustee organization can learn from and improve its practices. To avoid future breaches, a trustee organization should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.
- [45] As noted earlier, the SHA indicated it will not be re-instating the Medical First Responder. I find that this is an appropriate step to take in preventing a similar privacy breach since a root cause of this privacy breach is the Medical First Responder’s disregard of the MOU, the Confidentiality Pledge, and the Code of Professional Conduct set out for licensed members of SCoP.
- [46] Further, in its investigation report, the SHA indicated it will be reviewing how to best support its medical first responders, including the requirements for requesting assistance and the parameters of including members of the public or other medical first responders from out of the area. Also, the SHA indicated that its mandatory privacy refresher courses are being rolled out starting in 2018 and 2019 for employees. In order to access the courses,

individuals need to enter an employee number. Therefore, as volunteers, medical first responders do not have access to the courses electronically. However, medical first responders are still able to access the privacy education video. Then, they are able to complete a paper version of the quiz and sign (or re-sign) the confidentiality statement. In the course of this investigation, the SHA indicated that it is training new volunteer staff and it is working to determine how to record the volunteer training within the SHA.

[47] I find that the SHA is taking appropriate steps in preventing a similar privacy breach from occurring.

[48] I recommend that the SHA treat volunteers the same as employees by requiring volunteers to take the mandatory privacy course. This will include continue working towards determining how to record volunteer training similar to how the SHA records employee training.

***Write an investigation report***

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

[50] SHA provided my office with its internal investigation report. I find that the SHA has sufficiently fulfilled this step in responding to a privacy breach.

[51] The purpose of information privacy laws, such as HIPA, is to protect patient privacy. In *R. v. Dymont*, [1988] 2 S.C.R. 417, La Forest J. stated:

Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual

that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the *Privacy Act*, S.C. 1980-81-82-83, c. 111.

- [52] Further, in that same decision, La Forest J. recognizes the vulnerability of patients and emphasizes physicians' ethical responsibility to maintain the confidentiality of information that physicians may derive from their patients:

The Task Force on Privacy and Computers, *supra*, pp. 23 et seq., like other similar studies, identified hospitals as one of the specific areas of concern in the protection of privacy. This is scarcely surprising. At one time, medical treatment generally took place in the home, or at the doctor's office, but even then, of course, **the confidentiality of the doctor-patient relationship was fully accepted as an important value in our society.** This goes back as far as the Hippocratic Oath. The Code of Ethics of the Canadian Medical Association sets forth, as item 6 of the ethical physician's responsibilities to his patient, that he "will keep in confidence information derived from his patient, or from a colleague, regarding a patient and divulge it only with the permission of the patient except when the law requires him to do so"; see T. D. Marshall, *The Physician and Canadian Law* (2nd ed. 1979), p. 14. **This is obviously necessary if one considers the vulnerability of the individual in such circumstances. He is forced to reveal information of a most intimate character and to permit invasions of his body if he is to protect his life or health.** Recent trends in health care exacerbate the problems relating to privacy in the medical context, particularly in light of the health-team approach in an institutional setting and modern health information systems. If the health-team approach gives a patient easy access to a wide range of medical services, it inevitably results in the fragmentation of the classical doctor-patient relationship among a team of medical and para-medical personnel. The dehumanization that can result has led some hospitals in the United States to appoint an ombudsman for patients.

[emphasis added]

- [53] From the standpoint that health care providers have an ethical responsibility to maintain patients' privacy, even outside of responsibilities under HIPA, and therefore maintain their dignity, I find this privacy breach to be seriously concerning. Even if I assume that the Medical First Responder had good intentions, her actions were reckless. She did not abide by the MOU or the Confidentiality Pledge that she signed, nor did she abide by SCoP's Code of Professional Conduct. Her actions compromised the patient's privacy and dignity. Further, especially for those who witnessed this privacy breach, trust in the health care

system may have been lost. If this is the case, it is my hope their trust can eventually be restored.

### **III FINDINGS**

[54] I find that HIPA is engaged.

[55] I find that a privacy breach occurred.

[56] I find that a root cause of this privacy breach is the Medical First Responder's disregard of the MOU, the Confidentiality Pledge, and the Code of Professional Conduct set out for licensed members of SCoP.

[57] I find that the SHA has responded to this privacy breach appropriately.

### **IV RECOMMENDATIONS**

[58] I recommend that the SHA make efforts to contact the students and request that they not disclose the personal health information any further as described in paragraph [32].

[59] I recommend that the SHA treat volunteers the same as employees by requiring volunteers to take the mandatory privacy course as described in paragraphs [47] to [49].

Dated at Regina, in the Province of Saskatchewan, this 9th day of September, 2019.

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