Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 089-2021

Dr. Marilyn Davidson, Dr. Barry Gilliland, Dr. Natasha Payton (Saskatoon Obstetric & Gynecologic Consultants)

September 13, 2022

Summary: In December 2020, Saskatoon Obstetric & Gynecologic Consultants (SOGC) suffered a ransomware attack that affected approximately 20,000 patients. SOGC proactively reported this incident to my office. The Commissioner found that SOGC was not able to fully contain the breach as there is no guarantee that data had not been retained by the malicious actors behind this ransomware attack. Additionally, while SOGC had posted a notice on its website that ransomware attack had occurred, additional avenues for providing notice should be considered. The Commissioner also found that due to a lack of retention of system logs, SOGC was unable to fully investigate this matter and recommended SOGC implement a number of safeguards to prevent future instances.

I BACKGROUND

[1] On April 12, 2021, a lawyer on behalf of Saskatoon Obstetric & Gynecologic Consultants (SOGC) proactively reported a privacy breach to my office, which provided as follows:

> On the evening of December 23, 2020, the physicians discovered that they could not remotely log in to the SOGC system and on December 24, 2020 the external IT services provider alerted SOGC that the system appeared to be offline. SOGC's system suffered a ransomware attack on or around December 22, 2020… It appears that the incident resulted from someone opening a malicious email attachment, which resulted in threat actors gaining access to the system and launching malware to lock SOGC's content and then demanding payment to unlock the content.

[2] On April 20, 2021, my office notified SOGC that we would be monitoring their response to this matter and that it may result in a formal investigation pursuant to sections 42(1)(c)

and 52 of *The Health Information Protection Act* (HIPA). On April 20, 2022, my office advised that due to the number of affected individuals, our office would be undertaking a formal investigation regarding this matter.

II DISCUSSION OF THE ISSUES

1. Is HIPA engaged and do I have jurisdiction in this matter?

[3] HIPA applies when three elements are present: 1) there is personal health information; 2) a trustee is involved; and 3) the personal health information is in the custody or control of the trustee.

[4] Based on the information SOGC provided to my office, the ransomware attack allowed for the malicious actors to have access to the entire SOGC environment, including the medical records of approximately 20,000 patients. Medical records would include information such as an individual's registration information and details regarding health services provided to that individual. This information would qualify as personal health information, as defined at sections 2(m)(i), (ii), (iv) and (v) of HIPA:

> **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;
> …
>
> (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;

[5] As such, the first part of the test is met. I will now consider the second part.

[6] For the second part of the test, SOGC advised that at the time of the ransomware attack, the trustees of the personal health information were three physicians, Dr. Marilyn Davidson, Dr. Barry Gilliland, who has since retired, and Dr. Natasha Payton. SOGC provided documentation to support that, at the time, these three made up the Executive Committee at SOGC. As the Executive Committee at SOGC, and as physicians licensed pursuant to *The Medical Professions Act, 1981*, they qualify as trustees pursuant to section 2(t)(xii)(A) of HIPA 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] This supports the second part of the test; I will now consider the third part.

[8] In my office's Investigation Report 306-2019, I defined "custody" and "control".

[9] Custody is the physical possession of a record by a trustee with a measure of control.

[10] Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the records, including restricting, regulating and administering it use, disclosure or disposition. Custody is not a requirement.

[11] SOGC's legal counsel indicated that, "SOGC entered into an EMR Agreement which confirms that the physicians share a single database and that the Executive Committee will have control over the use, access and disclosure of the information and be the trustees of the information in the system." It also provided a copy of the agreement that reflects this.

[12] At the time of the ransomware attack, these three physicians were jointly responsible for all medical records. As such, the records were in their custody or control, which meets the third part of the test.

[13] As all three parts of the test are met, I find HIPA is engaged. Therefore, I have jurisdiction to investigate this matter.

2. Did SOGC respond appropriately to the privacy breach?

[14] SOGC's legal counsel had a Security Incident Report (SRG report) completed by an external consultant, Security Resource Group Inc. (SRG). The SRG report summarizes SRG's findings of the ransomware attack on SOGC. SOGC's legal counsel expressed concerns about which details from the incident report my office would include in the Investigation Report as those details could be misused by malicious actors. SOGC's legal counsel also cited SRG's report is a solicitor-client privileged document, and also referenced my office's Review Report 039-2021. That report considers a request to access an 840-page Data Forensics Analysis relating to a ransomware attack on eHealth Saskatchewan. That Data Forensics Analysis report was considered in my office's Investigation Report 009-2020, 053-2020, 224-2020, in which my office discussed details of the forensics analysis I found necessary to include to establish grounds for my findings and recommendations.

[15] Section 54(4) of HIPA provides that the Commissioner may disclose, in a report, information deemed necessary for that purpose:

> **54**(4) In a report prepared pursuant to this Act, the commissioner may disclose any information that the commissioner considers necessary to disclose to establish grounds for the findings and recommendations in the report.

[16] I will, then, include only details in this Investigation Report that I determine are necessary to establish my findings and recommendations.

[17] The SRG report states that "it is suspected that a malicious email attachment was opened on a workstation", which resulted in the ransomware attack. The SRG report also indicated that the malicious actors behind the ransomware attack "were able to attain privileged user permissions and therefore had the keys to the environment… they had access to the entire SOGC environment." The SRG report provides the following regarding the intent of the attack:

> The attack on December 22, 2020 was confirmed as a ransomware breach, meaning the malicious access to the SOGC environment was intended to gain as much access to the SOGC IT assets as possible and lock down business operation data and demand payment to unlock that content.
>
> The malware code used for this attack is well known in the cyber security industry and is designed to insert and lock down a customer. It is designed to exfiltrate business critical information for sale on the dark web, should the ransom not be paid.

[18] As SOGC does not appear to dispute that a privacy breach occurred, and as the documentation provided to my office including the SRG report supports this, I will move on to consider if SOGC appropriately addressed the breach. My office's Rules of Procedure outlines that my office will analyze whether the trustee properly managed the breach and took the following steps in responding to the privacy breach:

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

[19] I will now consider if SOGC appropriately addressed these four best practice steps.

Contained the breach (as soon as possible)

[20] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice

- Recovering the records
- Shutting down the system that has been breached
- Revoking access privileges
- Correcting weaknesses in physical security.

[21] Effective and prompt containment may reduce the magnitude of a breach and, in some instances, the risk to individuals.

[22] At the time of the ransomware attack, SOGC engaged an external information technology (IT) service provider for its IT services. On December 23, 2020, SOGC physicians discovered that they could not remotely log in to the SOGC system. On December 24, 2020, the IT service provider alerted SOGC that the system appeared to be offline. After investigating the outage, the IT service provider reached the conclusion that a ransomware attack had occurred.

[23] Prior to SRG's involvement on December 28, 2020, SOGC shut down local network and internet connectivity. SOGC's legal counsel then contracted with SRG on December 29, 2020, to assist with the response to the ransomware attack. SRG's report outlines it took steps such as shutting down open ports and helping develop a recovery plan. As part of this, there was a settlement with the malicious actors on the decryption software for the encrypted data, and confirmation that all exfiltrated data would be deleted. This settlement was reached on January 7, 2021, with the decryption software provided to SOGC on January 16, 2021.

[24] SRG's report, which was completed in January 2021, noted that it had conducted dark web monitoring and that there was no evidence the data had been posted for sale. In April 2022, SOGC stated that it had conducted another dark web scan and did not find any malicious hits related to SOGC or this incident on the dark web.

[25] My office's Investigation Report 009-2020, 053-2020, 224-2020 provided the following explanation of the different levels of the internet:

> [74] First, I would like to explain the dark web. There are three levels of internet – surface web, dark web, and deep web. The following is a description of each found on the Center for Internet Security's (CIS) website:
>
> - **The Surface Web** is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft's Internet Explorer or Edge, and Google Chrome.
>
> - **The Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Users must log in or have the specific URL or IP address to find and access a particular website or service. Some pages are part of the Deep Web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, so they are not indexed by search engines, while others explicitly block search engines from identifying them. Many Deep Web sites are data and content stored in databases that support services we use every day, such as social media or banking websites. The information stored in these pages updates frequently and is presented differently based on a user's permissions.
>
> - **The Dark Web** is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access. Two popular tools for this are Tor and I2P. These tools are commonly known for providing user anonymity. Once logged into Tor or I2P the most direct way to find pages on the Dark Web is to receive a link to the page from someone who already knows about the page. The Dark Web is well known due to media reporting on illicit activity that occurs there. Malicious actors use the Dark Web to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data. However, just like the Surface Web, there are several legitimate activities on the Dark Web as well, including accessing information, sharing information, protecting one's identity, and communicating with others. Many news organizations operate on the Dark Web to protect confidential sources.
>
> (https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/, accessed on October 30, 2020)
>
> [75] The dark web is best known for illegal and criminal activity that is conducted anonymously.

[26] While SOGC took steps to contain the breach, conducted dark web monitoring and received assurances from the malicious actors that any exfiltrated data would be deleted, there is no guarantee the malicious actors would not retain copies of the information. As discussed in my office's Investigation Report 009-2020, 053-2020, 224-2020, there have been cases

where stolen data is found for sale on the dark web years later. Based on this, I find SOGC did not contain the breach.

[27] A critical part of SOGC's ongoing attempts to contain the breach is to continue monitoring if the stolen data resurfaces. The most likely place for the data to resurface is on the dark web. As such, I recommend that SOGC continue to conduct dark web monitoring for five years from the date of the privacy breach and notify any affected individuals of any evidence of activity on the dark web.

Notified affected individuals (as soon as possible)

[28] It is a best practice to inform affected individuals and my office of a privacy breach in most cases. The following is a list of individuals organizations that may need to be notified as soon as possible after learning of the incident:

- The organization's privacy officer
- My office
- The police, if criminal activity is suspected and
- The affected individual(s) (unless there are compelling reasons why this should not occur).

[29] Notification to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact the affected individuals directly.

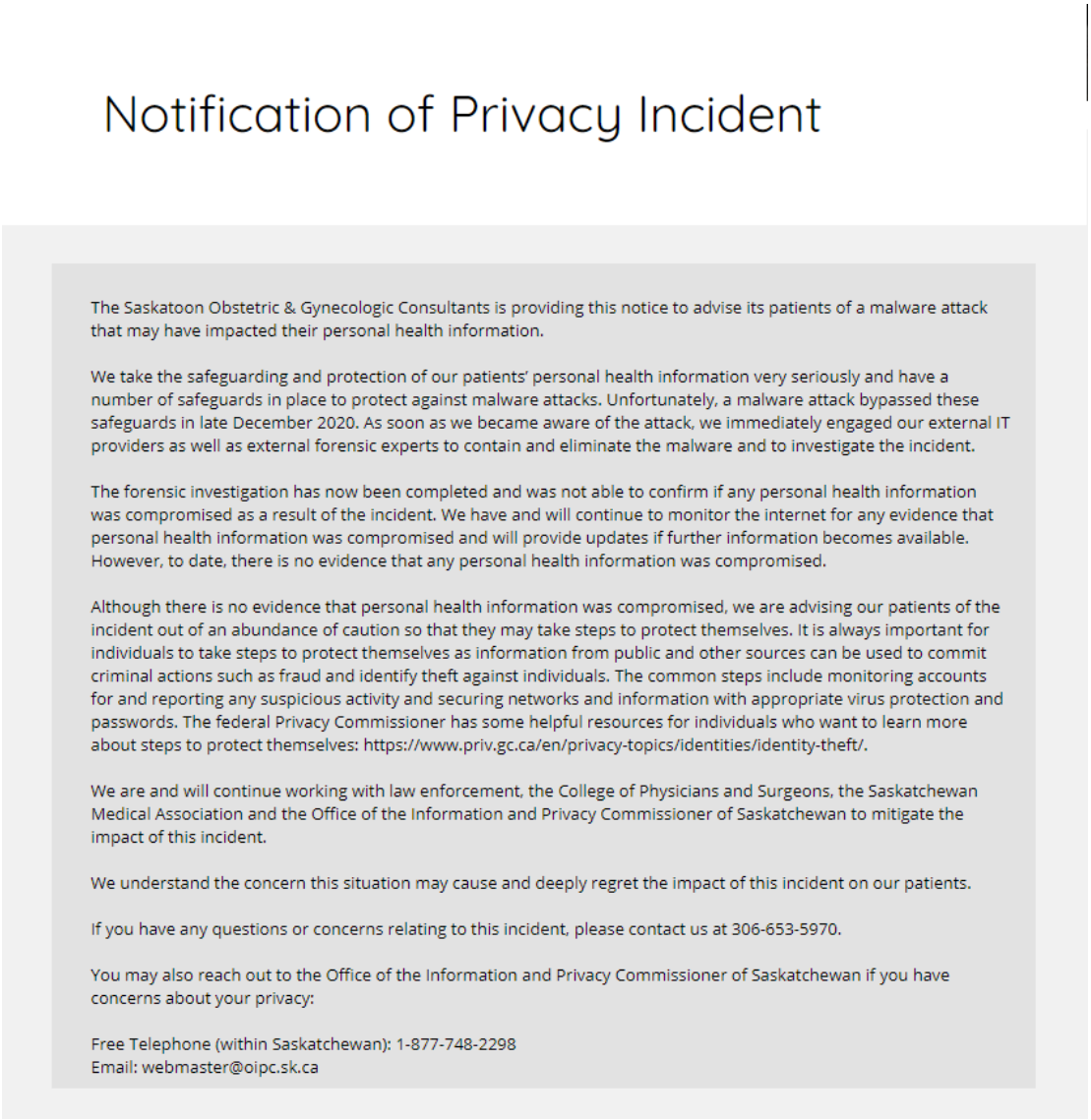
[30] However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements.

[31] Notification should include the following:

- a description of the breach (a general description of what happened)
- a detailed description of the personal information or personal health information involved
- the steps taken and planned to mitigate the harm and to prevent future breaches
- if necessary, advice on actions the individual can take to protect themselves
- contact information of an individual within the organization who can answer general questions and provide further information
- a notice that individuals have a right to complain to my office, including contact information and
- recognition of the impacts of the breach on affected individuals and an apology.

[32] SOGC proactively reported this incident to my office, the Saskatoon Police Service (SPS), the College of Physicians and Surgeons of Saskatchewan and the Saskatchewan Medical Association.

[33] To notify the affected individuals, SOGC posted a notice on its website regarding this incident. The notice on its website advised as follows:



Notification of Privacy Incident

The Saskatoon Obstetric & Gynecologic Consultants is providing this notice to advise its patients of a malware attack that may have impacted their personal health information.

We take the safeguarding and protection of our patients' personal health information very seriously and have a number of safeguards in place to protect against malware attacks. Unfortunately, a malware attack bypassed these safeguards in late December 2020. As soon as we became aware of the attack, we immediately engaged our external IT providers as well as external forensic experts to contain and eliminate the malware and to investigate the incident.

The forensic investigation has now been completed and was not able to confirm if any personal health information was compromised as a result of the incident. We have and will continue to monitor the internet for any evidence that personal health information was compromised and will provide updates if further information becomes available. However, to date, there is no evidence that any personal health information was compromised.

Although there is no evidence that personal health information was compromised, we are advising our patients of the incident out of an abundance of caution so that they may take steps to protect themselves. It is always important for individuals to take steps to protect themselves as information from public and other sources can be used to commit criminal actions such as fraud and identify theft against individuals. The common steps include monitoring accounts for and reporting any suspicious activity and securing networks and information with appropriate virus protection and passwords. The federal Privacy Commissioner has some helpful resources for individuals who want to learn more about steps to protect themselves: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/.

We are and will continue working with law enforcement, the College of Physicians and Surgeons, the Saskatchewan Medical Association and the Office of the Information and Privacy Commissioner of Saskatchewan to mitigate the impact of this incident.

We understand the concern this situation may cause and deeply regret the impact of this incident on our patients.

If you have any questions or concerns relating to this incident, please contact us at 306-653-5970.

You may also reach out to the Office of the Information and Privacy Commissioner of Saskatchewan if you have concerns about your privacy:

Free Telephone (within Saskatchewan): 1-877-748-2298
Email: webmaster@oipc.sk.ca

[34] While SOGC included notice of the incident on its website, the notice does not fully acknowledge the ransomware attack's impact to individuals' personal health information, such as details regarding the types of information that may have been included in the privacy breach. Additionally, while placing notice on your website is one avenue of providing mass notification, it is possible that many of the affected individuals, such as former patients, may not have accessed SOGC's website in order to see the notice. Current patients might not either.

[35] Based on the preceding, I find that SOGC has not provided sufficient notification to affected individuals.

[36] I recommend SOGC consider other avenues to provide notification, including direct notification to active SOGC patients, and mass notification, such as media advisories and advertisements. This may assist in reaching additional affected individuals that may not access SOGC's website. The notification should clearly acknowledge that the malicious actors had access to all affected individuals' personal health information.

[37] In addition to continued monitoring and reporting of dark web activity to affected individuals I previously recommended in this Investigation Report, I also recommend SOGC offer identity theft protection, including credit monitoring, to any affected individuals for a minimum of five years from the date their information is discovered on the dark web.

Investigated the breach

[38] Investigating the privacy breach to identify root causes is key to understanding what happened. It is an important step in mitigating the risk of a future breach of a similar nature from occurring.

[39] After SOGC encountered issues on December 23, 2020, its IT service provider started to investigate the issue. Based on the SRG report, on December 26, 2020, the IT service provider notified SOGC that it had identified the ransomware attack during troubleshooting on December 24, 2020. SOGC then contracted with SRG on December 29, 2020 to conduct a forensic analysis into the ransomware attack and assist in its response to the incident.

[40] As noted earlier, SOGC suspects that a staff person opened a malicious email attachment on a workstation that resulted in the ransomware attack. The Information and Privacy Commissioner of Ontario resource *Technology Fact Sheet: Protect Against Phishing (July 2019)* explains what phishing is and provides some examples:

> **What is Phishing?**
>
> Phishing is a type of online attack in which an attack – using both technological and psychological tactics – sends one or more individuals an unsolicited email, social media

post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.

Phishing attacks can be generic or customized, and can target both individuals and entire organizations. Attacks that target a specific individual or organization are commonly referred to as spear phishing attacks.

The main goal of a phishing attack is to get the individual to do something that compromises the security of their organization. Attackers achieve this when recipients:

- reply to phishing emails with confidential information
- open email attachments that contain malware
- click on a link that leads to a fake website or page that installs malware
- enter usernames and passwords or other sensitive information on a fake website

…

Examples of Phishing

Phishing attacks often imitate legitimate sources and work by exploiting people's trust, curiosity, fear, and desire to be helpful and efficient.

Phishing messages are often disguised as genuine messages and can include:

- emails that look like official work-related items, such as full mailbox notifications, spam quarantines, password reset alerts, building evacuation plans, benefits enrollment, invoices, and confidential documents

- emails about business-related topics such as shipping confirmations, wire transfer requests, invitations to download documents from cloud storage services or to access and online file-sharing services to retrieve, create or edit a document

- emails that try to replicate offers or accounts that people already have, such as bank, income tax or frequent flyer accounts, photo tagging, social networking, gift card notifications, and online shopping security updates

[41] Based on the SRG report, it appears that SRG faced obstacles with the data being supplied by SOGC's IT service provider in order to conduct its analysis. For example, firewall logs had been overwritten, according to the IT service provider, as SOGC had not subscribed to firewall data retention.

[42] As trustee, SOGC has a duty to protect the personal health information in its custody and control pursuant to section 16 of HIPA. A trustee also has a duty under HIPA to ensure its information management service provider (IMSP) is meeting its obligations as per its written agreement with the IMSP pursuant to section 18 of HIPA. Such an agreement needs to appropriately outline the services the IMSP will provide and its expectations to complete those services (e.g., retention period for firewall and server logs).

[43] The SRG report provides that "thousands of login failures had been generating as far back as November 8, 2020" for the IT account that was accessed by the malicious actors responsible for the ransomware attack. However, based on the anti-virus logs, it appears there were unsuccessful attempts at accessing the account made prior to the December 23 ransomware attack. Due to the issues with accessing server and firewall logs, SOGC was not able to determine if these login failures were related to the malicious actors. The lack of firewall logs also prevented SOGC from determining what data had been exfiltrated in the December 23 ransomware attack.

[44] SOGC took steps to engage with experts to respond to the ransomware attack and investigate how the attack occurred. Because of the lack of data needed for SRG to complete its analysis and prepare its report, it does not appear SOGC was able to reach concrete findings.

[45] SOGC had an agreement in place with its IT service provider to provide regular monitoring and reporting to SOGC, as well as noting it would make attempts to rectify any problem in a timely manner. It is also the expectation of SOGC that the IT service provider have appropriate security protocols implemented including investigation of suspicious activity and retention of firewall and network security logs. SOGC is the trustee that has the responsibility to make certain that its IT service provider has appropriate safeguards in place to meet the duty to protect under HIPA.

[46] For the reasons cited in the preceding paragraphs, I find SOGC's investigation was not adequate. I recommend SOGC develop and implement a policy and procedure, or ensure

the agreements with its IT service providers, contain language regarding the retention of firewall and network security logs, and that regular reviews of those logs are conducted to enable monitoring of SOGC's system.

[47] I further recommend that SOGC conduct a comprehensive review of security protocols to ensure they include provisions for in-depth investigation when early signs of suspicious activity are detected.

Prevented future breaches

[48] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, this is what steps can be taken to prevent a similar privacy breach from occurring. To assist, some questions trustees can ask are:

- 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?

[49] SRG's report provided SOGC with the following recommendations to prevent future ransomware attacks, which I am summarizing, as follows:

- Implement a security awareness program and conduct regular tests of that program
- Implement network segmentation
- Schedule regular vulnerability assessments
- Upgrade older vulnerable technologies
- Filter email
- Formalize the use of a firewall

- Implement password expiry and password handling policies
- Create a network diagram and asset list and
- Have data backup procedures.

[50] My office followed up with SOGC to determine if it had implemented the recommendations from the SRG report. SOGC advised it had implemented the majority of the recommendations, but that it has since changed IT service providers and made changes to their system configuration, which has made some recommendations redundant. SOGC's legal counsel further explained that SOGC now engages Accuro which is a cloud based electronic medical record (EMR) that is certified by the Saskatchewan Medical Association, rather than storing medical records on an on-site server managed by an IT service provider.

[51] Although SOGC indicated it has implemented some preventative measures, I find that the details provided are not comprehensive or detailed enough at this point to adequately ensure the prevention of similar breaches.

[52] Section 16 of HIPA outlines the obligation of a trustee to ensure it has appropriate safeguards in place to protect personal health information 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:
>
> (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.

[53] My office requested SOGC provide copies of relevant policies, procedures and agreements that it has in place to prevent future instances. SOGC's legal counsel advised it terminated its relationship with its previous IT service provider and now uses a cloud based EMR system for its medical records. SOGC's legal counsel also indicated that, "SOGC does not have internal IT resources and so the relevant policies are those of the service providers that SOGC engages". SOGC further advised that at the time of hiring, it discusses privacy and cyber precautions with employees, and that it would provide annual reminders. SOGC also has staff read and sign a confidentiality statement. The confidentiality statement does indicate that employees are to comply with HIPA and other applicable policies and procedures.

[54] A privacy agreement similar to the *Sample Privacy Agreement for Trustees: Protection of Personal Health Information* developed by my office may provide SOGC staff with additional guidance on how to comply with HIPA when conducting their work. It may also provide them with a better understanding of what they are agreeing to when they sign an agreement to comply with HIPA. I recommend SOGC develop and implement a privacy agreement for staff to sign on an annual basis, similar to the *Sample Privacy Agreement for Trustees: Protection of Personal Health Information* developed by my office. To support this, I also recommend SOGC develop and implement a formal annual privacy training program for staff.

[55] Malicious actors are discovering new ways every day to trick employees into clicking links and opening documents that contain viruses and malware, including ransomware. SOGC must ensure it develops and implements appropriate policies, or ensure the IT service providers' policies to safeguard the personal health information in its custody or control are in compliance with HIPA. With respect to safeguards, I recommend SOGC undertake the following to ensure the prevention of similar breaches from occurring:

1. That SOGC review SRG's recommendations, which I have outlined at paragraph [49] of this Report, with its new IT service provider to ensure necessary safeguards are in place, or safeguards that those that will provide equal to or greater protection than those recommended in SRG's report.

2. That SOGC ensures it has a written agreement with its new IT service provider clearly outlines the services the IT service provider will provide.

3. That SOGC's acceptable IT usage policies and procedures outline what employees can and cannot do, including examples of acceptable usage and types of threats. As part of this, there should be a requirement for ongoing awareness training. SOGC should continually review and update these policies and procedures, as well as its awareness training.

III FINDINGS

[56] I find that HIPA is engaged.

[57] I find that SOGC has not contained the breach.

[58] I find that SOGC has not provided sufficient notification to affected individuals.

[59] I find that SOGC was not able to fully investigate the ransomware attack.

[60] I find that although SOGC has indicated that some preventative measures have been implemented, they were not comprehensive or detailed.

IV RECOMMENDATIONS

[61] I recommend SOGC continue to conduct dark web monitoring for five years and provide notification to the affected individuals, should there be any evidence of activity on the dark web.

[62] I recommend SOGC consider other avenues to provide notification, including direct notification to active SOGC patients and additionally mass notification, such as media advisories and advertisements.

[63] I recommend SOGC offer identity theft protection, including credit monitoring to affected individuals for a minimum of five years from the date an affected individual's information is discovered on the dark web.

[64] I recommend that in its notification efforts that it notify affected individuals that SOGC will provide identify theft protection, including credit monitoring, for up to five years for any concerned affected individual who requests it.

[65] I recommend SOGC develop and implement a policy and procedure, or ensure the agreements with its IT service providers, contain language regarding the retention of firewall and network security logs, and that regular reviews of those logs are conducted to enable monitoring of SOGC's system

[66] I recommend that SOGC conduct a comprehensive review of security protocols to ensure it includes in depth investigation when early signs of suspicious activity are detected.

[67] I recommend SOGC develop and implement a privacy agreement for staff to sign on an annual basis, similar to the *Sample Privacy Agreement for Trustees: Protection of Personal Health Information* developed by my office. To support this, I also recommend SOGC develop and implement a formal annual privacy training program for staff.

[68] I recommend that SOGC review SRG's recommendations, which I have outlined at paragraph [49] of this Report, with its new IT service provider to ensure necessary safeguards are in place.

[69] I recommend that SOGC ensures it has a written agreement with its new IT service provider clearly outlining the services the IT service provider will provide.

[70] I recommend that SOGC's acceptable IT usage policies and procedures outline what employees can and cannot do, as well as a requirement for ongoing awareness training, as outlined at paragraph [55] of this Report.

Dated at Regina, in the Province of Saskatchewan, this 13th day of September, 2022.

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