Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 022-2018

No Trustee

August 17, 2018

Summary: The Assiniboine Valley Health and Wellness Foundation Incorporated (AVHWF) proactively reported a privacy breach to the Information and Privacy Commissioner (IPC) when its electronic medical records (EMR) system had been infected with ransomware. Data was recovered from backups and it was able to rebuild its server for the EMR. The IPC found that *The Health Information Protection Act* (HIPA) does not apply in these circumstances. He recommended that the Minister of Health make legislative changes to HIPA that would broaden the definition of trustee to include organizations whose primary purpose is the provision of health services.

I BACKGROUND

[1] The Assiniboine Valley Health and Wellness Foundation Incorporated (AVHWF) is a non-profit corporation. It owns the Assiniboine Valley Medical Centre (Medical Centre). Within this Medical Centre is a medical clinic. The AVHWF facilities lease agreements with four physicians who practice medicine at the medical clinic.

[2] On January 9, 2018, AVHWF proactively reported a privacy breach to my office. It reported that its medical centre was closed from December 23, 2017 to January 1, 2018. Upon reopening on January 2, 2018, it discovered its computer system, which included its electronic medical records (EMR) system, was down because its server had been infected with ransomware. The firewall had been removed from the server, suggesting that the computer system had been successfully attacked. AVHWF's Information Technology (IT) service provider was able to recover data through backups and rebuild the server.

[3] On January 31, 2018, my office notified AVHWF that it would be undertaking an investigation.

[4] On February 21, 2018, my office received AVHWF's internal investigation report.

II DISCUSSION OF THE ISSUES

1. Is *The Health Information Protection Act* (HIPA) engaged?

[5] HIPA is engaged 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.

[6] First, I need to determine if there is personal health information involved in this incident. Subsection 2(m) of HIPA provides 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;

[7] The EMR system contains information about the patients. Therefore, I find that there is personal health information as defined by subsection 2(m) of HIPA.

[8] Second, I need to determine if there is a trustee as defined by subsection 2(t) of HIPA:

> 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) the provincial 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;

[9] AVHWF itself does not qualify as a trustee as defined above. However, the physicians who practice medicine at the medical clinic qualify as trustees pursuant to subsection 2(t)(xiii) of HIPA.

[10] Third, I need to determine if the physicians have custody or control over the personal health information.

[11] The facilities lease agreement between AVHWF and the physicians indicates that the EMR system is the property of AVWHF. It also says that while the physicians are responsible for the integrity and safety of all electronic files and data stored on the internal network, the files are not transferable from the property without written permission from the patient. This suggests that the physicians do not have control over the personal health information. For example, if one of the physicians left to work at another medical clinic, the patient record would remain at the AVWHF's medical clinic. Unless the patient provides written consent for AVWHF to transfer the record, then the record remains solely in AVWHF's custody and control.

[12] Therefore, the physicians (who are the trustees in this case) do not have custody or control over the personal health information. It is AVWHF, which is not the trustee in this case, that has custody and control. Therefore, I find that HIPA is not engaged in this case.

[13] In my office's Investigation Reports 183-2016, 186-2017, 187-2017, 292-2016, and 245-2016, my office proposed to expand the definition of "trustee" in HIPA 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.

[14] I recommend that the Minister of Health make legislative changes to HIPA that broaden the definition of trustee to include organizations whose primary purpose is the provision of health services.

2. Has AVWHF followed best practices?

[15] Although I have determined that HIPA does not apply in this case, patients who receive health services at the medical clinic may be under the impression that their personal health information is protected under HIPA.

[16] My office recommends that organizations undertake the following steps when responding to a potential privacy breach:

- Contain the breach,
- Notify affected individuals,
- Investigate the breach,
- Prevent similar breaches in the future,
- Write a privacy report.

[17] In this case, it appears that AVHWF undertook most of these steps. Its Information and Technology (IT) service provider detected the attack and was able to restore the data from backups and rebuild the server. It also retrieved the audit log for the EMR system to determine if the personal health information had been accessed in the attack. Based on the audit log, it does not appear that the electronic medical records system was accessed.

[18] I recommend that AVWHF investigate further to determine if personal health information was stored beyond the EMR system. For example, schedules of patient appointments in a calendar or billing information. If so, then such personal health information may have been accessed in the attack. If this is the case, I recommend that the AVWHF notify the affected individuals. If AVWHF is not able to identify who the affected individuals are, or if there is a large number of affected individuals, then I suggest that the AVWHF put up a notice of the privacy breach on its website. This notice should include the following:

- A description of what happened;

- A detailed description of the personal information or personal health information that was involved;
- If known, 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 organization is taking to prevent similar privacy breaches in the future;
- The contact information of an individual within the organization who can answer questions and provide further information; and
- Where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[19] The purpose of notifying affected individuals is to enable affected individuals to take steps to protect themselves from harm. For example, if billing information was accessed, then an example of harm is the misuse of individuals' health services number. One way for individuals to determine if their health services number has been misused is to request an audit report from eHealth Saskatchewan. This audit report will show who has accessed their personal health information in the Pharmaceutical Information Program (PIP), Picture Archiving Communications System (PACS), or the Electronic Health Record (eHR) Viewer. Instructions on how individuals may request access to their audit report is at this link: https://www.ehealthsask.ca/Pages/privacy-and-access.aspx. Individuals can use this audit report to determine if his or her personal health information is accurate. If it is inaccurate, this inaccuracy may indicate his or her personal health information has been misused. Individuals should take steps to correct their personal health information with the respective health care providers. Inaccuracies in personal health information can lead to misinformed decisions made by physicians. Or it can affect an individual's ability to qualify for insurance.

[20] Finally, it is possible that AVHWF's activity of operating a medical centre and leasing space to physicians to operate the medical clinic is subject to the federal private sector privacy legislation entitled the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Office of the Privacy Commissioner of Canada provides oversight for PIPEDA. I recommend that AVHWF determine if it is subject to PIPEDA. If it is, then it should determine its responsibilities under PIPEDA.

III FINDING

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

IV RECOMMENDATIONS

[22] I recommend that AVWHF investigate further to determine if personal health information was stored beyond the EMR system. If there was, I recommend that AVWHF provide notice to the affected individuals pursuant to paragraph [18].

[23] I recommend that AVHWF determine if it is subject to PIPEDA. If it is, then it should determine its responsibilities under PIPEDA.

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

Dated at Regina, in the Province of Saskatchewan, this 17th day of August, 2018.

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