Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 162-2018

Dr. Falah Majid Medical P.C. Inc.

January 29, 2019

Summary: eHealth Saskatchewan (eHealth) detected that an employee at the Dr. Falah Majid Medical P.C. Inc. (Clinic) inappropriately accessed the personal health information of three individuals involved in a collision involving the Humboldt Broncos. eHealth proactively reported these privacy breaches to the Information and Privacy Commissioner (the IPC). The IPC made a number of findings including how the lack of privacy training is the root cause of the privacy breaches. The IPC made a number of recommendations including that the Clinic appoint one of its employees to be its Privacy Officer, and that privacy policies and procedures be established.

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 9, 2018, eHealth Saskatchewan (eHealth) proactively added the individuals involved in the collision to its watch list. This means that whenever the individual's profile in the Electronic Health Record Viewer (the Viewer) was accessed, an email notification is sent to eHealth's Privacy, Access and Patient Safety Unit.

[3] Also on April 9, 2018, an employee, S, at the Dr. Falah Majid Medical P.C. Inc. (the Clinic) accessed the personal health information of two individuals involved in the collision using the Viewer.

[4] On April 17, 2018, eHealth proactively masked the Viewer profiles of the deceased individuals. When a profile is masked, then a user of the Viewer can only view the profile in limited circumstances. On that same day, the employee viewed a third individual's personal health information using the Viewer. This particular individual was deceased. Therefore, she was unable to view any information other than demographic information because the individual's profile was masked.

[5] eHealth detected and investigated the accesses. It determined that the employee did not have a legitimate need-to-know. eHealth reported the accesses to my office. Through eHealth's investigation, the employee also admitted to looking up her own personal health information in the Viewer.

[6] It should be noted that this employee is no longer working at the Clinic.

II DISCUSSION OF THE ISSUES

1. Does *The Health Information Protection Act* (HIPA) apply to this matter?

[7] 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.

[8] 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;

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

[10] Second, the Dr. Falah Majid Medical P.C. Inc. as a business corporation 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 one shareholder of Dr. Falah Majid Medical P.C. Inc. is Dr. Falah Majid He is a health professional licensed pursuant to *The Medical Profession Act, 1981*. Subsection 2(t)(xii) of HIPA defines a 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;

[11] I find that Dr. Falah Majid is the trustee in this case.

[12] Third, when an employee at the Dr. Falah Majid Medical P.C. Inc. views personal health information from the Viewer, that view is a collection of personal health information. Therefore, I find that Dr. Falah Majid, as the single shareholder of the Dr. Falah Majid Medical P.C. Inc., has custody over the personal health information.

[13] Based on the above, I find that HIPA is engaged.

2. Did privacy breaches occur when the employee 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 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, the employee admitted she looked up the three individuals' personal health information for the following reasons:

- her family members had heard one of the individuals had died and she wanted to verify the information,
- she thought another individual was a patient at the Clinic so she looked up the individual, and
- she wanted to verify a detail that was reported by the media about one of the individuals.

[18] The three above reasons are not in accordance with sections 23 or 24 of HIPA.

[19] Further, in her correspondence with eHealth, the employee admitted she looked up her own personal health information in the Viewer. While the employee has a right to request her own personal health information, she should only be accessing her own personal health information through the same channels as other individuals. Her user privileges in accessing the Viewer is to perform her job duties and is not a perk to be used for her own convenience. In Investigation Report 308-2017, 309-2017, 310-2017, my office explained the consequences of snooping:

> [60] Accessing information stored within the eHR Viewer for reasons beyond performing job duties is inappropriate. If legitimate users of the eHR Viewer were permitted to access any person's personal health information without a need-to-know, then patients' trust in the confidentiality of their personal health information would be undermined. The consequences include individuals avoiding seeking treatment or care, or they may be compelled to withhold or falsify information. Upholding patients' trust means upholding the integrity of the health care system.
>
> [61] Users of the eHR Viewer should not regard their access privileges as a perk to satisfy their own curiosity, to meet their own personal needs, or as a benefit or convenience to family, friends, and/or colleagues. Users of the eHR Viewer must still submit a formal access to information request pursuant to Part V of HIPA if they wish to receive access to personal health information – which is a right afforded to all Saskatchewan citizens under HIPA. Users of the eHR Viewer are not the winners of a two-tiered system where they can help themselves to any personal health information while others have to undertake the task of submitting a formal access to information request under HIPA to gain access to personal health information.

[20] I find that privacy breaches occurred when the employee looked up the three individuals' and her own personal health information in the Viewer.

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

[21] 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.

[22] Below is an analysis of each step.

Step 1: Contain the breach

[23] 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.

[24] 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

[25] 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.

[26] 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

[27] 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.

[28] As already noted in the background, the employee accessed the three individuals' and her own Viewer profiles for curiosity reasons rather than on a need-to-know basis. Based on the information provided to my office, the Clinic does not have any privacy training materials or a privacy manual for its employees. Therefore, employees are not trained on how they are to manage personal health information in such a way that is compliant with HIPA.

[29] After eHealth had detected the privacy breaches and contacted the Clinic the employee had indicated that as a result of eHealth's audit, she read "eHealth's privacy policy" and is "now fully aware of what is not acceptable". This suggests she had not received any privacy training prior to being provided access to the Viewer.

[30] Based on the above, I find that the lack of privacy training to be a root cause of the privacy breaches.

Step 4: Plan for prevention

[31] 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.

[32] As noted above, the lack of privacy training is a root cause of the privacy breaches.

[33] The Clinic indicated to my office that someone from the Saskatchewan Medical Association (SMA) had come to its office to provide training on August 9, 2018. The training covered the need-to-know principle. I find this to be an appropriate first step in preventing similar privacy breaches.

[34] I recommend that the Clinic appoint one employee to be its Privacy Officer.

[35] I recommend that this Privacy Officer establish policies and procedures for the Clinic. The Privacy Officer should contact the SMA for assistance. The SMA has resources available on its website to assist physicians and their staff to develop policies and procedures to manage personal health information in accordance with HIPA.

[36] Further, I recommend that Dr. Falah Majid and his employees:

- review eHealth's Privacy and Security of the eHR Viewer privacy and security training video annually, and
- a notation should be made on each employees' personnel file that date and time in which the employee viewed, understands, and agrees with the training video.

Step 5: Write an investigation report

[37] 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.

[38] The Clinic did not provide my office with any evidence that showed it wrote an investigation report. I find that it did not complete this step of responding to a privacy breach. I recommend that it document these privacy breaches, the lessons it has learned, and the steps it will take to prevent similar privacy breaches in the future.

III FINDINGS

[39] I find that HIPA is engaged.

[40] I find that privacy breaches occurred when the employee, S, looked up the three individuals' and her own personal health information in the Viewer.

[41] I find that the lack of privacy training to be a root cause of the privacy breaches.

[42] I find that the Clinic receiving privacy training from the SMA to be an appropriate first step in preventing similar privacy breaches in the future.

[43] I find that the Clinic did not write a privacy breach investigation report.

IV RECOMMENDATIONS

[44] I recommend that the Clinic appoint one employee to be its Privacy Officer.

[45] I recommend that Dr. Falah Majid and the Privacy Officer establish privacy policies and procedures for the Clinic.

[46] I recommend that Dr. Falah Majid and his employees:

- review eHealth's Privacy and Security of the eHR Viewer privacy and security training video annually, and
- a notation should be made on each employees' personnel file that date and time in which the employee viewed, understands, and agrees with the training video.

[47] I recommend that Dr. Falah Majid document the privacy breaches discussed in this report, the lessons learned, and the steps that will be taken 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