Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 245-2016

No Trustee

April 5, 2017

Summary: The Office Manager of Professional Sport Rehabilitation Corporation (Pro Sport) proactively reported a privacy breach involving a ransomware attack on its electronic medical record (EMR) database. The Commissioner found that Pro Sport did not qualify as a trustee for the purpose of *The Health Information Protection Act* (HIPA). He also found that the personal health information in question was in the custody and under the control of Pro Sport and therefore parts of HIPA did not apply. He recommended that Pro Sport follow privacy best practices even though it was not a trustee. He recommended that Pro Sport only collect health services numbers in accordance with section 11 of HIPA. The Commissioner also recommended that the Minister of Health amend HIPA to include professional and business corporations whose primary purpose is the provision of health services.

I BACKGROUND

[1] On October 12, 2016, the Office Manager of Professional Sport Rehabilitation Corporation (Pro Sport) called my office seeking advice on how to handle a privacy breach which involved a ransomware attack on its electronic medical record (EMR) database that occurred that day. The ransomware attack encrypted all data in its database. My office provided resources which outline steps and best practices for dealing with a privacy breach. My office also encouraged Pro Sport to proactively report the breach to my office.

[2] On October 26, 2016, Pro Sport proactively reported the breach to my office and provided an "Incident Report". On the same day, my office provided notification of our intention to undertake an investigation.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[3] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

[4] First I must determine whether personal health information was involved in this breach. Subsection 2(m) of HIPA defines personal health information as follows:

> **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;

[5] Pro Sport indicated that the following data items were affected by the ransomware attack: name, address, phone numbers, Saskatchewan health numbers, details of injuries and treatment plans. All of this data would qualify as personal health information as defined in subsection 2(m) of HIPA.

[6] Next, I must determine if there is a trustee as defined by subsection 2(t) of HIPA which provides:

> **2** In this Act:
> …
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (i) a government institution;
>
> (ii) a regional health authority or a health care organization;
> …
> (iv) a licensee as defined in *The Personal Care Homes Act*;
>
> (v) a person who operates a facility as defined in *The Mental Health Services Act*;
>
> (vi) a licensee as defined in *The Health Facilities Licensing Act*;
>
> (vi.1) a licensee as defined in *The Patient Choice Medical Imaging Act*;
>
> (vii) an operator as defined in *The Ambulance Act*;
>
> (viii) a licensee as defined in *The Medical Laboratory Licensing Act, 1994*;
>
> (ix) a proprietor as defined in *The Pharmacy and Pharmacy Disciplines Act*;
>
> (x) a community clinic:
>
> (A) as defined in section 263 of *The Co-operatives Act, 1996*;
> …
> (C) incorporated or continued pursuant to *The Non-profit Corporations Act, 1995*;
>
> (xi) the Saskatchewan Cancer Foundation;
>
> (xii) a person, other than an employee of a trustee, who is:

> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
>
> (B) a member of a class of persons designated as health professionals in the regulations;
>
> (xiii) a health professional body that regulates members of a health profession pursuant to an Act;
>
> (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;
>
> (xv) any other prescribed person, body or class of persons or bodies;

[7] Information Services Corporation lists Pro Sport as a Business Corporation. Pro Sport, as a Corporation, is not captured by the definition of trustee in subsection 2(t) of HIPA.

[8] There are two Directors/Officers of Pro Sport: one Physical Therapist licenced pursuant to *The Physical Therapists Act, 1998* and one Sports Therapist. These two individuals are shareholders of the Corporation, and neither is a majority shareholder.

[9] The Physical Therapist qualifies as a trustee pursuant to subsection 2(t)(xii)(A) of HIPA because he is a health professional that is licenced pursuant to an Act for which the Minister of Health is responsible.

[10] In past reports by my office, trustees who have had sole ownership of a corporation have been found to have had custody or control of the personal health information of the Corporation (see Investigation Report H-2011-001).

[11] I must determine whether the personal health information in question is in the custody or under the control of the Physical Therapist or the Corporation.

[12] Pro Sport has indicated that the equipment that physically holds the EMR is located on property leased by the Corporation. Therefore, I find that the Corporation has physical possession of the personal health information in question.

[13] I then must determine if the Physical Therapist, as a trustee, has any measure of control over the personal health information in question. Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. To establish control, custody is not a requirement.

[14] To make my determination, I have modified 15 criteria that my office has used to determine whether public bodies have control over records pursuant to *The Freedom of Information and Protection of Privacy Act* (FOIP) or *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). All 15 criteria do not have to be met in order to find that a trustee has a measure of control. They can be found in my office's resource *IPC Guide to HIPA.* Some of the criteria that are relevant in this case are as follows:

- The record was created by the trustee or a staff member of the trustee in the course of his or her duties performed for the trustee;
- The record is specified in a contract as being under the control of a trustee and there is no understanding or agreement that the records are not to be disclosed;
- The trustee has a right of possession of the record; and
- The trustee has the authority to regulate the record's use and disposition;

[15] Also, the guidance provided by the Saskatchewan Medical Association in its reference manual entitled *Privacy and Security Resource Materials for Saskatchewan EMR Physicians: Guidelines, Samples and Templates* is relevant for determining what control trustees may have over personal health information. It reframes the 15 criteria into a HIPA context.

1. Is the health professional collecting, using or disclosing personal health information as an employee of a trustee?
2. Is the health professional part of a group practice?

a. Does each health professional have his/her own EMR or a separate patient list within a common EMR?

b. Do employees, medical students and residents, work for just one health professional?

c. If the health professional were to leave the current location of practice could he/she take the records or a copy of them to a new practice location?

[16] In addition to being a director and a shareholder, the Physical Therapist is the President, Secretary and Treasurer of Pro Sport. The Sports Therapist is a director, shareholder and Vice President. They reported, however, that there are no job descriptions for the various roles. Practically, they share all responsibilities. In other words, the role of President, Secretary or Treasurer does not have a clear responsibility for the EMR.

[17] Pro Sport also reported that currently four other physical therapists, four massage therapists and two chiropractors are employed by or contract with the Corporation. None are employed by or contract specifically with the Physical Therapist.

[18] Less than 20 percent of the clients in Pro Sport's EMR have been seen by the Physical Therapist in question. Further, the EMR is organized so that any other Pro Sport employee can access the personal health information of the clients of the Physical Therapist and make additions, if coverage is needed.

[19] Finally, Pro Sport's Shareholder agreement prohibits any director or shareholder of the Corporation from "disclosing" "Confidential Information" such as "client lists" without the "express written consent of the Corporation". Further, this clause "shall survive the termination" of the agreement.

[20] With these factors in mind, I find that the Corporation has custody and control over the personal health information in question. The Physical Therapist, who qualifies as a trustee, does not have control of the personal health information. As a result, parts of HIPA do not apply to the personal health information affected by the breach.

[21] The fact that corporations that provide health services in Saskatchewan, such as Pro Sport, are not covered by the definition of trustee in HIPA is wrong. Many health professionals in our province choose to form a business or professional corporation for a variety of reasons. Depending on how these corporations are organized, a trustee may intentionally or unintentionally avoid the responsibilities imposed by HIPA. As a result, citizens do not have the same access and privacy rights and protections with respect to their personal health information.

[22] Further, an in-depth analysis was required to determine if HIPA applies in this case. Many citizens in Saskatchewan may not know if the personal health information entrusted to their health care provider is protected by HIPA.

[23] In my office's 2015-2016 Annual Report and in my office's Investigation Reports 183-2016, 186-2016 & 187-2016 and 292-2016, my office proposed to expand the definition of trustee to the following:

> (xv) a person who operates a facility whose primary purpose is the provision of health services provided by health professionals licensed or registered pursuant to an Act.

[24] I recommend that the Minister of Health make legislative changes to HIPA that broaden the definition of trustee to include business and professional corporations whose primary purpose is the provision of health services.

2. Should Pro Sport follow privacy best practices?

[25] Although I have determined that parts of HIPA do not apply, some of Pro Sport's clients may be under the impression their personal health information is protected by the Act. Therefore, it is important that Pro Sport follow best practices to protect the personal health information. Pro Sport has also acknowledged the importance of protecting personal health information. The following is a list of best practices that Pro Sport should consider following.

[26] It is possible that Pro Sport is subject to the federal private sector privacy legislation entitled the *Personal Information Protection and Electronic Documents Act* (PIPEDA). I recommend that Pro Sport determine if it is subject to this law and understand what responsibilities PIPEDA may impose.

[27] Section 11 of HIPA restricts the collection of the Saskatchewan health services number by non-trustees. It provides:

> 11(1) An individual has the right to refuse to produce his or her health services number or any other prescribed identifying number to any person, other than a trustee who is providing a health service, as a condition of receiving a service.
>
> (2) Except as provided in subsection (3), no person shall require an individual to produce a health services number as a condition of receiving any product or service.
>
> (3) A person may require the production of another person's health services number:
>
> (a) for purposes related to:
>
> (i) the provision of publicly funded health services to the other person;
>
> (ii) the provision of a health service or program by a trustee; or
>
> (b) where authorized to do so by an Act or regulation.

[28] I recommend that Pro Sport only collect health services numbers of clients where the service provided is publically funded. I also recommend that it create a plan to securely destroy all health services numbers in its custody that were not required to collect public funds from the EMR and its paper records.

[29] Through my investigation, I have also determined that the adoption of these best practices would benefit Pro Sport in dealing with the ransomware breach and preventing similar breaches:

- ensure all affected individuals are notified of the breach. If contact information is out-of-date, this can be achieved by placing advertisements in the local paper;
- create a comprehensive written privacy policy for its organization;

- Create a policy that restricts personal devices from accessing the database; and
- Revise and enforce record retention and destruction schedules.

3. What steps should other trustees take when disclosing personal health information to Pro Sport?

[30] Pro Sport reported that it sometimes collects personal health information directly from other trustees through, for example, referrals. In light of my finding that Pro Sport does not qualify as a trustee, section 21 of HIPA is relevant. It provides:

> 21 Where a trustee discloses personal health information to a person who is not a trustee, the trustee must:
>
> (a) take reasonable steps to verify the identity of the person to whom the information is disclosed; and
>
> (b) where the disclosure is made without the consent of the subject individual, take reasonable steps to ensure that the person to whom the information is disclosed is aware that the information must not be used or disclosed for any purpose other than the purpose for which it was disclosed unless otherwise authorized pursuant to this Act.

[31] Those trustees disclosing the personal health information to Pro Sport without the consent of the subject individual must take extra care and follow the steps provided by section 21 of HIPA. The trustees should contact Pro Sport prior to the disclosure to discuss the purpose for disclosure and restrictions for use.

III FINDINGS

[32] I find that Pro Sport does not qualify as a trustee pursuant to subsection 2(t) of HIPA.

[33] I find that the personal health information involved in the breach is in the custody and under the control of Pro Sport.

[34] I find that HIPA does not apply in these circumstances.

IV RECOMMENDATIONS

[35] I recommend that Pro Sport determine if it is subject to PIPEDA and understand the responsibilities it imposes.

[36] I recommend that Pro Sport only collect health services number of clients where the service provided is publically funded.

[37] I recommend that Pro Sport create a plan to securely destroy all health services numbers in its custody that were not required to collect public funds from the EMR and its paper records.

[38] I recommend that Pro Sport follow privacy best practices.

[39] I recommend that Pro Sport ensure that all affected individuals are notified of the ransomware breach.

[40] I recommend that Pro Sport create a comprehensive written privacy policy for its organization.

[41] I recommend that Pro Sport create a policy that restricts personal devices from accessing the database.

[42] I recommend that Pro Sport revise and enforce record retention and destruction schedules.

Dated at Regina, in the Province of Saskatchewan, this 5th day of April, 2017.

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