Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 300-2017

Dr. Martha Briggs
Dr. Christine Lett
Dr. Angela Poole

January 16, 2018

Summary: Queen City Obstetrics and Gynecology Professional Corporation (QCOG) proactively reported a privacy breach to the Information and Privacy Commissioner (IPC) when it discovered that personal health information that should have been recorded to its electronic medical record was lost. Overall, the IPC found that QCOG made reasonable efforts to address the privacy breach and is taking appropriate steps to prevent or minimize the likelihood of a similar privacy breach in the future.

I BACKGROUND

[1] On November 23, 2017, Queen City Obstetrics and Gynecology Professional Corporation (QCOG) in Regina reported to my office that electronic information within its electronic medical record (EMR) was lost or that its EMR was not recording information from November 7, 2017 to November 22, 2017.

[2] QCOG's EMR is hosted on a server located within its premises. QCOG indicates data is saved onto the local server and then backed up locally within its own office and remotely offsite with its IT service provider.

[3] A disc failure in its server occurred in October 2017. On November 7, 2017, QCOG's IT service provider installed a new server. Unfortunately, a disc failure also occurred on the new server but QCOG was not notified of this disc failure.

[4] Then, on November 23, 2017, QCOG was informed by its IT service provider that all data from November 7, 2017 at 3:30pm to November 22, 2017 was lost. Data was not saved to the server nor was it being backed up locally or remotely.

II DISCUSSION OF THE ISSUES

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

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

[6] First, QCOG 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 three directors of QCOG are health professionals licensed pursuant to *The Medical Professional Act, 1981*. The shares that have been issued are equally split among the three health professionals and their respective professional corporations. 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;

[7] I find that there are three trustees in these circumstances. For ease of reference, I will refer to these three trustees as QCOG in this report.

[8] Second, personal health information in the EMR was either lost or the EMR was not recording personal health information. Therefore, personal health information is at issue in this investigation.

[9] Third, in terms of custody or control of personal health information, there is a Joint Venture Agreement among the three health professionals, their respective medical professional corporations, and QCOG. This Joint Venture Agreement states the following at clause 15(b):

> **QCOG MEDICAL PROF. CORP.** shall own and maintain all of the computer hardware, software and software licenses used to manage, maintain, store and share electronic information about the patients of the Joint Venturers.

[10] Based on the Joint Venture Agreement, I find that QCOG has custody and control over the EMR and the personal health information.

[11] I find that HIPA is engaged.

2. Was the duty to protect pursuant to section 16 of HIPA fulfilled?

[12] Section 16 of HIPA imposes a duty upon trustees to protect information. Specifically, subsection 16(b) of HIPA provides that trustees must have reasonable safeguards to protect against the loss of personal health information. Subsection 16(b) of HIPA provides as follows:

> 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:
>
> ...
>
> (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;

[13] Data loss events can occur due to a number of causes, including human error in accidentally deleting data, power outages, crime (such as theft), or natural disasters such as fires and floods. Since such events can occur, organizations should have business continuity plans and disaster recovery plans to ensure that its operations can be restored and continued in case of an adverse event. This should include ensuring data is protected and can be restored

if a data loss event occurs. Scheduled backups should occur at least once a day and should be a part of an organization's business continuity plan and disaster recovery plan.

[14] QCOG had provided my office with a copy of its Business Continuity and Disaster Recovery Plan (the plan). My office reviewed it and found that it was too vague and incomplete to meet QCOG's obligations under section 16 of HIPA. However, in the course of the investigation, QCOG expanded and defined its plan, which includes specifying that its IT service provider is responsible for backing up its EMR, that its IT service provider is contracted to assist with IT emergencies, and an emergency protocol for contacting its IT service provider. QCOG also states that the plan should be reviewed annually and updated as necessary.

[15] Even though my office initially found that QCOG's plan to be inadequate, I find that QCOG is meeting its obligations under section 16 of HIPA by expanding and defining its plan. To build on QCOG's plan, I recommend that QCOG specify which of its employees (e.g., its Privacy Officer) is responsible for reviewing the plan annually and updating it as necessary.

3. Did QCOG respond appropriately to this privacy breach?

[16] A loss of personal health information qualifies as a privacy breach. My office recommends that trustees take the following five steps when responding to a privacy breach:

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

Contain the breach

[17] To contain a breach is to recover the personal health information as much as possible. In this case, containing the breach will be efforts to restore the personal health information

that should have been saved to the EMR and then backed up on the server and on the local and remote backups.

[18] QCOG's efforts to contain the privacy breach included trying to recover data from its server and its backups. Unfortunately QCOG was not able to recover the data. Also, after it discovered its server and backups were not working, QCOG did not see patients until its server and backups were working again.

[19] QCOG has undertaken the following methods to recover as much personal health information as it can:

- Incoming faxes from November 7, 2017 to November 22, 2017 were recovered.
- Working with eHealth Saskatchewan to recover laboratory and pathology records.
- Working with the Ministry of Health, Medical Services Branch, to recover billing information QCOG had submitted to it up to November 21, 2017. This will identify all the patients that were seen and billed during the time period in which data was not being saved or backed up.
- Contacted Pooled Referrals (an initiative by the Ministry of Health) to have any referrals made to QCOG during this time period re-sent.
- Contacting pre-natal patients to find out when their next scheduled appointments are.
- Contacting referring health service providers of new patients and asking them to fax back to QCOG the consultant letter that QCOG had sent to them.
- Reviewing gynecology patients seen November 7, 2017 to November 22, 2017 and asking the referring physician to fax back to QCOG the consultation letter that QCOG sent them".

[20] I find that QCOG made reasonable efforts to recover as much of the personal health information that it could.

Notify affected individuals

[21] Notifying affected individuals that their personal health information has been lost is important so those individuals can take necessary steps to protect themselves, including ensuring continuity in their care.

[22] Through its containment efforts, QCOG was able to identify many of the affected individuals. In each of the patient charts of the affected individuals, QCOG has included documentation of this incident, a summary of what was likely discussed/planned during their visits in the time period of November 7, 2017 and November 22, 2017, and any additional actions that have been taken or is needed. To notify affected individuals, QCOG spoke with many affected individuals (such as at appointments) about the server failure, the loss of data, and steps it has taken to recover their personal health information. Further, in an email dated January 10, 2018 to my office, QCOG indicated to my office that for those whom it has not been in contact, it will send a letter notifying them of the privacy breach. QCOG will also send a letter to those whose family physician did not send any documentation back to it (as QCOG had requested physicians to send back to QCOG documentation it had sent to them, as described in paragraph [19]).

[23] QCOG acknowledged that it cannot know for sure if all affected individuals have been identified. It believes that if there are affected individuals that have not been identified, it would be a small number of individuals. However, in efforts to try to notify this small number of individuals, QCOG has posted notices at its offices and modified its telephone message for its telephone answering service to request that any patient seen between November 7, 2017 and November 22, 2017 identify themselves to its staff. These notices and telephone message will be in effect for three months.

[24] In the course of my office's investigation, my office recommended that QCOG post a notice on its website of the privacy breach for at least one year because its website has a further reach than putting notices up at QCOG's offices. In an email dated January 10, 2018, QCOG indicated to my office that it will post a notice of the privacy breach to its website.

[25] Based on the above, I find that QCOG has made reasonable efforts to notify affected individuals of this privacy breach.

Investigate the breach

[26] Investigating privacy breaches to identify the root cause is key to understanding what happened and to prevent similar breaches in the future.

[27] Both the local and remote backups were not working at the time the new server was installed on November 7, 2017. The lack of backups was not detected until November 22, 2017 when the IT service provider arrived at QCOG to install a disc to the new server.

[28] Procedures for backing up data should address how often backups should be occurring, who is responsible to ensure backups are occurring, how errors or disruptions to backups are detected, who is notified that there has been error or disruption, and who is responsible to ensure the errors or disruptions are fixed. Further, procedures should address the physical and technical safeguards for backups (such as restricting physical access and encryption).

[29] QCOG provided my office with a copy of its Privacy and Security Policies and Procedures Manual, which addresses backups and storage, as well as general security. I find that the procedures includes important elements including how often backups should be occurring. However, the backup procedures do not address how errors or disruptions to backups are detected, who is notified when there is an error or disruption, and who is responsible to ensure that errors or disruptions are fixed. I recommend that QCOG work with its IT service provider to develop such procedures.

Prevent future breaches

[30] Preventing future breaches means to implement measures to prevent future breaches from occurring. Below are steps QCOG is taking to prevent future breaches.

[31] QCOG has reviewed and made changes to its policies and procedures, including its Business Continuity and Disaster Recovery Plan (as described at paragraph [14]). QCOG also indicated to my office that it will update its policy and procedures with more detail to clarify responsibilities for backups and storage.

[32] QCOG has also met with its IT service provider in which QCOG made several recommendations on how it (the IT service provider) can make changes to its

communication systems, monitoring, backups, and stocking of needed hardware parts and not relying on back-ordered parts for servers.

[33] Furthermore, two additional drives have been installed to the server and two local backup systems have been installed. The remote backup system has been restored. The IT service provider is monitoring all the systems to ensure they are functioning.

[34] Also, QCOG will work with its IT service provider to ensure a detailed service contract is in place, including how the IT service provider will be responsible for backups. Further, the contract will state that QCOG is to be notified if there is an alert or failure in backing up data or if the system is not working properly.

[35] Finally, QCOG notes it is considering other options, including continuous backup options that could be installed or moving towards a cloud-based service instead of a local server.

[36] I find that QCOG is taking appropriate steps to prevent or minimize the likelihood of a similar privacy breach in the future.

Write a privacy breach report

[37] Documenting the privacy breach and the organization's investigation into the matter is a method to ensure that the organization follows through with plans to prevent similar privacy breaches in the future.

[38] QCOG documented its investigation into the privacy breach in a report that was submitted to my office. I find that QCOG has fulfilled this step of responding to a privacy breach.

III FINDINGS

[39] I find that HIPA is engaged.

[40] I find that QCOG is meeting its obligations under section 16 of HIPA by expanding and defining its Business Continuity and Disaster Recovery Plan.

[41] I find that QCOG made reasonable efforts to recover as much of the personal health information that it could.

[42] I find that QCOG has made reasonable efforts to notify affected individuals of this privacy breach.

[43] I find that QCOG's procedures for backups and storage to include important elements, including how often backups should be occurring.

[44] I find that QCOG is taking appropriate steps to prevent or minimize the likelihood of a similar privacy breach in the future.

[45] I find that QCOG has documented its own investigation into the privacy breach.

IV RECOMMENDATIONS

[46] I recommend that QCOG specify which of its employees (e.g. its Privacy Officer) is responsible for reviewing the plan annually and updating it as necessary.

[47] I recommend that QCOG work with its IT service provider to develop procedures for how errors or disruptions to backups are detected, who is to be notified when there is an error or disruption, and who is responsible to ensure that errors or disruptions are fixed, as described at paragraph [29].

Dated at Regina, in the Province of Saskatchewan, this 16th day of January, 2018.

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