Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT
351-2017, 031-2018, 143-2018, 144-2018, 145-2018

eHealth Saskatchewan, Dr. Stan Oleksinski (operating as West Hill Medical Clinic), Dr. Nico Basson and Dr. L.N. de Beer (operating as South Hill Medical Practice), Saskatchewan Health Authority (formerly Prince Albert Parkland Regional Health Authority), Dr. L.N. de Beer (operating as Dr. L.N. de Beer Medical Professional Corporation)

December 6, 2018

Summary: The College of Physicians and Surgeons of Saskatchewan (CPSS) laid charges against Dr. Josias Furstenberg involving access to eHealth Saskatchewan's (eHealth) eHR Viewer (the Viewer). The Commissioner also launched an investigation of the matter and the role of all trustees involved including eHealth, Dr. Stan Oleksinski (operating as West Hill Medical Clinic), Dr. Nico Basson and Dr. L.N. de Beer (operating as South Hill Medical Practice), Saskatchewan Health Authority (formerly Prince Albert Parkland Regional Health Authority), Dr. L.N. de Beer (operating as Dr. L.N. De Beer Medical Professional Corporation). The Commissioner focused on the governance structure and how Dr. Furstenberg gained access to the Viewer. He concluded there were insufficient safeguards in place to protect the personal health information in the Viewer. He made several recommendations including changes to how physicians are granted access to the Viewer and improved monitoring of safeguards.

I BACKGROUND

[1] On November 24, 2017, the College of Physicians and Surgeons of Saskatchewan (CPSS) laid several charges against Dr. Josias Furstenberg. Some of the allegations against Dr. Furstenberg included:

- causing a photograph of a patient "day sheet" to be sent to an individual without the expressed or implied consent of the persons listed on the "day sheet";
- exchanging text messages with an individual where personal health information about another individual was disclosed without express or implied consent;
- accessing the personal health information of a person through an eHealth Saskatchewan "computer program" without consent or a need-to-know; and
- breaching the Joint Service and Access Policy that pertained to accessing information from eHealth Saskatchewan.

[2] Dr. Furstenberg left the country and subsequently, CPSS revoked his medical licence. The *Council Decision* published by CPSS on June 16, 2018 indicated that Dr. Furstenberg admitted to the charges.

[3] As Dr. Furstenberg has left the country and no longer holds a medical licence in Saskatchewan, my office was unable to investigate the charges related to some of the collections and disclosures of personal health information.

[4] However, I have gathered enough information from eHealth Saskatchewan (eHealth) and other trustees who Dr. Furstenberg was working with to conduct an investigation with respect to personal health information accessed in eHealth's repositories.

Summary of investigation

[5] In November 2017, eHealth responded to CPSS' request for information about patient profile views in relation to an investigation it was conducting. It requested audit log information for the accesses to personal health information of three individuals. eHealth provided CPSS with audit logs on November 15, 2017. CPSS laid charges against Dr. Furstenberg on November 24, 2017.

[6] eHealth was made aware of CPSS' charges on February 12, 2018, when my office contacted eHealth to advise of our intention to undertake an investigation. My office provided formal notification on the same day.

[7] In the next four months, eHealth cooperated with both CPSS' investigation and this investigation. It provided its final investigation report to my office on June 12, 2018.

[8] eHealth determined that Dr. Furstenberg accessed the personal health information in question through eHR Viewer (the Viewer).

[9] eHealth's electronic system, the Viewer, enables users to view the following types of personal health information:

- Laboratory results;
- Medication information;
- Immunization information;
- Transcribed reports;
- Clinical encounters;
- Structured medical records; and
- Chronic disease information.

[10] The personal health information stored in the Viewer is collected from other organizations, including medical clinics or the Saskatchewan Health Authority (SHA). Then, whenever a user of the Viewer views personal health information on the Viewer, eHealth is disclosing personal health information to that particular user (or the user's employer). This report focuses on eHealth's disclosure of personal health information.

[11] Dr. Furstenberg accessed the personal health information of Individual 1 - 15 times on two separate days: January 11, 2016 and July 19, 2016. He accessed the personal health information of Individual 2 - 255 times on thirteen dates between February 1, 2017 and June 14, 2017. eHealth also included one view of Individual 3's personal health information in its investigation.

[12] In order for an individual to request to gain access to the Viewer, he or she must identify the "Authorized Provider Organization" (APO) with whom he or she is associated. An APO is an organization approved by eHealth to have access to personal health information stored within the electronic health record. Within each APO, there is an "Authorized

Approver" that reviews applications for a user account. The Authorized Approver will then either approve or decline the application of each individual.

[13] A user may be approved by several APOs at the same time. Each time a user logs in to the Viewer, he or she must select the APO in which the user is working for at that time. From March 2014 to February 2018, Dr. Furstenberg was able to use the Viewer through six APOs. The six APOs were:

- West Hill Medical Clinic (West Hill)
- South Hill Medical Practice (South Hill)
- Prince Albert Parkland Regional Health Authority (PAPRHA), which is now part of the SHA
- eHS Physicians (managed by eHealth)
- J. J. Furstenberg Medical Prof. Corp.
- Dr. L. N. de Beer Medical Professional Corporation (de Beer Corporation)

[14] As will be discussed, there is an agreement between eHealth and each APO which addresses responsibilities with respect to personal health information of the Viewer. As such, my office also notified West Hill, South Hill, the SHA, and the de Beer Corporation that they would be included in this investigation.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[15] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

[16] In its investigation report, eHealth indicated that Dr. Furstenberg accessed patient demographics, clinical documents and laboratory results of Individuals 1 and 2 in the Viewer.

[17] This information qualifies as personal health information pursuant to subsection 2(m) of HIPA.

[18] Also, there are five trustees involved in this investigation. Subsection 2(t) of HIPA provides:

> 2 In this Act:
> …
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> (i) a government institution;
>
> (ii) the provincial health authority or a health care organization;
> …
> (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
>
> (B) a member of a class of persons designated as health professionals in the regulations;
> …

[19] eHealth is a government institution pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and Part I of the Appendix of *The Freedom of Information and Protection of Privacy Regulations*. Therefore, eHealth qualifies as a trustee pursuant to subsection 2(t)(i) of HIPA. Thus, I have jurisdiction to investigate this matter.

[20] The SHA qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[21] South Hill is owned by two medical professional corporations. The first is Dr. Nico Basson Medical Prof. Corp. Dr. Nico Basson is a Director and majority shareholder. He is registered as a physician in good standing with CPSS. The other medical professional corporation is the de Beer Corporation. Dr. L.N. de Beer is a physician in good standing with CPSS. Both qualify as trustees pursuant to subsection 2(t)(xii)(A) of HIPA. I note,

however, Dr. de Beer and Dr. Basson were not owners of the clinic at the time Dr. Furstenberg worked at the clinic.

[22] West Hill is owned by Dr. W. Stan Oleksinski Medical Professional Corp. Dr. Stan Oleksinski is the director of this corporation and has the majority of voting shares. He is a physician in good standing with CPSS. He also qualifies as a trustee pursuant to subsection 2(t)(xii)(A) of HIPA.

[23] Dr. Furstenberg is the Director and majority shareholder of J.J. Furstenberg Medical Prof. Corp. His medical licence was revoked by CPSS on June 16, 2018.

[24] The personal health information in question in the Viewer was in the custody and control of eHealth at the time of the accesses. This investigation will also probe whether the other trustees have duties and responsibilities in this situation as well.

2. Were Dr. Furstenberg's accesses in the Viewer authorized by HIPA?

[25] Whenever a user views personal health information in the Viewer, eHealth is disclosing personal health information. Personal health information must only be disclosed in accordance with HIPA. Otherwise, the disclosure would qualify as a privacy breach. Further, when a user uses information from the Viewer, the viewing of it would qualify as a collection.

[26] The collection provisions of HIPA are found at sections 23, 24 and 25 of HIPA. The disclosure provisions are found at section 27 of HIPA. There is no need to reproduce them in this report. Trustees and their employees must also collect, use and disclose personal health information when there is a need-to-know. The need-to-know principle is the principle that trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual or other authorized purposes.

[27] My office was not able to interview Dr. Furstenberg. As such, I cannot be certain that the accesses were either authorized by HIPA. However, eHealth's investigation identified some indicators that demonstrate that the accesses were not authorized. Below is a table which summarizes the accesses in question:

Individual	APO indicated	Date	Notes
1	South Hill Medical Practice	January 11, 2016	Did not practice under this organization at time of access
1	West Hill Medical Clinic	July 19, 2016	Individual was not a patient at this clinic
2	SHA (PAPRHA)	February 1, 2017	Not accessed as a result of work required by, or done for this organization
2	eHS Physicians	February 1, 2017	
2	eHS Physicians	February 28, 2017	
2	SHA (PAPRHA)	March 1, 2017	Not accessed as a result of work required by, or done for this organization
2	SHA (PAPRHA)	March 2, 2017	Not accessed as a result of work required by, or done for this organization
2	SHA (PAPRHA)	April 1, 2017	Not accessed as a result of work required by, or done for this organization
2	SHA (PAPRHA)	April 4, 2017	Not accessed as a result of work required by, or done for this organization
2	J.J. Furstenberg Medical Prof. Corp.	May 1, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	May 2, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	May 3, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	May 5, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	May 23, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	May 27, 2017	
2	J.J. Furstenberg Medical Prof. Corp.	June 14, 2017	
3	eHS Physicians	February 3, 2017	Confirmed that Dr. Furstenberg provided a health service to this individual on this date

[28] During its investigation, eHealth determined that only one of the accesses in the Viewer was authorized. eHealth determined that Dr. Furstenberg was providing health services to Individual 3 on the date the personal health information was accessed.

[29] In the case of the first access into the personal health information of Individual 1 on January 11, 2016, Dr. Furstenberg was no longer practicing under the APO that he selected when he logged into the system, which was South Hill. For this reason, eHealth has indicated that this was an unauthorized disclosure and collection of personal health information.

[30] In the same vein, eHealth has worked with the SHA and West Hill to confirm that those organizations did not treat the individuals in question on specific dates listed in the table above or at all. Therefore, eHealth has determined these are unauthorized disclosures and collections of personal health information.

[31] eHealth was not able to determine with certainty that the rest of the disclosures and collections were authorized as it was not able to speak with Dr. Furstenberg.

[32] Only one of the accesses in question was authorized by HIPA.

3. Did eHealth meet its duty to protect pursuant to section 16 of HIPA?

[33] Section 16 of HIPA imposes a duty to protect personal health information upon trustees. Trustees must have safeguards in place to protect personal health information. Section 16 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:
>
> (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.

[34] In order to make a finding as to whether or not eHealth and the other trustees had met its duty to protect personal health information pursuant to section 16 of HIPA, I will review the events and administrative safeguards that eHealth had in place to control access to the Viewer.

Dr. Furstenberg's access in the Viewer

[35] Before I begin to assess the safeguards that eHealth had in place, I will examine how Dr. Furstenberg gained access to the Viewer. As noted previously, eHealth is the trustee of personal health information in the Viewer. eHealth then approves organizations to be APOs. APOs are organizations that provide health services. The APOs do not have to be trustees. Individuals associated with APOs can then apply online for access to the Viewer. The individual will indicate which APO they are applying under. Approvers within the APO will then let eHealth know if they approve or reject the individual's application.

[36] Over the span of approximately four years, Dr. Furstenberg was approved by six APOs. It appears that Dr. Furstenberg worked regularly at two clinics during this time. The table below depicts the APOs under which Dr. Furstenberg was approved:

Trustee	Viewer Access Requested	Viewer Access Approval	Dates worked
South Hill Medical Practice	March 4, 2014	March 4, 2014	Ended in July 2015
eHS Physicians	July 15, 2016	July 18, 2016	N/A
SHA (PAPRHA)	July 14, 2016	November 1, 2017	He did not provide services for PAPRHA since 2008
West Hill Medical Clinic	July 14, 2016	Never Approved	August 2015 – February 2017
J. J. Furstenberg Medical Prof Corp.	April 8, 2017	Became a APO on April 10, 2017	N/A
de Beer Corporation	May 11, 2017	Never Approved	Worked at clinic in Montreal Lake First Nation in 2016/2017

[37] According to the Joint Services/Access Policy (JSAP), APOs have the following responsibilities:

- responsible for all actions and omissions of Users authorized by the Authorized Approver;
- responsible to ensure all Users have completed all necessary training relating to the EHR Viewer or Integration and have completed appropriate privacy and security training;
- responsible to ensure all Users accessing personal health information in the EHR Viewer have signed a confidentiality oath or agreement; and
- responsible for all acts or omissions of the APO's employees, agents and contractors.

[38] In other words, the role of the APO is to ensure that those working under its authority are using the Viewer appropriately. eHealth is relying on the APO's to ensure the individual's it approves is properly trained and using the Viewer in accordance with HIPA. This is an appropriate safeguard. However, as demonstrated by this report, it is not properly executed. Below I will discuss concerns with each one of the APO's that approved Dr. Furstenberg.

a. ***South Hill Medical Practice***

[39] Dr. Furstenberg began working at South Hill in the 2011/2012 fiscal year. Dr. Furstenberg applied for access to the Viewer under South Hill on March 14, 2014 and was granted access to the viewer on the same day. Dr. Furstenberg left South Hill in July 2015 without ever having logged in to the Viewer. He began working at West Hill on August 20, 2015. Dr. Furstenberg's first login to the Viewer was on August 25, 2015 under South Hill, five days after joining West Hill.

[40] eHealth acknowledged that at, that time, it did not have a process to ensure users' access to the Viewer was revoked if those users no longer had a need-to-know or had transitioned to another healthcare organization. eHealth established a User Access Recertification Policy on December 8, 2015. Each June, eHealth sends a list of approved users to the appropriate APOs. Approvers of the APO must give positive feedback by the end of the

month regarding users that should still have access under their respective organization. eHealth would revoke the access of those that no longer require access. Through this procedure, eHealth determined that Dr. Furstenberg no longer required access to the Viewer under South Hill. On January 27, 2016, the Physician's access was revoked. This occurred 16 days after Dr. Furstenberg made the unauthorized access to Individual #1's personal health information on January 11, 2016.

[41] I note that all accesses made by Dr. Furstenberg under South Hill between August 25, 2015 and January 27, 2016 would have been inappropriate. I recommend that eHealth and South Hill work together to identify and notify all individuals whose personal health information were accessed in this manner by Dr. Furstenberg during this timeframe about these privacy breaches.

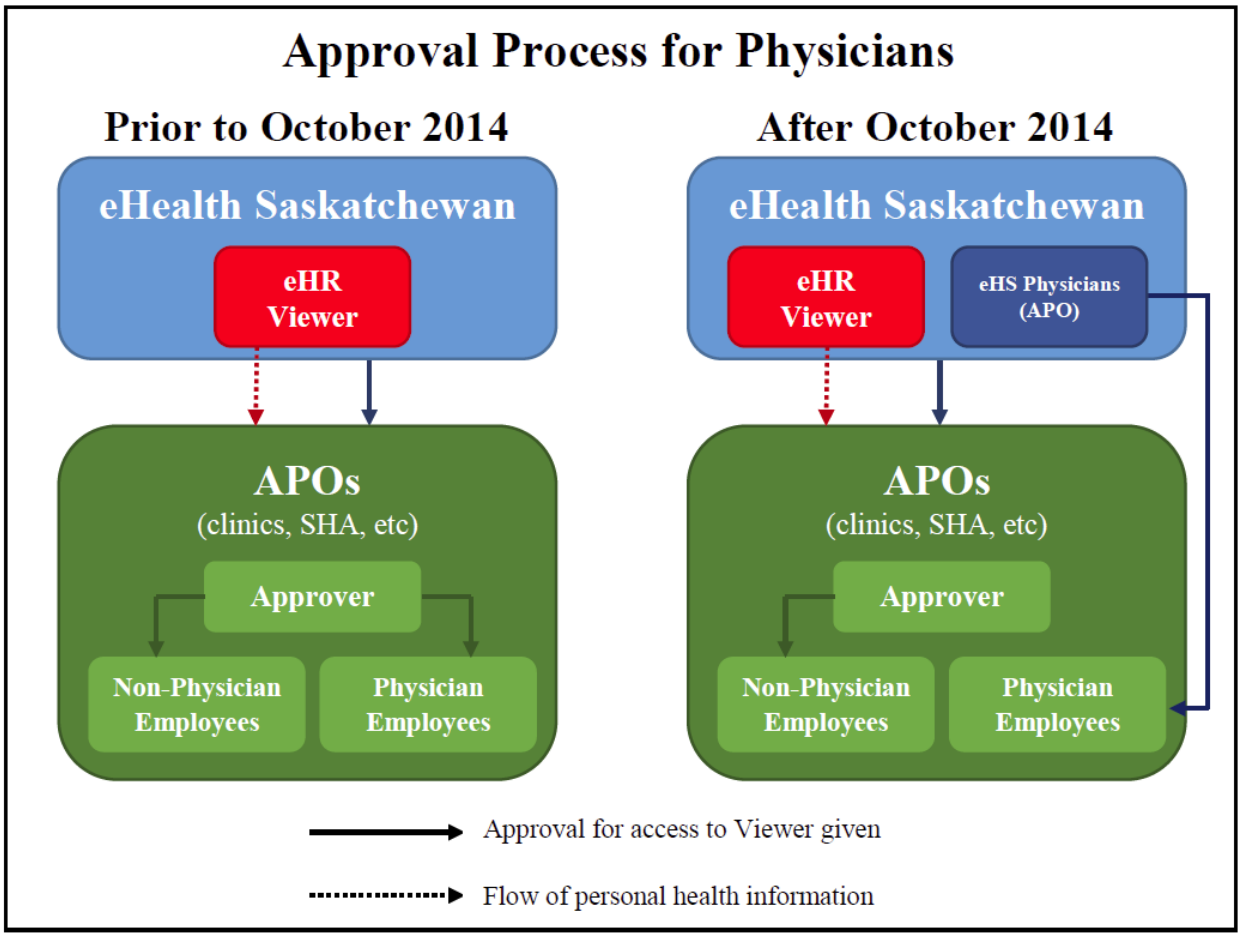
[42] I also note that a yearly purge of former users from the Viewer is not enough. Users that have gone to a different healthcare organization, or worse yet, left the field all together, should have access to personal health information of every person in this province revoked immediately. Otherwise, in some cases, that access can remain for up to a year. I recommend that eHealth work with its APOs to devise a more timely solution.

b. ***eHS Physicians***

[43] Dr. Furstenberg contacted eHealth on July 14, 2016 after he realized he no longer had access to the Viewer. eHealth explained the situation. On July 15, 2016, Dr. Furstenberg applied again for access under PAPHR and West Hill. On July 18, 2016, eHealth acknowledged the request and based on the information and sent PAPHR and West Hill a notice to either accept or reject Dr. Furstenberg's request. It also provided access under the APO eHS Physicians even though it was not requested by Dr. Furstenberg. eHealth indicated that if a physician requested access under a region or clinic specific organization, the physician will be provisioned under that organization as well as eHS Physicians.

[44] eHS Physicians is an APO created by eHealth in October 2014. It created 'borderless access for physicians'. Prior to October 2014, a physician, who was working under a

separate APO, would have to be approved by that APO. However, since creating eHS Physicians, physicians can be approved directly by eHealth. The diagram below depicts the approval process for physicians before and after October 2014.



[45] eHealth created eHS Physicians for a specific purpose. Prior to October 2014, it is my understanding that the regional health authorities and physicians were frustrated by the registration process to the Viewer. eHealth's submission states:

> In 2014, it was acknowledged that the new user approval process was a major barrier for timely physician access to the Viewer. The regional health authorities (now the Saskatchewan Health Authority, SHA) indicated that due to the contract nature of many of the arrangements with physicians in the province that the current approval process was not easily managed, nor did they feel they were the right approvers for this type of user. To address these concerns, eHealth began acting as the Approver for all physician requests to access the Viewer.

[46] eHealth's e-mail, dated October 21, 2014, indicated that reasons for this change included "Physicians are named Trustees under *The Health Information Protection Act* (HIPA) and are therefore individually responsible for the proper use and disclosure of personal health information." It also noted "Use cases for the majority of physicians show utilization of the eHR Viewer within multiple organizational settings where a provincial approval process is better suited."

[47] With respect, eHealth's analysis of trustees a defined by HIPA is not quite right. As per subsection 2(t)(xii)(A) of HIPA, a physician in good standing with CPSS ***can be*** a trustee because they are licenced pursuant to *The Medical Profession Act, 1981*. However, eHealth's analysis ignores the caveat built into subsection 2(t)(xii) which indicates that only "a person, other than an employee of a trustee" can be a trustee. HIPA does not define "employee", however, *The Freedom of Information and Protection of Privacy Act* (FOIP), another piece of privacy legislation to which eHealth is subject, defines employee as follows:

> 2(1) In this Act:
>
> …
>
> (b.1) "employee of a government institution" means an individual employed by a government institution and includes an individual retained under a contract to perform services for the government institution;

[48] I adopt this definition for my analysis of HIPA. This definition can apply to most relationships that physicians have with trustee organizations that they do not own.

[49] eHealth's analysis also ignores another factor, the personal health information in question must be in the custody or control of the physician in order to qualify as a trustee. eHealth qualifies as a trustee of the personal health information in the Viewer. When a physician accesses the personal health information, eHealth is disclosing it. If the physician is working on their own, or owns a clinic, that physician collects that personal health information. It is in the custody and control of that physician, who becomes the trustee of that information. However, when a physician is contracted by, or is an employee of, another trustee or healthcare organization, the collected personal health information is in the custody and control of the trustee organization and not the physician in question.

[50] Under any scheme, eHealth is responsible for ensuring that any disclosure of personal health information is made in accordance with HIPA. By setting up eHS Physicians, eHealth is disclosing personal health information to physicians who may not be trustees. Further, it is removing any control that some healthcare organizations have over the collection of personal health information from the Viewer made by physician employees.

[51] Further, eHealth's e-mail of October 21, 2014 indicated that CPSS would "act as the investigation and disciplinary body for complaints of inappropriate access to patient information within the eHR Viewer. As per their mandate, CPSS will respond accordingly to any complaint issued directly to them or through eHealth Saskatchewan to any inappropriate activity within the eHR Viewer." CPSS has authority to investigate inappropriate actions of physicians. In this case, CPSS investigated the actions of Dr. Furstenberg. It did not investigate the role that other physician APOs played in this role, nor did it have the authority to investigate the role of the SHA or eHealth in this breach.

[52] eHealth indicated that it had been alerted by CPSS on November 3, 2017 that it was investigating Dr. Furstenberg for unprofessional conduct and required information about patient profile views through the Viewer, made by Dr. Furstenberg, between January 1, 2014 and July 1, 2017. eHealth provided the Viewer audit reports to CPSS on November 15, 2017. On November 24, 2017, CPSS charged Dr. Furstenberg. My office found out about the charges through media reports on December 4, 2017. However, eHealth indicated it did not find out about the charges and the breach until my office notified them of my intention to undertake an investigation on February 12, 2018. Further, CPSS did not reveal to eHealth the identity of the individual to which Dr. Furstenberg admitted to accessing in the Viewer. This also hampered eHealth's investigation. It had no way of determining which accesses were authorized. Finally, without being formally told about the breaches by CPSS, Dr. Furstenberg's access to the Viewer was revoked on February 13, 2018.

[53] Through eHS Physicians, eHealth has created a system where they have little control over investigating breaches. Instead of having an APO being responsible for investigating questionable actions of physician employees, it indicated that CPSS would "respond

accordingly to any complaint issued directly to them or through eHealth Saskatchewan to any inappropriate activity within the eHR Viewer". eHealth has no authority over CPSS, but it does have a contractual relationship with APOs. In this case, it appears that eHealth was kept in the dark about Dr. Furstenberg's actions and was unable to contain the breach or investigate in a timely manner.

[54] Finally, as eHS Physicians created a 'borderless access' for physicians, this created unintentional consequences in the Viewer. It gave physicians who were approved under eHS Physicians access to personal health information under APOs who did not approve the physician. As will be discussed, Dr. Furstenberg was able to access personal health information in the Viewer under APOs that did not approve him.

c. ***SHA (PAPRHA)***

[55] Based on the information Dr. Furstenberg provided to eHealth on July 14, 2016, eHealth provisioned access under PAPRHA on July 18, 2016. PAPRHA granted him access to the Viewer on November 1, 2016.

[56] In its submission to my office, the SHA indicated that PAPRHA should not have approved Dr. Furstenberg for the Viewer. He had full privileges with PAPRHA from June 1, 2005 to approximately August 15, 2015 when his privileges were changed to 'limited' meaning it allowed for use of lab, diagnostic imaging, physiotherapy, and occupational therapy. Further, Dr. Furstenberg did emergency room shifts in one of PAPRHA's hospitals starting in December 2007 to 2008. However, he did not provide services for the region after that.

[57] That means that PAPRHA approved a physician in 2016 that had not worked in one of its facilities since 2008. It noted that Dr. Furstenberg did not fill out a form requesting access that was internal to PAPRHA's approval process.

[58] The SHA stated in its submission that "Physicians are to request access under the "eHR Physicians" organization, and not through the RHA".

*d. **West Hill Medical Clinic***

[59] Dr. Furstenberg applied for access to the Viewer on July 14, 2016 and eHealth also provisioned the request under West Hill. Dr. Furstenberg was working at West Hill for almost a year when he made this request.

[60] West Hill never approved Dr. Furstenberg as a user of the Viewer. However, because Dr. Furstenberg was approved under eHS Physicians, he was able to deliberately select West Hill when he logged in to the Viewer. This allowed him to choose West Hill as the APO when he logged in to the Viewer and accessed Individual 1's personal health information on July 19, 2016 even though West Hill did not approve him in the Viewer.

[61] Every access Dr. Furstenberg made in the Viewer under West Hill as the APO was unauthorized. I recommend that eHealth notify all other affected individuals, if any, of this breach.

*e. **J. J. Furstenberg Medical Prof Corp***

[62] On April 8, 2017, Dr. Furstenberg contacted eHealth to set up J.J Furstenberg Medical Prof Corp. as an APO for the Viewer. It took eHealth two days to do so. eHealth is unable to contact Dr. Furstenberg, who is the trustee, to determine if the accesses made under this APO into Individual 2's personal health information was authorized by HIPA.

*f. **Dr. L.N. de Beer Medical Professional Corporation***

[63] Dr. de Beer is part owner of South Hill. As noted, Dr. Furstenberg stopped working at South Hill in July 2015.

[64] Dr. Furstenberg applied for access to the Viewer under the de Beer Corporation on May 11, 2017. The de Beer Corporation never approved Dr. Furstenberg as a user of the Viewer.

[65] Dr. de Beer reports that he partners with a clinic in Montreal Lake First Nation where Dr. Furstenberg practiced during 2016 and 2017. Dr. de Beer is responsible for scheduling physicians, but the First Nation owns the clinic and the medical records.

[66] It is not clear why both South Hill and the de Beer Corporation are both APOs and what need there would be for an individual to be approved to access the Viewer by one or the other, or both. I recommend that eHealth and Dr. de Beer work together to clarify this situation.

[67] Although none of the accesses in question were under the de Beer Corporation, because Dr. Furstenberg was signed up under eHS Physicians, he could also log in to the Viewer under the de Beer Corporation. I recommend that eHealth investigate whether Dr. Furstenberg made any accesses under this APO and if so, notify affected individuals of this breach.

What other safeguards were in place with respect to Dr. Furstenberg's access to the Viewer?

[68] My Investigation Report 308-2017, 309-2017, 310-2017, issued earlier this year, also dealt with inappropriate accesses in the Viewer. In that Report, I analyzed many safeguards that eHealth had in place to protect personal health information in the Viewer. The following is a summary:

- eHealth has adopted a Joint Services/Access Policy (JSAP). APOs sign a "Request for Organization Approval" form that APOs sign when they apply for access. The "Request for Organization Approval" form and requires the APO to access data in accordance with HIPA and the JSAP. Individuals users must also agree to abide by the JSAP when they first log in. The JSAP indicates that:

    - eHealth is the trustee of personal health information, but outlines responsibilities of APOs;

    - APOs must approve or reject requests for user access to the Viewer;

    - APOs are responsible for appointing an employee to be the Authorized Approver within the APO who is responsible to manage and designate users and user roles with the eHR Viewer (subsection 5.1.2 (b) of JSAP);

- APOs are responsible for ensuring all users that they authorize have completed the necessary training on how to use the eHR Viewer, privacy and security training, and have signed a confidentiality oath or agreement (subsections 5.1.2(g) and 5.1.2(h) of JSAP);

- section 5.4 of the JSAP explicitly states that APOs and their authorized users are only to collect and use data on a need-to-know basis for an "Authorized Health Purpose", which is to support and or provide care to the patient to whom the information relates;

- users are also required to accept the JSAP before logging in to the Viewer for the first time. This signals agreement to comply with several terms of use, including:

  - collect and use the personal health information for the sole purpose of supporting or providing a healthcare service to the individual to whom the information relates;

  - only access and use the personal health information on a strict need to know basis to support or provide the healthcare service;

  - ensure appropriate safeguards are in place within the clinic or facility to protect the security and confidentiality of personal health information.

– eHealth has made a number of training resources, including documents and videos, for users and Authorized Approvers for APOs on how to use the eHR Viewer available on its website which covers:

  - that users are to only access the records of patients the user is directly providing care and treatment to, and they are not to access any other records for any other purpose;

  - highlights the offence provision within HIPA;

– When a user is granted access to the eHR Viewer and logs into the eHR Viewer for the first time, the user must 'accept' the eHR Viewer Training Declaration. This declaration is to confirm that the user has reviewed the eHR training resources on eHealth's website.

[69] I also note that the JSAP requires APOs to have safeguards in place. Section 5.1.2 of the JSAP requires APOs to have a privacy officer appointed and to have other, HIPA compliant, safeguards in place to protect personal health information collected from the Viewer. Therefore, I will determine if other APO's had the appropriate safeguards in place.

[70] South Hill provided my office with copies of its privacy policies and confidentiality agreements. South Hill indicated that they were created when it established its in house electronic medical record (EMR). The policies and procedures focus on the EMR and do not address access to personal health information from the Viewer. Dr. Furstenberg did not sign a confidentiality agreement with South Hill. Further, Dr. Furstenberg was simply required to read the policies and review eHealth's training material. No other training was offered by South Hill.

[71] South Hill does not have adequate privacy policies or procedures to meet the requirements of section 16 of HIPA. I recommend that South Hill revise its policies and procedures to address the Viewer, require its physicians to sign confidentiality agreements and enhance its training for its staff and physicians.

[72] Dr. de Beer has indicated that he has not signed a confidentiality agreement with the clinic in Montreal Lake First Nation. I recommend that Dr. de Beer take steps to ensure he is not the trustee of personal health information in that clinic. If so, I recommend he ensure there are safeguards in place to protect it.

[73] West Hill does not have customized policies, procedures or training. It relies on external resources to educate its medical office assistants such as a June 2006 letter from the Canadian Medical Protective Association and "Legislative Authority: Health Information Protection Act of Saskatchewan, 2003 (HIPA)". Further, it appears that West Hill does not have such expectations for staff physicians. Its submission stated: "All Physician's are encouraged to apply for the eHR Viewer… It would be assumed that Dr. Furstenberg would use the eHR Viewer appropriately and as required when he was working at our clinic."

[74] My office has noted in Investigation Report H-2013-003 that asking an employee to read a complicated privacy statute, and not to provide more instruction through simple and accessible tools and resources, is insufficient for HIPA compliance. Further, in Investigation Report LA-2013-001, my office stated that it is not enough for a trustee to adopt the policies or other resources of another organization, unless it has first ensured

those policies and procedures are tailored to meet the unique and specific needs of the trustee.

[75] Section 16 of HIPA requires that a trustee establish policies and procedures to maintain administrative, technical and physical safeguards. Relying on the work done by a separate organization is not adequate. West Hill does not have adequate privacy policies or procedures to meet the requirements of section 16 of HIPA. Further, as an APO, it has violated the requirements of the JSAP. I recommend that West Hill develop customized policies and procedures, require its physicians to sign confidentiality agreements and enhance its training for its staff and physicians.

[76] PAPRHA did have strong confidentiality policies in place during the period. This included a specific procedure on access to the Viewer. However, the SHA reported that the procedure was not followed. The employee of who approved Dr. Furstenberg could not provide an explanation. The SHA noted that it would be reviewing all physicians who were approved by PAPRHA for access to the Viewer.

Did eHealth, or any of the APOs, meet the duty to protect?

[77] I have several concerns with the accountability structure that has been created by eHealth with respect to giving APOs and users access to personal health information in the Viewer.

[78] First, it is important for eHealth to demand its APOs to have privacy policies, procedures and training programs that are compliant with section 16 of HIPA. However, it does not check to make sure they are in place. The JSAP states:

> As part of the sign-up process for access to the EHR Viewer, APOs will be required to complete eHealth's standard Privacy and Security Checklist. eHealth will be relying on the APO's answers to the questions in the Checklist as part of the criteria to determine whether the APO will be granted access to the EHR Data.

[79] eHealth relies on APOs to ensure they have the appropriate safeguards in place. However, it is clear that in this case, that some of the APOs did not.

[80] I recommend that eHealth develop a check list of specific safeguards that the JSAP requires APOs to have in place. This would include:

- customized privacy policies and procedures that address access to and personal health information collected from the Viewer;
- a privacy officer;
- HIPA compliant technical safeguards on all devices that will be used to access the viewer;
- annual HIPA training for all employees;
- a procedure to ensure all approved users of the viewer have taken eHealth training on an annual basis; and
- HIPA compliant physical safeguards.

[81] I recommend that eHealth have new APOs fill out the checklist and sign it before approving the APO's access. I recommend that eHealth have all existing APOs complete and sign the checklist within one year. I recommend that eHealth require APOs to sign and submit the checklist annually.

[82] Similarly, eHealth relies on users of the Viewer to review the privacy training material it has available. However, it cannot be certain that users have actually taken the training. I recommend that eHealth develop a solution to force users of the Viewer to take the training and to track which users have taken the training. Ideally, eHealth should require new users to take a training course with quizzes and the issuing of a certificate on an annual basis. eHealth has expressed that there are challenges to implementing that solution. At the very least, eHealth should find a technical solution to force users to take the training once a year before access to the viewer is permitted. It should also track which users have taken the training. The training should be required on an annual basis.

[83] I recommend that eHealth amend the JSAP to reflect these changes.

[84] I am also concerned with the creation of eHS Physicians as an APO. As noted, it was created as a result of an erroneous analysis of HIPA. eHealth reported that it was done partly because the new user approval process was a major barrier for timely physician access to the Viewer. I note that Dr. Furstenberg was approved by South Hill on the same day and it took two days for J.J. Furstenberg Medical Prof Corp to be approved as an APO.

My office asked eHealth if it had any statistics about how long it took physicians to gain access to the Viewer prior to October 21, 2014. It responded that its Change and Transition Unit did not have any such statistics.

[85] I am not persuaded that it is justified to bypass the APO system for physicians based on how long it takes, especially when eHealth's analysis of a trustee is wrong. A physician would only have to go through the approval process once when joining a new APO. It is worth the time it takes to go through an established process so that all of the parties have an opportunity to understand data flows from the Viewer and the accountability structure. In addition, it is a good opportunity to review safeguards in place.

[86] eHS Physicians is a solution to be convenient for physicians, but it misses the mark in terms of the protection of personal health information. It assumes that every physician is a trustee and does not take in to account who is actually trustee of the personal health information. As a result, it is a physician centric solution, not a patient centric solution. It is in a physician's best interest to take the time to familiarize themselves with privacy rules, structures and the privacy legislation that applies to them. In turn, it will benefit patients.

[87] Further, eHS Physicians has caused other unintended consequences in the Viewer; namely it allowed physicians to access personal health information under APOs that had not been given approval.

[88] I recommend that eHealth end the practice of approving physicians directly through eHS Physicians.

[89] One may argue that Dr. Furstenberg alone made the decision to access personal health information in the Viewer without proper authorization. However, the evidence shows that Dr. Furstenberg did not receive privacy training from any of the APOs discussed in this report. Further, eHealth cannot be sure the J.J. Furstenberg Medical Prof Corp had the proper safeguards in place or that Dr. Furstenberg actually went through the training material available. Dr. Furstenberg has access to the personal health information of every individual in this province and there was not effective safeguards in place.

[90] Finally, I am disappointed by the lack of rigor in removing access of users that should no longer have access to the Viewer. Even though eHealth found out that CPSS was investigating Dr. Furstenberg on November 3, 2017, it did not know the nature of the allegations. As a result, it was not able to remove Dr. Furstenberg's access to the Viewer until February 13, 2018. It is best practice to remove an individual's access to personal health information while investigating allegations of inappropriate behavior or when an individual is no longer working in the province. This is in part due to the issues I discussed at paragraphs [51] to [53]. Also, Dr. Furstenberg was no longer working for South Hill for six months before his access was cut off. The current policy has APOs checking once a year as to whether all approved users should still have access to the Viewer. This is insufficient.

[91] I recommend that eHealth amend the JSAP to require APOs to let eHealth know within a week if an approver should no longer have access to the Viewer. APOs are in the best position to know when an employee or a physician is no longer working for an organization, or in the province, and should no longer have access to the Viewer. This is another reason why it is important that non-trustee physicians be approved by the APOs they work for and not directly by eHealth. Nevertheless, eHealth can take an active role in monitoring the status of physicians. It reported that it receives updates from CPSS when there are changes to a physician's licence but admitted it does not have a procedure to monitor and take action when required. I recommend that eHealth set up a protocol to proactively determine if physician's access to the Viewer should be revoked if their medical licence changes.

[92] I am not satisfied that eHealth had adequate safeguards in place to protect the personal health information of Individuals 1 and 2. I am also not satisfied that South Hill, West Hill or the de Beer Corporation have adequate safeguards in place to comply with HIPA.

4. Did eHealth respond appropriately to the privacy breach?

[93] 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

[94] eHealth reported that it contained the breach on February 13, 2018 when it disabled Dr. Furstenberg's account and access to the Viewer. This is a positive step, however, eHealth was first made aware of potential concerns with Dr. Furstenberg by CPSS on November 3, 2017. It did not become aware of the charges until February 12, 2018.

[95] I recommend that eHealth discuss the situation with CPSS and come to an agreement on how to handle future physician privacy breaches involving personal health information in eHealth's custody and control.

Notify affected individuals

[96] eHealth reported that it notified individuals 1 and 2 on May 28, 2018.

[97] I also recommend that eHealth work with South Hill to identify further affected individuals of any unauthorized accesses Dr. Furstenberg made in the Viewer after he left South Hill. I also recommend that eHealth identify and notify any individuals that Dr. Furstenberg accessed under the APOs of the de Beer Corporation and West Hill that did not approve him for access.

Investigate the Breach / Write a privacy breach report

[98] eHealth investigated the breach and provided a privacy breach report to my office. The contents have been discussed in this report.

Prevent Future Breaches

[99] eHealth is working on the following action items in response to its investigation of the breach:

1. Implement an operational procedure to ensure Access Management Services is notified of changes to physician license statuses.
2. Investigate and configure the eHS Physicians organization so it no longer provides borderless access to physicians. Ensure physicians, approved under eHS Physicians, require approval to access the Viewer under APOs.
3. Test to ensure that physicians can no longer access APOs that have not been approved by an Authorized Approver.
4. Identify and fix a number of discrepancies that exist within the Viewer account registration process.
5. Fix the Current Account List report, sent to Authorized Approvers through eHealth's User Access Recertification Procedure, to ensure Authorized Approvers validate the continued need-to-know access for all users listed in the report.
6. Ensure the User Access Recertification Policy is reviewed to ensure the policy is accurate and current.
7. Review and update the Viewer JSAP.
8. Mandate training and the re-accepting of JSAP declaration on an annual basis.
9. Remind APO's of their responsibility to audit and monitor the View use of their approved users.
10. Notify the College of the second privacy breach.

[100] I recommend that eHealth implement these measures. I find that eHealth responded to the breach appropriately.

III FINDINGS

[101] I find that eHealth did not have adequate safeguards in place to protect the personal health information of Individuals 1 and 2.

[102] I find that South Hill, West Hill and the de Beer Corporation do not have adequate safeguards in place to comply with HIPA.

[103] I find eHealth responded adequately to the breach.

IV RECOMMENDATIONS

[104] I recommend that eHealth work with its APOs to devise a more timely solution to identify approved users that should no longer have access to the Viewer and revoke access.

[105] I recommend that South Hill revise its policies and procedures to address the Viewer, require its physicians to sign confidentiality agreements and enhance its training for its staff and physicians.

[106] I recommend that eHealth and Dr. de Beer work together to clarify if both South Hill and the de Beer Corporation should be APOs.

[107] I recommend that Dr. de Beer take steps to ensure he is not the trustee of personal health information in the clinic at Montreal Lake First Nation. If so, I recommend he ensure there are safeguards in place to protect it.

[108] I recommend that West Hill develop customized policies and procedures, require its physicians to sign confidentiality agreements and enhance its training for its staff and physicians.

[109] I recommend that eHealth develop a checklist of specific safeguards that the JSAP requires APOs to have in place. I recommend that eHealth have new APOs fill out the checklist and sign it before approving the APO's access. I recommend that eHealth have all existing APOs complete and sign the checklist within one year. I recommend that eHealth require APOs to sign and submit the checklist annually.

[110] I recommend that eHealth develop a solution to force users of the Viewer to take the privacy training and to track which users have taken the training.

[111] I recommend that eHealth end the practice of approving physicians directly through eHS Physicians.

[112] I recommend that eHealth amend the JSAP to reflect these changes.

[113] I recommend that eHealth discuss the challenges it had investigating these breaches with CPSS and come to an agreement on how to handle future physician privacy breaches involving personal health information in eHealth's custody and control.

[114] I recommend that eHealth set up a protocol to proactively determine if physicians' access to the Viewer should be revoked if their medical licence changes.

[115] I also recommend that eHealth work with South Hill to identify further affected individuals of any unauthorized accesses Dr. Furstenberg made in the Viewer after he left South Hill. I also recommend that eHealth identify and notify any individuals that Dr. Furstenberg accessed under the APOs of the de Beer Corporation and West Hill that did not approve him for access.

[116] I recommend that eHealth implement the action plan it identified in its investigation report.

Dated at Regina, in the Province of Saskatchewan, this 6th day of December, 2018.

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