Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 162-2023

Dr. Bonnie Richardson
(Queen City Medical Specialists)

January 8, 2024

Summary: Dr. Richardson of Queen City Medical Specialists (QCMS), proactively reported to my office that a privacy breach had occurred when a physician at their clinic, viewed the patient records of another physician without an apparent need to do so. Dr. Richardson requested that the Commissioner investigate. The Commissioner found that Dr. Richardson who is a physician and owns the clinic (QCMS) is the trustee in this matter. The Commissioner agreed with the trustee, and found that a privacy breach occurred. The Commissioner also found that the trustee managed the privacy breach appropriately. The Commissioner recommended that in the future, the trustee include more details in the notification letters and that the trustee implement a schedule of proactive system audits, if it has not already done so.

I BACKGROUND

[1] On July 5, 2023, Dr. Richardson of Queen City Medical Specialists (QCMS), proactively reported a privacy breach to my office. Dr. Richardson explained that on March 13, 2023, that a physician [Physician X] at QCMS viewed their patient records without a need to do so.

[2] On August 15, 2023, my office notified Dr. Richardson that my office would be undertaking an investigation. At this time, my office also requested a copy of Dr. Richardson's internal investigation report.

[3] On November 20, 2023, Dr. Richardson provided their completed Privacy Breach Questionnaire (Questionnaire) to my office, along with supporting documentation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[4] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) there is a trustee; 2) there is personal health information; and 3) the personal health information is in the custody or control of the trustee.

[5] First, subsection 2(1)(t)(xii)(A) of HIPA defines a "trustee" as follows:

> **2**(1) 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; or

[6] Dr. Richardson is the sole director, officer and shareholder of "Richardson Duffy Holdings Ltd.," which owns the business named "Queen City Medical Specialists – 11th Avenue" (QCMS)." Dr. Richardson is a licensed physician, sole owner of their business and provided evidence to my office, that they hold the medical corporation permit for 2024, from the College of Physicians and Surgeons of Saskatchewan (CPSS). As such, Dr. Richardson is a trustee pursuant to subsection 2(1)(t)(xii)(A) of HIPA. In this Investigation Report, I will use the term "trustee" for Dr. Richardson, where applicable.

[7] Second, I need to consider if personal health information is involved. The trustee indicated that Physician X viewed charts of their patients. The trustee also provided my office with

copies of these four patients' referrals to explain that the trustee was their assigned doctor. The trustee explained their working relationship with Physician X as follows:

> …[Physician X] is not an employee of the clinic. [Physician X] is an independent contractor who at the time rented space in the QCMS clinic. [Physician X] has [their] own EMR/Accuro log in. Every physician in the clinic has their own EMR with independent password…

[8] My office noted that the medical charts of these four affected patients included each patient's first and last name, date of birth, health services number (HSN), address, medical history, diagnosis/ medical problem, medication list, family history, known allergies and lifestyle notes. This information would qualify as personal health information as defined by subsections 2(1)(m)(i), (ii), (iii), (iv) (A), (B) and (v) of HIPA as follows:

> **2**(1) 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] As such, there is personal health information involved in this incident.

[10] Third, the breach occurred when Physician X viewed charts of Dr. Richardson's patients on Accuro. The trustee provided a copy of a receipt showing an Accuro payment and confirmed that they paid for their Accuro login and Physician X paid for their own.

However, the trustee also provided a copy of their rental agreement with Physician X, that confirmed that the cost for the computer server that held all the patients' records and personal health information, was paid for by the trustee. As such, the personal health information was in the custody and under the control of the trustee.

[11] As all three elements are present, I find that HIPA is engaged and that I have jurisdiction to undertake this investigation.

2. Did a privacy breach occur?

[12] I first need to determine that a privacy breach occurred.

[13] As explained in paragraph [7], the trustee provided my office with copies of these four patients' referrals and medical charts to explain that they were the assigned doctor. My office noted that these medical charts included each patients' first and last name, date of birth, health services number (HSN), address, medical history, diagnosis/ medical problem, medication list, family history, known allergies and lifestyle notes. As explained above, this information would qualify as personal health information as defined by subsections 2(1)(m)(i), (ii), (iii), (iv) (A), (B) and (v) of HIPA.

[14] The trustee explained that on March 23, 2023, the clinic's privacy officer/office manager was notified by a medical office assistant (MOA) that Physician X was noted to have accessed a patient's medical chart on March 13, 2023, without an apparent need-to-know. The privacy officer then, with the assistance of the Electronic Medical Record (EMR) vendor (Accuro), conducted an audit, which revealed that several questionable accesses were made using Physician X's credentials. The trustee further explained as follows:

> … [Physician X] is an independent physician contractor with [their] own EMR [login]. [They] had no reason to access the personal health information of the patients [they] did. There was no phone call, coverage, request, lab or erroneous document or fax that would have prompted [them] to enter the charts. The snooping occurred remotely and after hours. [They] intentionally changed the physician profile to Dr. Richardson from [Physician X] to snoop through [their] patient records… There was no reason to enter those charts. Furthermore, [they] did not report accessing the charts. When the breach

> was discovered [they] denied then blamed the office manager for "framing [them]" and gave various insufficient information on [their] intentions.
>
> [Physician X] was encouraged to self-report the breach. [Physician X] is no longer working at QCMS. The breach was referred to [their] regulating body – CPSS [College of Physicians and Surgeons of Saskatchewan] for investigation and follow up. I would ask you follow up with CPSS…

[15] The trustee also provided a copy of their email exchange regarding the audit conducted by their Accuro service provider. This email included explanation from the Accuro representative as below:

> … I then created an Audit log search for all [sic] March 1 2023 to present (March 27 2023) For the provider [Physician X] and the activity "View Medical Summary". I then compared the list of patients created by the Audit log with the list of patients Dr. Richardson saw in March. I was looking for where the patients overlapped. I was able to find 4 total results, Patient [1] whom we were already aware of and 3 others. Please see some interesting details below
>
> - Patient [1] – Appointment with Dr. Richardson on March 7 2023 – Viewed by [Physician X's initial] on March 13 at 6.28 PM
> - Patient [2] – Appointment with Dr. Richardson on March 7 2023 – Viewed by [Physician X's initial] on March 13 at 6:26 PM
> - Patient [3] – Appointment with Dr. Richardson on March 7 2023 – viewed by [Physician X's initial] on March 13 at 6:23PM
> - Patient [4] - Appointment with Dr. Richardson on March 7 2023 – viewed by [Physician X's initial] on March 13 at 6:25PM
>
> I repeated the above workflow for February and January 2023 but was unable to find any more instances of [Physician X's initial] looking at Dr. Richardson's [sic] patients…

[16] The trustee also provided a copy of the complaint letter they filed with the CPSS on July 5, 2023 to my office. In this complaint letter, they outlined some of the following:

- Physician X has never had anything to do with the patients whose records were accessed.
- Physician X implies that [their] password was changed.

- No office staff can change a password.
- Passwords are only known to the Accuro account holder.
- If a person unsuccessfully logs in 3 times the admin can hit "reset" meaning you can attempt to log in with your own password. Only the Accuro user can change their password.
- An Accuro audit has been performed. Physician X's password was not "rested" ["reset"] as alleged.
- In order to log into the server remotely a person must use their mobile phone and use a "Tru-Grid"/authenticator program that requires the user to enter a random number code that changes every 30 seconds.
- Accuro logs Physician X logging in remotely and changing password at 09:19am on March 13, 2023.
- Accuro logs Physician X logging in remotely from home and looking at the charts in question, between 6:23pm – 6:25pm on March 13, 2023.
- That CPSS investigate the matter and take disciplinary action against Physician X.

[17] The trustee explained that when they discovered the privacy breach in Accuro, they contacted Physician X to understand if they had authority or a need-to-know their patients' medical charts. Physician X denied that they accessed the patients' charts and stated that probably someone in their office had viewed them. I note that the evidence supports that Physician X (or someone using their credentials) had logged in remotely, and would have needed to do so using their mobile phone and an authenticator app. If someone had done as Physician X has suggested, then Physician X would still have been responsible for the accesses made.

[18] At the time of writing this Investigation Report, my office contacted CPSS to determine if it had conducted its investigation and any resulting recommendations. CPSS explained that it has its internal processes and that if it found enough evidence to warrant an investigation, then it would initiate forming an investigation committee and the process could take three to nine months.

[19] It appears, then, that Physician X (or someone else, as they apparently alleged) accessed the medical charts of four of Dr. Richardson's patients on March 13, 2023, without an apparent need-to-know this information. "Need-to-know" is the rule that personal information (or personal health information) should only be available to those employees in an organization that have a legitimate need to know that information for the purpose of delivering their mandated services. Unauthorized access to personal health information without a need-to-know is often referred to as "snooping."

[20] Based on the evidence before me, I agree with the trustee and, therefore, find that a privacy breach occurred.

3. Did the trustee respond to the privacy breach appropriately?

[21] At this stage, my office will move on to consider how the trustee managed the privacy breach. My office will analyze whether the trustee properly managed the privacy breach and took the following steps in responding to it:

- Contained the breach (as soon as possible).
- Notified affected individuals (as soon as possible).
- Investigated the breach.
- Prevented future breaches.

[22] Based on the information that QCMS provided to my office, I will now assess how it addressed each of these four steps. I will make any recommendations, as necessary, following my analysis of each of the four steps.

Contained the breach (as soon as possible)

[23] It is important to contain the breach immediately. In other words, ensure that personal health information is no longer at risk. This may involve:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal information.
- Correcting weaknesses in physical security.

[24] The trustee identified that Physician X (or someone using their credentials as they apparently alleged) viewed the medical charts of four of the trustee's patients. This occurred remotely and after work hours on March 13, 2023. The trustee stated that they met with Physician X on April 13, 2023, to discuss the access that had been made without apparent need, the audit conducted via Accuro and the logins detected remotely and after hours. The trustee explained that during this meeting, Physician X gave their verbal notice to leave the clinic, and their last day at QCMS was May 31, 2023. Therefore, as of June 1, 2023, Physician X's access at QCMS was cancelled. When employee snooping is suspected, an important step to take is to meet with the individual suspected of the snooping to establish what occurred.

[25] Based on the information provided by the trustee, I find that it took appropriate steps to contain the privacy breach.

Notified affected individuals (as soon as possible)

[26] Notification to individuals affected by a breach should occur as soon as possible after key facts about the breach have been established. It is best to contact affected individuals directly, such as by telephone, letter, or in person. However, there may be circumstances where it is not possible, and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include: a notice on a website, posted notices, media advisories and advertisements. Ensure the breach is not compounded when using indirect notification.

[27] Notifications should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[28] The trustee informed my office that it had notified the affected individuals via phone call, as follows:

> …The patients were contacted and informed that their medical charts were accessed inappropriately by another doctor. They were notified that it was reported to the Privacy Commission and that a letter would be sent indicating this. Patients were concerned that "is my information floating around?" Patient asked which Doctor it was and they were advised that it could not be disclosed and asked if Dr. Richardson was still their doctor. Patients were told that the Privacy Commission was contacted and that the physician had left the clinic. I am unsure if the patients fully grasped that their complete medical information was looked at…

[29] The trustee also followed up with each affected individual by letter, advising that:

- A physician other than Dr. Richardson had accessed their personal health information;
- Dr. Richardson had proactively reported this privacy breach to my office and committed to follow any recommendations that may result from such investigation; and

- Dr. Richardson provided the affected individuals my office's contact information, encouraged them to contact my office for any concerns and provided an envelope to mail in their concerns to my office.

[30] I note that at the time of writing this Investigation Report, my office had not received any complaints from the affected individuals.

[31] Based on the above, I find that the trustee provided adequate notification to the four affected individuals. However, I recommend that in the future, the trustee include more details in the notification letters. For example, descriptions of the personal health information accessed, the possible types of harm that may come as a result, and steps the affected individuals can take to protect themselves.

Investigated the breach

[32] Once a breach has been contained the next step is to investigate the breach. Here are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach.
- What occurred.
- How did the privacy breach occur.
- What is the applicable legislation and what specific sections are engaged.
- What safeguards, policies, and procedures were in place at the time of the privacy breach.
- Was the duty to protect met.
- Who are the affected individuals.

[33] The trustee stated that it became aware of the breach on March 23, 2023. At that point, the trustee investigated this matter as follows:

> …The breach was noted by a MOA and reported to the privacy officer. The privacy officer notified the medical director and an investigation occurred. The EMR vendor ACCURO with the support of IT Net Results conducted an investigation…
>
> It was discovered that personal health information of 4 individuals were accessed by [Physician X] consecutively where [sic] [they] did not have a reason to "know". [Physician X] accessed the health information remotely and outside of business hours. Each of the 4 individuals had their personal health information "snooped on".

[34] Pursuant to section 16 of HIPA a trustee has a duty to protect personal health information in its custody or under its control. Section 16 of HIPA states:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[35] "Administrative safeguards" are controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules, and access restrictions.

[36] "Technical safeguards" mean the technology and the policy and procedures for its use to protect personal information and control access to it. Examples of technical safeguards include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems. Technical safeguards

generally include technical security services and mechanisms. General features of technical safeguards can include: firewalls, encrypted transmissions with VPN technology, use of private keys to decrypt files, individualized passwords within an inquiry-based system limited by user roles, use of Oracle for backup systems, no access to the server allowed except for domain administrators, data masks, built-in ability for process audits.

[37] Upon request for further information, the trustee provided a video explaining the log-in procedure into Accuro. The video explained how it required a physician to 1. enter their login credentials (name and password) and 2. enter the Tru-Grid auto-generated code on the physician's phone; making this a two-step authentication process. The trustee further explained that all personal health information was backed up on QCMS' server.

[38] Based on the trustee's response, it appears that the root cause of this privacy breach was administrative in nature, or Physician X's failure to follow established procedures regarding accessing patient records only on a "need-to-know" basis. The trustee has since strengthened those procedures and other administrative safeguards. I will address those in the next section of this Investigation Report. In terms of technical safeguards, it appears that the trustee has appropriate technical safeguards in place.

[39] Based on the detailed explanations and documentation the trustee provided to my office, I find that it conducted an adequate investigation.

Prevent future breaches

[40] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

- What steps can be taken to prevent a similar privacy breach.
    - Can your organization create or make changes to policies and procedures relevant to this privacy breach.
    - Are additional safeguards needed.

- Is additional training needed.
- Should a practice be stopped.

[41] One of the preventative measures that the trustee appears to have focused on was strengthening administrative safeguards. The trustee provided my office with a copy of its policy manual titled "QCMS Privacy and Security Policy and Procedures Manual" and a copy of its policy "Trustee Statement of Accountability". My office noted that this policy manual addressed the following in-depth:

- Accountability
  - Responsibilities of the Privacy Office and the Office Manager
  - Obligations of Employees and Third parties
  - Privacy and security awareness, education and training
  - Accuracy and integrity
  - Identified purpose and openness
  - Challenging Compliance
  - Ceasing to be a physician at QCMS

- Patient Rights
  - Patient access to own record
  - Amending patient record upon request
  - Authorized representative who makes decisions on behalf of patients

- Collection, use, disclosure and consent
  - Collection
  - Use
  - Disclosure
  - Managing patient consent and masking in the EMR

- Safeguards
  - Agreements
  - Management of Breaches
  - Business continuity and disaster recovery plan
  - Retention, storage and destruction of paper records
  - Scanning and destruction of paper records
  - Electronic backups
  - User account management
  - Auditing
  - Destruction of office equipment and medical devices
  - General security software
  - Security of the Office

[42] The trustee also provided my office with a copy of its signed "Trustee Statement of Accountability" document. This document is signed by every physician working at QCMS, including Dr. Richardson and 13 other physicians. This document provides confirmation that each of these physicians understand their obligations regarding access [collection], use and disclosure of personal health information pursuant to HIPA and the trustee's internal policy titled, "Trustee Statement of Accountability."

[43] Based on the information provided by the trustee, it appears that the trustee has necessary policies in place. The trustee also took appropriate action by proactively reporting this privacy breach to my office and the CPSS to investigate which is a positive step.

[44] Therefore, I find that the trustee has adequate measures in place to prevent any future privacy breaches of this nature.

[45] One recommendation I do make, however, is that the trustee, if it has not already done so, implement a schedule of proactive system audits to identify any unauthorized accesses or potential privacy breaches.

III FINDINGS

[46] I find that I have jurisdiction to conduct this investigation.

[47] I find that a privacy breach occurred.

[48] I find that the trustee took appropriate steps to contain the privacy breach.

[49] I find that the trustee provided adequate notification to the affected individuals of the privacy breach.

[50] I find that the trustee conducted an adequate investigation.

[51] I find that the trustee has measures in place to prevent similar breaches from occurring.

IV RECOMMENDATIONS

[52] I recommend that in the future, the trustee include more details in the notification letters. For example, descriptions of the personal health information accessed, the possible types of harm that may come as a result, and steps the affected individuals can take to protect themselves.

[53] I recommend that the trustee, if it has not already done so, implement a schedule of proactive system audits to identify any unauthorized accesses or potential privacy breaches.

Dated at Regina, in the Province of Saskatchewan, this 8th day of January, 2024.

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