Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 177-2018

Dr. Russom Ockbazghi and Dr. Warren N. Huber of Humboldt Clinic Limited

January 29, 2019

Summary: eHealth Saskatchewan (eHealth) detected that a physician at Humboldt Clinic Limited inappropriately accessed the personal health information of two individuals involved in a collision involving the Humboldt Broncos. eHealth proactively reported these privacy breaches to the Information and Privacy Commissioner (IPC). The IPC made a number of findings including that privacy breaches occurred when the physician accessed the personal health information of two individuals in the Electronic Health Record Viewer. The IPC made a number of recommendations including that the Humboldt Clinic Limited provide training to its employees and contractors on the need-to-know principle.

I BACKGROUND

[1] On April 6, 2018, a highway collision occurred involving the hockey team Humboldt Broncos which left 16 dead and 13 injured.

[2] On April 7, 2018, Dr. D accessed the personal health information of two individuals. For the first individual, the Viewer's audit log recorded 61 events in which Dr. D's accessed personal health information. For the second individual, the Viewer's audit log recorded eight events.

[3] From April 8, 2018 to April 10, 2018, Dr. D continued to access the personal health information of one of the individuals. On April 8, 2018, the Viewer's audit log recorded 15 events. On April 9, 2018, the Viewer's audit log recorded 25 events. Finally, on April 10, 2018, the Viewer's audit log recorded 13 events.

[4] eHealth followed up with both Humboldt Clinic and Dr. D. regarding the accesses. Dr. D explained to eHealth that there is a delay in the personal health information appearing in Humboldt Clinic's electronic medical record (EMR). Therefore, he was not able to access the personal health information through Humboldt Clinic's EMR right away. As such, he gained access to the personal health information through the Viewer.

[5] eHealth determined that Dr. D accessed personal health information without a legitimate need-to-know under *The Health Information Protection Act* (HIPA). Therefore, eHealth reported the accesses to my office.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply to this matter?

[6] HIPA is engaged when three elements are present: 1) personal health information, 2) trustee, and 3) the trustee has custody or control over the personal health information.

[7] First, 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;

[8] I find that information in the Viewer would qualify as personal health information as defined above.

[9] Second, Humboldt Clinic is a business corporation and is not captured by the definition of "trustee" in subsection 2(t) of HIPA. However, according to the Information Services Corporation's Corporate Registry, the shareholders are two medical professional corporations, Dr. Russom Ockbazghi Medical Prof. Corp. and Dr.Warren N. Huber Medical P.C. Inc. The shareholders of each of those two medical professional corporations include health professionals licensed pursuant to *The Medical Profession Act, 1981* – Dr. Russom Ockbazghi and Dr. Warren N. Huber. Subsection 2(t)(xii) 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:
>
> ...
>
> (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;

[10] I find that Dr. Russom Ockbazghi and Dr. Warren N. Huber are the trustees in this case.

[11] Third, when an employee or contractor at Humboldt Clinic views personal health information from the Viewer, that view is a collection of personal health information. Further, the contract between Humboldt Clinic and Dr. D provides that Dr. D is not to remove patient records from the Clinic except with the express written consent of the Clinic. It provides:

> 7.2 The Doctor agrees that patient records shall not be removed from the Clinic except with the express written consent of the Clinic.

[12] Therefore, based on the above, I find that the trustees in this case have custody and control over the personal health information.

[13] I find that HIPA is engaged.

2. Did privacy breaches occur when Dr. D viewed personal health information in the Viewer?

[14] A privacy breach occurs when personal health information is collected, used, and/or disclosed without authority under HIPA.

[15] The need-to-know principle is the principle that trustees and their staff should only collect, use, or disclose information necessary for the diagnosis, treatment or care of an individual or other purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 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.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
> …
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[16] Further, section 24 of HIPA restricts the collection of personal health information by trustees. It provides:

> 24(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.

> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[17] In this case, Humboldt Clinic indicated that the two individuals were Dr. D's patients. Dr. D attended to one of the patients 13 times from August 22, 2016 to January 18, 2018. Dr. D attended to the other patient nine times from September 2, 2014 to January 18, 2018.

[18] For one of the individuals, Humboldt Clinic explained to eHealth that Dr. D wanted to know what injuries the individual sustained, if the individual received care, or if it was an instant fatality. For the other individual, Humboldt Clinic explained to eHealth that Dr. D was concerned. Based on these explanations, Dr. D did not have a need-to-know. There must be a trigger, such as a request for service or a requirement of the patient for care by Dr. D in order for Dr D to access patient information. Neither individuals requested nor required care from Dr. D as both were deceased.

[19] The above reasons are not in accordance with sections 23 or 24 of HIPA. I find that privacy breaches occurred when Dr. D looked up the two individuals' personal health information in the Viewer.

3. Did Humboldt Clinic properly respond to the privacy breaches?

[20] If a privacy breach has occurred, my office recommends five best practice steps. These are:

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

[21] Below is an analysis of each step.

Step 1: Contain the breach

[22] The first step to responding to a privacy breach is to contain the breach. In this case, to contain the privacy breach was to either suspend or terminate the employee's access to the Viewer.

[23] eHealth is the trustee for the Viewer so eHealth took steps to contain the breach. See Investigation Report 161-2018 on eHealth for more information.

Step 2: Notify affected individuals

[24] The second step to responding to a privacy breach is notifying the affected individuals that their personal health information was inappropriately accessed. This is important so that they can take appropriate steps to protect themselves from any potential harm. Unless there is a compelling reason not to do so, trustees should always be notifying affected individuals. An effective notification 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 organization are 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;
- A notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[25] In this case, eHealth notified the affected individuals or the next-of-kin. See Investigation Report 161-2018 on eHealth for more information.

Step 3: Investigate the privacy breach

[26] The third step to responding to a privacy breach is to investigate. Trustees should investigate to understand what happened and to identify the root cause of the privacy

breach. An investigation will assist trustees in developing and implementing measures to minimize or prevent similar privacy breaches in the future.

[27] In a letter dated October 30, 2018, Humboldt Clinic informed my office that it did not undertake an investigation into the matter. Therefore, it did not identify the root cause of the privacy breach.

Step 4: Plan for prevention

[28] Prevention is perhaps the most important step in a trustee's response to a privacy breach. Trustees should learn from the privacy breach and improve its practices in order to avoid similar privacy breaches in the future.

[29] As noted above, Humboldt Clinic did not conduct an investigation into this matter. Without an investigation to understand what happened, it would be difficult to implement an effective plan for prevention.

[30] It did, however, describe the privacy training it provides to its physicians. First, when employees are first hired, they are required to read Humboldt Clinic's *Privacy and Security Policy and Procedure Manual*, which consists of the following:

- Privacy Policy, Effective Date April 1, 2016
- Security Policy, Effective Date April 1, 2016
- Patient Access Rights Policy, Effective Date April 1, 2016
- Patient Access Rights Procedure, Effective Date April 1, 2016
- Procedure for Responding to a Privacy Breach or Incident, Effective Date August 17, 2011
- Destruction or Disposal of Records or Devices Containing PHI, Effective Date June 14, 2011
- Procedure for Masking Electronic Medical Records, Effective Date July 8, 2011
- Monitoring Audit Logs, Effective Date April 1, 2016
- Procedure for Continuing Clinic Operations in the Event of EMR Failure/Disaster Recovery, Effective Date February 1, 2017

[31] Then, employees are required to sign a confidentiality pledge.

[32] In terms of training on how to use the Viewer, users at the clinic have completed eHealth's online training sessions, which includes the following:

- Introduction to the eHR Viewer,
- Privacy and Security of the eHR Viewer,
- Understanding Laboratory Results in the eHR Viewer,
- Medication Information in the eHR Viewer,
- Immunization Information in the eHR Viewer,
- Discharge Summaries in the eHR Viewer,
- Viewing Chronic Disease Management Information in the eHR Viewer,
- Filtering for Specific Laboratory Results in the eHR Viewer,
- Viewing Cumulative Results in the eHR Viewer, and
- Understanding and Viewing Clinical Encounters in the eHR Viewer.

[33] Humboldt Clinic provided my office with Dr. D's certificates of completion for each of the above training sessions.

[34] Finally, Humboldt Clinic explained that any further training or updates are dealt with at staff meetings.

[35] While it is good that Humboldt Clinic has policies, procedures, and training as detailed above, it is evident that that they are not always being followed. For example, its Privacy Policy emphasizes the need-to-know principle. It provides as follows:

1. Our staff collects, uses, and accesses and discloses personal health information only for the purpose of providing, continuing or supporting the provision of health care. The use, access or disclosure of patient information for any other purpose is not undertaken by our staff without the express consent of the patient, or unless such use has been authorized by law.

2. All staff members in our Medical Practice fully protect the confidentiality of the information and the privacy of the individuals to whom the information pertains to by collecting, using, accessing or disclosing the minimal amount of information required and only on a need-to-basis.

[36] Dr. D accessed the personal health information in the Viewer because he was concerned. Being concerned does not mean he is providing, continuing or supporting the provision of health care, nor does it mean he has a need-to-know the personal health information.

[37] I find that Humboldt Clinic has the tools to prevent a similar privacy breach in the future. I recommend that it provide training to its employees and contractors on the need-to-know principle. Further, I recommend that it regularly remind employees and contractors of the need-to-know principle in its staff meetings.

Step 5: Write an investigation report

[38] The fifth step to responding to a privacy breach is writing an investigation report. Trustees should document their investigation, the root causes they have identified, and their plan for prevention. This is to ensure that trustees follow through with their plans to prevent similar breaches in the future.

[39] Humboldt Clinic did not conduct an investigation into this matter so it did not complete this fifth and final step of responding to a privacy breach. I recommend that it document privacy breaches, the lessons it has learned, and the steps it will take to prevent similar privacy breaches in the future.

III FINDINGS

[40] I find that HIPA is engaged.

[41] I find that privacy breaches occurred when Dr. D looked up the two individuals' personal health information in the Viewer.

[42] I find that Humboldt Clinic did not investigate this privacy breach.

[43] I find that Humboldt Clinic has the tools to prevent a similar privacy breach in the future.

[44] I find that Humboldt Clinic did not write a privacy breach report.

IV RECOMMENDATIONS

[45] I recommend that Humboldt Clinic provide training to its employees and contractors on the need-to-know principle.

[46] I recommend that Humboldt Clinic regularly remind employees and contractors of the need-to-know principle in its staff meetings.

[47] I recommend that Humboldt Clinic document privacy breaches, the lessons it has learned, and the steps it will take to prevent similar privacy breaches in the future.

Dated at Regina, in the Province of Saskatchewan, this 29th day of January, 2019.

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