Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 043-2019
INVESTIGATION REPORT 272-2019

Dr. Roy Chernoff, Dr. Colin Halbgewachs

August 27, 2019

Summary: The Applicant requested access to the Applicant's personal health information. However, due to a data loss failure, the trustees were not able to provide a copy of a chest x-ray to the Applicant. The Information and Privacy Commissioner (IPC) found that the trustees conducted an adequate search for records. The IPC made a number of recommendations to the trustees to prevent a similar data loss in the future.

I BACKGROUND

[1] On September 26, 2013, the Applicant received a chest x-ray at North Heights X-Ray, a business located in Saskatoon.

[2] A few years later, on November 13, 2017, North Heights X-Ray lost 247 gigabytes of data due to a hard drive failure.

[3] Soon after, on January 22, 2018, an entity named 102039795 Saskatchewan Ltd purchased North Heights X-Ray.

[4] Then, in a letter dated July 2, 2018, the Applicant requested the following from North Heights X-Ray:

> Thank for your effort in producing the image of my chest xray [sic] performed on September 26, 2013 and confirmation that retaining it is required by regulation during our conversation on June 21st.

> Please send it and all related records for which your office is responsible to the address above, including records that were created by third parties and other health record trustees in accordance with the Health Information Protection Act.

[5] North Heights X-Ray responded to the Applicant in a letter dated January 9, 2019. Enclosed in the letter was the radiology report associated with the chest x-ray but not the chest x-ray itself. North Heights X-Ray offered the following explanation of how x-rays were lost. The explanation is as follows:

> North Heights Data Loss
>
> Sometime on November 13, 2017 the primary storage unit suffered a hard drive failure. Due to how the storage units work when this happened the storage unit started to perform extremely poorly since it was too full now that it has one less hard drive than before. When this was diagnosed at 10:30pm it was going to be too late to get a replacement hard drive in time for the morning. So to get the unit operational for the morning information some x-rays were deleted from the primary storage unit. The data removed was approximately 247GB and was within the following dates:
>
> - September 2013 - November 2013
> - February 2014 - December 2014
>
> The intention was that after the drives were replaced and the primary storage unit was operating properly the x-rays would be restored from the backup storage unit. Unfortunately the nightly backup process was configured to mirror the primary storage unit, so when the backup process ran it removed the files from the backup storage unit as well. This oversight was not discovered until June 19, 2018 while searching for the reason that some x-ray images were not retrievable.

[6] In an email dated January 22, 2019, the Applicant requested a review by my office.

[7] On February 5, 2019, my office notified Dr. Roy Chernoff (Dr. R. Chernoff) and Dr. Colin Halbgewachs (Dr. C. Halbgewachs) that it would be undertaking a review.

[8] Further, on August 9, 2019, my office notified Dr. R. Chernoff and Dr. C. Halbgewachs that it would be undertaking an investigation into the loss of personal health information.

II RECORDS AT ISSUE

[9] The first issue is whether Dr. R. Chernoff and Dr. C. Halbgewachs' efforts to search for records responsive to the Applicant's access request was adequate. The second issue is whether or not Dr. R. Chernoff and Dr. C. Halbgewachs met their duty to protect pursuant to section 16 of *The Health Information Protection Act* (HIPA). As such, there are no records at issue.

III DISCUSSION OF THE ISSUES

1. Is HIPA engaged and do I have jurisdiction to conduct this review and investigation?

[10] HIPA is engaged when three elements are present: 1) personal health information, 2) a trustee, and 3) the personal health information is in the custody or control of the trustee. Below is an analysis to determine if the three elements are present.

Personal health information

[11] 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;

[12] I find that information such as a chest x-ray qualifies as personal health information as defined by subsection 2(m) of HIPA.

Trustee

[13] Subsection 2(t)(xii)(A) of HIPA defines "trustee" as follows:

> 2 In this Act:
> ...
> (t) "trustee" means any of the following that have custody or control of personal health information:
> ...
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible;

[14] Both Dr. R. Chernoff and Dr. C Halbgewachs are licensed health professionals pursuant to *The Medical Profession Act, 1981*. Therefore, they both qualify as a "trustee" pursuant to subsection 2(t)(xii)(A) of HIPA.

Custody or control of personal health information

[15] According to Information Services Corporation's (ISC) Corporate Registry, North Heights X-Ray is owned by 102039795 Saskatchewan Ltd. Dr. R. Chernoff and Dr. C. Halbgewachs are equal shareholders of 102039795 Saskatchewan Ltd. As such, I find that Dr. R. Chernoff and Dr. C Halbgewachs would have custody or control of the personal health information requested by the Applicant.

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

[17] Pursuant to subsection 43(1) of HIPA, I find that my office has the authority to undertake a review in this matter. Further, pursuant to subsection 52(d) of HIPA, I find that my office has the authority to undertake an investigation into the privacy aspects of this matter.

2. Has Dr. R. Chernoff and Dr. C. Halbgewachs conducted an adequate search?

[18] Sections 12 and 32 of HIPA provides individuals with the right to request access to personal health information in the custody or control of a trustee. These sections provide as follows:

> 12 In accordance with Part V, an individual has the right to request access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.
> ...
> 32 Subject to this Part, on making a written request for access, an individual has the right to obtain access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.

[19] When a trustee receives a written request for access, the trustee should conduct an adequate search for records responsive to the request. In a review with my office, trustees must demonstrate that they have conducted a reasonable search to locate records.

[20] The trustees in this case have a record of all the images (or x-rays) taken since December 2004. Therefore, they conducted a database search for the Applicant and noted that the Applicant had attended North Heights X-Ray once. Due to the data loss that occurred on November 13, 2017, it only has the radiology reports that are based on the images (or x-rays) taken but not the images themselves. The trustees provided a copy of the radiology report associated with the Applicant's chest x-ray but not the x-ray itself.

[21] Based on the above, I find that the trustees have conducted an adequate search for records.

3. Has Dr. R. Chernoff and Dr. C. Halbgewachs met the duty to protect personal health information pursuant to section 16 of HIPA?

[22] The data loss occurred when Dr. R. Chernoff and Dr. C. Halbgewachs were not the trustees of the personal health information at North Height X-Ray. Nonetheless, my office's concern is whether or not Dr. R. Chernoff and Dr. C. Halbegwachs have implemented safeguards so that data losses such as the one that occurred in this case does not occur in the future.

[23] Data loss events can occur due to a number of causes, including human error in deleting data, technology failure, power outages, crime (such as theft), or natural disasters such as fires or floods. Organizations should be prepared for data loss events by having business continuity plans and disaster recovery plans. In fact, section 16 of HIPA imposes a duty upon trustees to protect personal health information. Specifically, subsection 16(b)(ii) of HIPA provides that trustees must have reasonable safeguards to protect against the loss of personal health information. Subsection 16(b)(ii) of HIPA provides:

> 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:
>
> ...
>
> (ii) loss of the information;

[24] As described in the background section of this Report, the data loss was a result of a hard drive failure in the primary storage unit for images. In order to get the primary storage unit to work in time for the following day, 247 gigabytes of data was deleted. This deletion was done with the intention of restoring the deleted information from the backup storage unit once the hard drive in the primary storage unit was replaced. However, soon after the data was deleted from the primary storage unit, the nightly backup process ran. As a result, the backup storage unit mirrored the primary storage unit. Since the backup storage mirrored the primary storage unit, the deleted data no longer resided on the backup storage unit.

[25] When I consider the above, the data loss was a result of two factors. The first factor was the lack of a disaster recovery plan to deal with hardware failure. A disaster recovery plan is a plan that enables an organization to restore critical processes, including access to data, so that business may resume. The second factor contributing to the data loss is the lack of awareness or the oversight of the nightly backup process. Below, I will analyze the safeguards Dr. R. Chernoff and Dr. C. Halbgewachs have implemented to determine if they protected against a similar data loss event.

Information Management Service Provider / Custody or control of images

[26] In efforts to implement safeguards to prevent a similar data loss, Dr. R. Chernoff and Dr. C. Halbgewachs signed a services agreement with Saskatoon Medical Imaging (SMI) when they became owners of North Heights X-Ray. SMI is the radiologist groups that reads the images taken at North Heights X-Ray. According to the services agreement, SMI is to maintain two digital copies of each x-ray exam for archiving purposes. As such, SMI is an information management service provider (IMSP) as defined by subsection 2(j) of HIPA, which provides:

> 2(j) "information management service provider" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[27] Any agreement signed by Dr. R. Chernoff and Dr. C. Halbegewachs with an IMSP should abide by section 18 of HIPA. Section 18 of HIPA establishes the rules for the trustee/IMSP relationship. It provides:

> 18(1) A trustee may provide personal health information to an information management service provider:
>
> (a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;
>
> (b) to enable the information management service provider to provide the trustee with information management or information technology services;
>
> (c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or
>
> (d) for the purpose of combining records containing personal health information.
>
> (2) Not yet proclaimed.

> (3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).
>
> (4) Not yet proclaimed.
>
> (5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

[28] Section 18 of HIPA provides that an IMSP manages personal health information on behalf of the trustee. However, clause 10 of the services agreement provides that the images from North Heights X-Ray becomes the property of SMI:

> **10. Property Rights**
>
> X-Ray images made by 102039795 Saskatchewan Ltd. are the exclusive property and responsibility of SMI. Radiologist reports undertaken by SMI are the exclusive property and responsibility of SMI.

[29] Therefore, based on clause 10, it appears that SMI is claiming ownership of the images and is not maintaining the images on behalf of Dr. R. Chernoff and Dr. C. Halbgewachs. This suggests that Dr. R. Chernoff and Dr. C. Halbgewachs neither have custody nor control over the x-ray images. The lack of custody or control is a significant barrier to Dr. R. Chernoff and Dr. C. Halbgewachs' ability to meet their duty to protect personal health information pursuant to section 16 of HIPA because they cannot effectively implement safeguards. Further, without custody or control, Dr. R. Chernoff and Dr. C. Halbgewachs would not be able to fulfill their other duties under HIPA, including responding to access requests under HIPA. I find that the agreement between Dr. R. Chernoff and Dr. C. Halbgewachs with SMI is not in compliance with section 18 of HIPA. I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs determine if they are able to revise the agreement they have with SMI so that the agreement is in compliance with section 18 of HIPA. The revised agreement should provide that Dr. R. Chernoff and Dr. C. Halbgewachs maintain control over the images they provide to SMI, and that SMI will cooperate with and assist Dr. R. Chernoff and Dr. C. Halbgewachs in fulfilling their duties under HIPA.

Mirrored Servers and backing up of data

[30] According to the services agreement, SMI agreed to store two images of each x-ray coming from North Heights X-Ray into SMI's archives. Clause 7 of the agreement provides as follows:

> **7. X-Ray and PACS Equipment**
>
> SMI shall maintain two (2) digital copies of each x-ray exam for archiving purposes subject to the required retention period as prescribed by governing bodies.

[31] In a letter dated July 30, 2019, Dr. R. Chernoff and Dr. C. Halbgewachs informed my office that SMI has two mirrored servers, one of which resides off-site. When SMI receives an image from North Heights X-Ray, a copy of the image is saved on one of the servers. Then, the image is immediately forwarded to the other server. They note that "all modalities have an internal memory, just in case images are corrupted in transition". They also advised my office that SMI anticipates that all images will be held indefinitely.

[32] Based on the above, I find that Dr. R. Chernoff and Dr. C. Halbgewachs still have not implemented safeguards that would prevent a similar data loss event. While SMI's "two mirrored servers" may be a part of the solution, they do not make up the entire solution to prevent a similar data loss event. For example, other elements of a solution would include:

- determining who is responsible for maintaining SMI's two servers, and
- determining how hardware failures are detected, who should be notified in such an event, and what their roles and responsibilities are.

[33] Further, mirrored servers are good for business continuity and for disaster recovery. If the primary server fails, then the organization can rely on the secondary server until the primary server is fixed. However, mirrored servers are not necessarily sufficient on its own for backing up data. If the secondary server is mirroring the primary server and data is lost on the primary server (for example, data is deleted as it was in this case), then the data is also lost on the secondary server. That is because only the latest version of data is saved on the secondary server. Clause 12.3 of the standard ISO/IEC 27002:20013 by the International

Organization for Standard (ISO) and International Electrotechnical Commission (IEC) provides that the extent and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization. It is not evident to me that the trustees in this case has considered the extent and the frequency of backups that they require to protect against a similar data loss event. I recommend that, in addition to the mirrored servers, Dr. R. Chernoff and Dr. C. Halbgewachs explore additional backup options so that data can be restored from a previous version. In the event of a data loss, they can rely on the backup to restore the data. This may require Dr. R. Chernoff and Dr. C. Halbgewachs seeking the advice of an Information Technology service provider.

[34] In Investigation Report 300-2017, my office recommended that the trustee in that case implement procedures for backing up data, including the following:

- How often backups should be occurring,
- Who is responsible for ensuring backups are occurring,
- How errors or disruptions to backups are detected,
- Who is notified that there has been an error or disruption, and
- Who is responsible to ensure the errors or disruptions are fixed.

[35] Further, the procedures should also address the physical and technical safeguards for backups (such as restricting physical access to the backups and encryption of the data). I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs establish and implement procedures for backing up its data according to the above points. They should also reference ISO/IEC 27002:20013 when establishing their backup procedures.

Retention

[36] As mentioned earlier, Dr. R. Chernoff and Dr. C. Halbgewachs advised that SMI intends to retain the images indefinitely. Subsection 17(1) of HIPA addresses retention periods for personal health information but it has not yet been proclaimed. However, subsection 13.9 and 13.9.1 of the *Guidelines for the Protection of Health Information* (the Guidelines) by Digital Health Canada (formerly known as Canada Health Informatics Association)

provides some guidelines for health care organizations. The Guidelines recognize that in health care, it is sometimes difficult to determine when the information will no longer be needed. Therefore, information is often kept for an indeterminate length of time. Even so, health care organizations must determine the appropriate retention periods. More recent information will be retained as active files while older information might be archived. Whatever the storage medium, health care organizations must take care to adequately protect against loss, theft, unauthorized use, disclosure or access. I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs consult the Guidelines by Digital Health Canada and establish retention periods of the images and also establish appropriate storage mediums for the active files and for older files. Maintaining personal health information indefinitely unnecessarily leaves it open to privacy breaches.

PACS

[37] In the letter dated July 30, 2019 to my office, Dr. R. Chernoff and Dr. C. Halbgewachs indicated that all their images will soon be sent to the provincial Picture Archiving and Communications System (PACS). In other words, PACS will be another area in which images will be backed up.

[38] Dr. R. Chernoff and Dr. C. Halbgewachs provided my office with a copy of an agreement between eHealth Saskatchewan (eHealth) and SMI. Based on this agreement, SMI will be providing a copy of the data on its servers to eHealth so that eHealth can include the data on PACS. The agreement specifies the following regarding trusteeship:

> **Trusteeship:** The Radiology Clinic [SMI] is the trustee of the Community PACS data while it is in the Radiology Clinic's local medical imaging system. Once the Community PACS data has been transferred to eHealth, eHealth becomes the trustee of the Community PACS data.

[39] While a copy of the x-rays will be saved on PACS, PACS should not be considered a form of backup that could be used to restore data after a data loss event. The purpose of PACS is to make diagnostic images and associated radiology orders and reports from community based radiology clinics electronically available to physicians and other approved health

care providers providing patient care within Saskatchewan. The purpose of PACS is not for eHealth to act as a backup of data for community clinics. Further, there would be no legislative authority in HIPA for eHealth to disclose personal health information to Dr. R. Chernoff and Dr. C. Halbgewachs for such a purpose. I find that Dr. R. Chernoff and Dr. C. Halbgewachs cannot rely on PACS as a safeguard to protect against a similar data loss event. I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs not rely on PACS as a backup to restore data after a data loss event.

IV FINDINGS

[40] I find that HIPA is engaged.

[41] I find that my office has the authority to undertake a review in this matter.

[42] I find that my office has the authority to undertake an investigation into the privacy aspects of this matter.

[43] I find that Dr. R. Chernoff and Dr. C. Halbegwachs have conducted an adequate search for records.

[44] I find that the agreement between Dr. R. Chernoff and Dr. C. Habegewachs with SMI is not in compliance with section 18 of HIPA.

[45] I find that Dr. R. Chernoff and Dr. C. Halbgewachs have not implemented necessary safeguards that would prevent a similar data loss event.

[46] I find that Dr. R. Chernoff and Dr. C. Halbgewachs cannot rely on PACS as a safeguard to protect against a similar data loss event.

V RECOMMENDATIONS

[47] I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs determine if they are able to revise the agreement they have with SMI so that the agreement is in compliance with section 18 of HIPA. The revised agreement should provide that Dr. R. Chernoff and Dr. C. Halbgewachs maintains control over the images they provide to SMI, and that SMI will cooperate with and assist Dr. R. Chernoff and Dr. C. Halbgewachs in fulfilling their duties under HIPA.

[48] I recommend that, in addition to the mirrored servers, Dr. R. Chernoff and Dr. C. Halbgewachs explore additional backup options so that data can be restored to a previous version. In the event of a data loss, they can rely on the backup to restore the data. This may require Dr. R. Chernoff and Dr. C. Halbgewachs seeking the advice of an information technology service provider.

[49] I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs establish and implement procedures for backing up its data as described at paragraphs [34] and [35]. They should also reference ISO/IEC 27002:20013 when establishing their backup procedures.

[50] I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs consult the Guidelines by Digital Health Canada and establish retention periods of the images and also establish appropriate storage mediums for the active files and for older files.

[51] I recommend that Dr. R. Chernoff and Dr. C. Halbgewachs not rely on PACS as a backup to restore data after a data loss event.

Dated at Regina, in the Province of Saskatchewan, this 27th day of August, 2019.

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