Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 168-2024, 177-2024, 178-2024, 179-2024

Andrew Gilbertson carrying on business under Hill Avenue Drugs Ltd.
University of Saskatchewan
Ministry of Health
eHealth Saskatchewan

September 6, 2024

Summary: Mr. Andrew Gilbertson, the University of Saskatchewan College of Pharmacy and Nutrition (U of S), eHealth Saskatchewan (eHealth), and the Ministry of Health (Health) proactively reported that a 4th year PharmD student/intern completing an experiential learning rotation at Hill Avenue Drugs Pharmacy in Regina inappropriately accessed the personal health information of 114 individuals. The inappropriate accesses were in the Pharmaceutical Information Program (PIP) and the electronic Health Record (eHR) Viewer. The A/Commissioner investigated the incidents and had a number of findings including that the four parties did not appropriately handle the privacy breaches in accordance with the four best practice steps. Specifically, investigating the breaches for root causes and setting out a comprehensive plan for prevention. The A/Commissioner made a number of recommendations including that within 30 days of issuance of the Investigation Report, the U of S amend its *Student Placement Agreement*, and Mr. Gilbertson develop policies and procedures in compliance with section 16 of *The Health Information Protection Act*. Further, the A/Commissioner recommended that going forward eHealth provide access to the eHR Viewer under the Approver Organization associated to the site rather than the U of S. Finally, the A/Commissioner recommended that within 30 days of issuance of the Investigation Report, Health, eHealth and the U of S review the current understanding of responsibility for supervision, protection of personal health information in the systems and the roles of each party in the event of a privacy breach for future placements.

I BACKGROUND

[1] Between June 25, 2024, and July 4, 2024, Mr. Andrew Gilbertson, the University of Saskatchewan College of Pharmacy and Nutrition (U of S), eHealth Saskatchewan (eHealth), and the Ministry of Health (Health) contacted my office to proactively report that a year 4 PharmD student completing an experiential learning rotation at Hill Avenue Drugs Pharmacy (the "pharmacy") in Regina inappropriately accessed personal health information of others. The accesses were via the Pharmaceutical Information Program (PIP) and the electronic Health Record (eHR) Viewer of people that were not under the care of the pharmacy, and that the student had no professional reason to access.

[2] On June 26, 2024, Mr. Andrew Gilbertson from the pharmacy contacted my office to advise that the student was dismissed, and the breach was currently contained.

[3] On July 5, 2024, my office sent notifications to the pharmacy, the U of S, Health and eHealth advising that my office would be investigating the matter. My office requested that all four parties provide my office with a completed *Privacy Breach Questionnaire* provided by my office and other documentation by August 5, 2024. Between July 29, 2024, and August 30, 2024, all four parties provided the requested materials which included answers to several follow-up questions of my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction to investigate this matter and which Acts are engaged?

[4] In order for my office to investigate this matter, I must have jurisdiction. In order to have jurisdiction, one or more of the three Acts my office oversees must be engaged. Based on the organizations involved in this matter, I will consider if *The Health Information Protection Act* (HIPA) and/or *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) are engaged.

Is HIPA engaged?

[5] HIPA is engaged when there are three elements present: 1) personal health information, 2) a trustee, and 3) the trustee has custody or control over the personal health information. Below is an analysis to see if these three elements are present and if HIPA is engaged.

[6] For the first element, the eHR Viewer allows users to view the following types of information:

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

(www.ehealthsask.ca/services/her-viewer)

[7] PIP allows users to view the following types of information:

- Medication profiles of individuals
- Allergy/intolerance information
- Prescriptions

(www.ehealthsask.ca/pip)

[8] The information available to view in the eHR Viewer and PIP constitute personal health information pursuant to subsection 2(1)(m) of HIPA which provides:

> **2**(1) In this Act:
>
> ...
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

[9] In eHealth's submission to my office, it indicated that the student accessed laboratory results, hospital visit information, electronic medical record visit information, immunization information, clinical documents, medical imaging reports and prescription information.

[10] Therefore, the first element is present for HIPA to be engaged.

[11] For the second element, I have previously found that both Health and eHealth qualify as trustees for purposes of HIPA in Investigation Reports 103-2018, 105-2019, 106-2019 at paragraph [17] and 413-2019, 414-2019, 415-2019 at paragraph [15].

[12] For Hill Avenue Drugs Ltd. my office conducted an Information Services Corporation corporate registry search. The proprietor and majority shareholder for Hill Avenue Drugs Ltd. appears to be Andrew Gilbertson (Mr. Gilbertson). Mr. Gilbertson is also a pharmacist licensed pursuant to *The Pharmacy and Pharmacy Disciplines Act*. Mr. Gilbertson provided my office with a copy of his *Proprietary Pharmacy Permit* issued by the Saskatchewan College of Pharmacy Professionals which was valid from December 1, 2023, to November 30, 2024. In addition, to the HIPA provisions listed below, subsection 2(1)(t)(xv) of HIPA points to *The Health Information Protection Regulations, 2023* (HIPA Regulations). These provisions of HIPA provide as follows:

2(1) In this Act:

…

> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (ix) a proprietor as defined in *The Pharmacy and Pharmacy Disciplines Act*;
>
> …
>
> (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;
>
> …
>
> (xv) any other prescribed person, body or class of persons or bodies;

[13] For subsection 2(1)(t)(xv) of HIPA, subsection 4(b) of the HIPA Regulations provides that every person who owns or operates a privately-owned facility in or from which health services are provided by a health professional, qualifies as a trustee. This provision would also apply to Mr. Gilbertson. Subsection 4(b) of the HIPA Regulations provides as follows:

> **4** for the purposes of subclause 2(1)(t)(xv) of the Act, the following are prescribed as trustees:
>
> …
>
> (b) every person who owns or operates a privately-owned facility in or from which health services are provided by a health professional;

[14] Therefore, Mr. Gilbertson qualifies as a trustee as defined by subsections 2(1)(t)(ix) and (xii)(A) of HIPA and subsection 4(b) of the HIPA Regulations.

[15] It should also be noted that subsection 2(1)(b) of the HIPA Regulations also defines an "employee". This will be relevant throughout this Investigation Report as it pertains to the student on rotation at Hill Avenue Pharmacy. Subsection 2(1)(b) of the HIPA Regulations provides:

> **2**(1) In these regulations:
>
> …
>
> **"employee"** means:
>
> …

> (b) an individual who, with the authorization of a trustee, acts on behalf of the trustee with respect to personal health information and for the purposes of the trustee, and not for the individual's own purposes, whether or not the individual has the authority to bind the trustee, is paid by the trustee or is remunerated by the trustee;
>
> but does not include a health professional who is retained under a contract, that is not an employment agreement, to perform services for the provincial health authority;
>
> …

[16] Based on subsections 2(1)(t)(ix), (xii)(A) and (xv) of HIPA and subsection 4(b) of the HIPA Regulations, there are three trustees involved. Therefore, the second element is met for HIPA to be engaged.

[17] For the third element, "custody" is the physical possession of a record by a trustee with a measure of control. "Control" connotes authority. Personal health information is under the control of a trustee when the trustee has the authority to manage the information, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control to be present (Investigation Report 306-2019 at paragraphs [15] to [16]).

[18] I have previously found that Health has custody and control of the personal health information in PIP in several review and investigation reports including Investigation Reports H-2010-001 at paragraph [8] and 282-2016 at paragraph [10]. I have also previously found that eHealth has custody and control of the personal health information in the eHR Viewer in several previous review and investigation reports including Investigation Report 413-2019, 414-2019, 415-2019 at paragraphs [16] to [18].

[19] Further, in my office's Investigation Report H-2010-001 at paragraph [89], I found that every time a pharmacist views personal health information in PIP, it is a disclosure by Health and a collection by the pharmacist. I have also found the same when it comes to the eHR Viewer in my Investigation Report 308-2017, 309-2017, 310-2017 at paragraphs [19] and [20].

[20] In this case, the student was accessing the personal health information in PIP and the eHR Viewer at Mr. Gilbertson's pharmacy. Based on the definition of an "employee" at subsection 2(1)(b) of the HIPA Regulations, the student would qualify as an employee of Mr. Gilbertson and was authorized by Mr. Gilbertson to act on his behalf with respect to personal health information in PIP and the eHR Viewer.

[21] Therefore, Mr. Gilbertson would have had custody with a measure of control over the personal health information at issue.

[22] Based on the above analysis, all three trustees in this case were involved in collecting and/or disclosing the personal health information at issue. Therefore, I find that all three trustees had custody or control over the personal health information.

[23] In conclusion, HIPA is engaged for the aspects of this investigation involving Mr. Gilbertson, Health and eHealth.

Is LA FOIP engaged?

[24] The U of S does not fit the definition of a "trustee" as defined at subsection 2(1)(t) of HIPA. However, it does qualify as a "local authority" as defined by subsection 2(1)(f)(xi) of LA FOIP.

[25] The U of S had a role in the placement of the student at the pharmacy which I will address later in this Investigation Report. Since the U of S is a local authority but not a trustee, I find that only LA FOIP, and not HIPA, is engaged for the aspects of this investigation involving the U of S and its role in placement of the student. This is consistent with my findings in Investigation Report 308-2017, 309-2017, 310-2017 at paragraph [18] which involved the U of S College of Medicine and a breach of the eHR Viewer.

2. Did a privacy breach occur?

[26] Personal health information must be collected, used and/or disclosed in accordance with HIPA. To do otherwise, may be a breach of privacy.

[27] The need-to-know principle is the principle that trustees, and their staff should only collect, use, and/or disclose what is necessary for the diagnosis, treatment or care of an individual or other purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 of HIPA, which provides:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
> …
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[28] Section 24 of HIPA restricts the collection of personal health information by trustees as follows:

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[29] The student's placement started May 6, 2024, until he was escorted out of the pharmacy on June 25, 2024. Based on the submission from the pharmacist, Mr. Gilbertson, on June 24, 2024, the student was overheard speaking to himself saying "oh – he is still alive". The student was asked who he was reviewing and he quickly shutdown a number of patient searches. Following an audit, it was determined the student was looking up patients that were not customers/patients of the pharmacy. The snooping started five days into the student's placement. It should be noted that eHealth confirmed for my office that the student was logging into PIP and the eHR Viewer using his own log-in credentials.

[30] It also appeared most of the student's views were of those with a shared ethnicity, similar interests, age groups or recognizable names within the province. All four parties concluded that the student appeared to be looking up individuals' personal health information out of curiosity and not a legitimate business purpose or need-to-know.

[31] I agree with this conclusion. This constitutes 'snooping'. Further, these reasons for access are not in accordance with sections 23 or 24 of HIPA. Accessing personal health information in PIP and the eHR Viewer for reasons beyond job duties is inappropriate and in violation of HIPA. Each access by the student for these reasons constituted a breach of privacy.

[32] Based on the submission from eHealth and its attached audit report, it appears the student accessed the personal health information of 16 individuals in the eHR Viewer during his placement.

[33] Based on the interim and final submissions from Health, it appears the student accessed the personal health information of 108 individuals in PIP during his placement.

[34] After confirming the numbers with eHealth on August 29, 2024, there were a total of 371 inappropriate access or breaches of privacy between both systems impacting 114 individuals. Therefore, I find there were 371 breaches of privacy in this case.

3. To what extent are the trustees and the local authority responsible for these breaches?

[35] As stated earlier in this Investigation Report, Health is the trustee responsible for PIP and eHealth is the responsible trustee for the eHR Viewer. However, the analysis does not end there. In this case, a U of S student was inappropriately accessing PIP and the eHR Viewer at the pharmacy, so it goes beyond just overall responsibility for these systems and an isolated case of snooping. It is also about how access to the systems were provisioned to the student, the extent of the student's access and who was responsible for supervision.

How access to the systems were provisioned to the student

[36] Prior to gaining access to PIP and the eHR Viewer, students must complete a number of things via their program through the U of S. According to the submission from the U of S, prior to placement at a pharmacy and prior to gaining access to PIP and the eHR Viewer, students go through the following preparations:

- Students register as an intern with the Saskatchewan College of Pharmacy Professionals.
- When a student is at the 4th year level, like the student involved in this matter was, there are various competencies expected for that level. 4th year students must demonstrate that they have the ability to practice as a new pharmacist entering practice. The competencies expected are derived from the Association of Faculties of Pharmacy of Canada *Educational Outcomes* and the National Association of Pharmacy Regulatory Authorities *Professional Competencies for Canadian Pharmacists at Entry to Practice*. This student would have been well aware of these expectations and required competencies.
- Students sign the U of S confidentiality agreement annually. The U of S provided my office with a copy of the most current signed agreement of this student dated April 29, 2024.
- The *Procedures for Concerns with Pharmacy and Nutrition Student Professional Behavior* outlines expected behaviors for all students. In this case, the student had these reiterated during an orientation course in April 2024.
- Students are required to review the *Experiential Learning Handbook* and are required to sign a *Self-declaration* that they have reviewed and understood the contents of the handbook.

- Students are required to complete both PIP training and eHR Viewer training as part of the program, both of which address privacy and confidentiality expectations and requirements. Students *Self-declare* their completion and understanding of the requirements necessary to access and utilize each system. All training and documentation must be completed prior to access to the systems.

- Students are required to watch a recorded *HIPA* training video and sign a *Self-declaration* upon completion.

[37] Naturally, the next steps are to gain access to PIP and the eHR Viewer prior to placement in a pharmacy. To better understand what this process looked like for the student in this case, my office requested the U of S, Health, and eHealth explain the steps.

Access to PIP

[38] PIP is a centralized online system that is updated when drugs are prescribed and/or dispensed to persons in Saskatchewan. Health care providers rely on the information available in PIP to make decisions about a patient's health care, including what medications to prescribe to avoid drug interactions. Inaccurate information in an individual's PIP profile could lead to harmful and even fatal decisions by health care providers (Investigation Report 103-2018, 105-2019, 106-2019 at paragraph [30]). Therefore, it is imperative to protect against unauthorized access to this sensitive information.

[39] For access to PIP, the U of S provided the following:

- The student's placement started on May 6, 2024.

- Once students are placed at a particular site, both the student and site are notified.

- There are no formal agreements that occur with each placement. There is an overarching perpetual agreement with the site to place students called a *Student Placement Agreement*.

- For PIP, the student reaches out to their assigned site 2-3 weeks prior to starting their placement. The manager at the site approves access to PIP. The site manages the termination of the access. For each rotation at a different site, the student does the same.

- The role of the U of S is to provide students with the links to training and to ensure they complete the training. The U of S does not have a role in providing access to PIP.

[40] The U of S indicated it did not have a role in providing the student access to PIP. Therefore, as Health is the trustee responsible for PIP, my office requested Health explain the steps involved for this student's access to PIP. Health indicated that the student already had an active PIP account from a prior work placement so the Approver, Mr. Gilbertson, would have linked the student to the pharmacy in PIP. Health's records show that Mr. Gilbertson (or the pharmacy) linked the student on May 6, 2024.

[41] My office followed up again with Health to gain further understanding of the active PIP account. Health advised that the student self-registered for a PIP account and completed the *PIP Basic User Training* on September 4, 2021. Further, including the pharmacy, the student was linked and unlinked three times with two sites between September 14, 2021, and June 25, 2024, for internships (twice at Shoppers Drug Mart and once at the pharmacy) as per the table below:

User Organization:	Address:	Start Date (linked by Approver):	End Date (Unlinked by Approver):
Shoppers Drug Mart #2465	4- 4420 Rochdale Boulevard Regina SK S4X 4N9	14-Sep-21	16-Jan-22
Shoppers Drug Mart #2465	4- 4420 Rochdale Boulevard Regina SK S4X 4N9	27-Jun-22	24-Jul-22
Hill Ave Drugs Pharmacy	3410 Hill Avenue Regina SK S4S 0W9	6-May-24	25-Jun-24

[42] So, it appears with each placement, the site links the student to the site's PIP account and unlinks the student at the end of the internship. Further, it appears that the student's PIP account remains active until formally closed. My office followed up with eHealth with regard to whether PIP can be accessed from anywhere. eHealth confirmed that PIP is a web-based application and can be accessed from anywhere. However, in order to access any personal health information within PIP, the user must be linked to a User Organization.

[43] Each trustee that participates in PIP must have a designated Approver who approves User accounts for their organization (linking). According to Health, the Approver for the student in this case was Mr. Gilbertson. Mr. Gilbertson signed a *Joint Service & Access Policy* (JSAP) on May 17, 2011. The JSAP sets out the responsibilities and rules for collection, use, and disclosure of personal health information in PIP. Health provided my office with a copy of the JSAP in place with Mr. Gilbertson. Section 5.1.2 of the JSAP signed by Mr. Gilbertson states as follows:

> **5.1.2 Collection, Use and Disclosure of PIP Data**
> …
> Each User Organization accepts responsibility for ensuring that authorized Users comply with this Policy and do not improperly use or disclose the PIP Data.

[44] In addition to the JSAP, section 16 of HIPA sets out a trustee's duty to protect personal health information in its custody or control. Section 16 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:
>
> (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.

[45] Section 16 of HIPA is one of the most important features of the Act. Without comprehensive written policies and procedures, the risk that a trustee will fall short of its many statutory responsibilities is dramatically increased.

[46] When asked what safeguards were in place at the pharmacy, including policies and procedures, Mr. Gilbertson, in his submission to my office, indicated that he "would like this to be answered by the University of Saskatchewan College of Pharmacy and Nutrition". Further, the pharmacy reviews "privacy with all new hired staff" and the pharmacy has always "trusted that privacy has been addressed and committed to at the level of" the U of S. No policies and procedures were referenced or provided to my office, so I am unable to assess what this trustee has in place for safeguards pursuant to section 16 of HIPA.

[47] All parties in this matter have a role in the protection of personal health information. Mr. Gilbertson appears to be of the view that the U of S was responsible for the student and the protection of the personal health information within PIP despite the JSAP in place between Health and Mr. Gilbertson. This responsibility for PIP is spelled out in the JSAP. Regardless of whether it is a student placement or another employee or the pharmacist himself, Mr. Gilbertson is responsible for how PIP is accessed within the pharmacy as agreed to in the JSAP.

[48] In terms of the U of S, it provided my office with a copy of its *Student Placement Agreement* signed by Mr. Gilbertson on February 14, 2018. From a review of that agreement, it does not appear to clearly spell out the role of the U of S or the pharmacy in the event a student violates HIPA while in a pharmacy placement. If it expects to place students in pharmacies where the trustee, like Mr. Gilbertson, provides access to a system they are responsible for, the U of S should have responsibilities and expectations spelled out in this agreement so confusion around responsibility does not occur again in the future. I recommend the U of S amened this agreement with Mr. Gilbertson and all trustees going forward so it spells out how such situations will be handled and what the expectations/responsibilities of the U of S and the trustee in such situations will be. To view this as an isolated incident would be naïve and short sighted. Inappropriate access has likely occurred with prior students in other placements elsewhere and will likely occur again. Clear lines of responsibility and supervision will be needed for all student placements at all sites.

[49] As it is not clear what policies and procedures Mr. Gilbertson has in place at the pharmacy that apply to staff and students accessing PIP, I must conclude that he is not in compliance with section 16 of HIPA and must develop said policies and procedures immediately. In addition, I recommend the U of S not place any further students at this pharmacy until these policies and procedures are in place and the U of S and Mr. Gilbertson are clear on the roles of each organization in protecting the personal health information in PIP. The supervision and auditing of student access to PIP (and the eHR Viewer) should be built into the policies and procedures. I will address supervision later in this Investigation Report.

Access to the eHR Viewer

[50] The eHR Viewer is a system or database that brings personal health information together from various sources such as pharmacies and physicians. It standardizes and organizes the information for presentation on a client-centric basis. It offers system to system integration or a web-based viewer. It contains laboratory test results, prescription drug information, clinical documents, including discharge summaries, immunization information, chronic disease information and additional clinical information as added from time to time (from template JSAP provided by eHealth at p. 2).

[51] For access to the eHR Viewer, the U of S provided the following:

- For the eHR Viewer, access at any non-hospital site is solely arranged with the site outside of the PharmD program, as the U of S only provides access for hospital-based rotations. It is at the discretion of the [pharmacy] whether or not to provide access for the student during their time there.

- The role of the U of S is to provide students with the links to training and to ensure they complete the training. The U of S does not have a role in providing access, other than for hospital-based rotations requiring access to the eHR Viewer.

[52] The U of S indicated it did not have a role in providing the student access to the eHR Viewer. Therefore, as eHealth is the trustee responsible for the eHR Viewer, my office

requested eHealth explain the steps involved for this student's access to the eHR Viewer and any agreement signed with the student. eHealth indicated the following:

- eHealth does not have an agreement signed by the student as part of their access to the eHR Viewer.

- For background, when a new user requests access to the eHR Viewer, the request is transferred to eHealth's Access Management Services (AMS) Unit to provision access. The new user is provisioned access under an Authorized Provider Organization (APO), who then must have their access accepted or rejected by an Authorized Approver (Approver) of the APO. The Approver is accountable for the actions of its users and is required to ensure personal health information is used only on a need-to-know basis for the authorized purpose under the eHR Viewer Joint Services/Access Policy (JSAP).

- In this case, the College of Pharmacy and Nutrition was set up as an APO and became the Approver of pharmacy students in April 2020. When the student requested access to the eHR Viewer, AMS provisioned access under the College of Pharmacy and Nutrition and the request was accepted by the Approver.

- While the student did not sign an agreement as part of their eHR Viewer access, they did accept three acknowledgements the first time they logged in to the eHR Viewer. First, acceptance of the terms and conditions; second, they declared that they had completed eHR Viewer training; and third, they accepted a reminder regarding appropriate use. The acknowledgements were accepted on May 28, 2024.

[53] eHealth provided my office with a copy of the organizational request form it received from the College of Pharmacy and Nutrition (U of S) to be set up as an APO. It was dated April 17, 2020. From a review of the request, there is one designated authorized Approver at the College of Pharmacy and Nutrition at the U of S. The form indicates that Approvers will receive an email request to verify that members of the U of S, specifically the College of Pharmacy and Nutrition, who request access to the eHR Viewer ("Users") are allowed to have access. In bold letters on the request form, it states "**The Approved Organization and the Approver are accountable for the actions of Users.**" [Emphasis in original].

[54] The U of S appears to be unclear of its responsibilities in terms of the eHR Viewer and how this student was approved for access. The U of S has indicated it had no role, yet its own Approver accepted the student's request for access. Mr. Gilbertson has a JSAP in place with eHealth for the pharmacy's access to the eHR Viewer, but this student was not set up

under Mr. Gilbertson. The U of S should have had no role in the provision of access to PIP or the eHR Viewer.

[55] Going forward, eHealth should provide access to the eHR Viewer only under the APO associated to the site rather than the U of S (except hospital-based rotations which I have not assessed in this investigation). In this case, it would be more appropriate to have had Mr. Gilbertson approve the student's access under Mr. Gilbertson's APO as he is responsible for ensuring the protection of the personal health information in the eHR Viewer and direct supervision of the student on site. I recommend eHealth make this change going forward for all students placed in non-hospital rotations.

What was the extent of the student's access to the systems?

[56] None of the parties addressed the extent of the student's access to personal health information in PIP or the eHR Viewer. Safeguarding the systems can include limiting access for authorized users to only what is needed to get the job done. Full access may not be necessary. Students may only need access to portions of PIP and the eHR Viewer for a successful rotation. It is not clear if the U of S, Health or eHealth have considered this.

[57] My office reached out to eHealth to request confirmation of the student's full access in the system and if limiting student access to only what is needed is an option going forward. eHealth advised that for PIP, students are assigned the "Viewer" user role, which means they have the ability to view demographic information, create patient lists and view all medication profiles. However, it is important to note that when a user conducts a patient search in PIP, the user is taken to a patient confirmation screen to verify they have selected the individual to whom they are providing health care services. On the patient confirmation screen, the user must select a reason for accessing the medication profile and select the patient confirmation button. Once the patient has been confirmed, the user is taken to the patient medication profile. Regarding this student, our records indicate that he selected "dispensing" as the purpose for accessing the medication profiles of the 108 individuals who were not patients of the pharmacy.

[58] For the eHR Viewer, eHealth advised that students are assigned the "View Profile" role, which means they have the ability to view demographic information and eHR Viewer profiles only in the case of unmasked patients. This role does not have the ability to view masked patients eHR Viewer profiles.

[59] On the question of whether limiting student access is an option, eHealth advised that PIP and the eHR Viewer are provincial views of patient information and user access cannot be restricted to the patients of an Approved Organization. It is the responsibility of each Approved Organization to ensure that its users access and use information only on a need-to-know basis to provide or support patient care. I appreciate eHealth's assistance throughout this investigation. It has been very responsive to my office's requests. Understanding the student's access highlights why supervision and random user audits are so important.

Who was supervising the student?

[60] I applaud Mr. Gilbertson and his staff for catching the student in the act of inappropriately accessing personal health information in the systems and for taking almost immediate action. Had this not occurred, the breaches would have been ongoing. However, it is clear in this particular case that supervision of access to PIP and the eHR Viewer should be by Mr. Gilbertson as he has ultimate responsibility for what occurs in his pharmacy and has agreed to protecting the personal health information in both systems under JSAPs with Health and eHealth. In addition, as noted earlier in this Investigation Report, subsection 2(1)(b) of the HIPA Regulations defines an "employee" of a trustee. The student, in this case, would fit the definition of an employee of Mr. Gilbertson for purposes of HIPA.

[61] All parties should be on the same page going forward in terms of what supervision of future student placements will look like. The Saskatchewan College of Pharmacy Professionals has a policy in place titled, *Supervision of Pharmacy Interns* and dated September 14, 2021. The U of S provided my office with a copy of this policy, and it is available online at the Saskatchewan College of Pharmacy Professionals' website. The policy states:

POLICY

1. Responsible Supervisor

1.1. **The responsibility of providing supervision is by default the pharmacy manager**.

1.2. The pharmacy manager may delegate the responsibility of providing supervision to one or more supervising members if those individuals agree.

1.3. The supervising member must be competent in the activity being supervised.

1.4. The supervising member must ensure the standards of practice are met at all times by the supervised individual.

STANDARDS OF PRACTICE

2. Responsibilities of the Supervisor

…

2.3. The supervising member is responsible for the actions performed by the pharmacy intern.

2.4. The supervising member, providing direct supervision, must be able to:

2.4.1. observe and check each action performed by the pharmacy intern;

2.4.2. perform the activity being supervised; and

2.4.3. promptly intervene or stop the actions of the pharmacy intern when necessary.

[Emphasis added]

[62] On July 6, 2024, Mr. Gilbertson provided a copy of his Proprietary Pharmacy Permit #0158, where he is listed as a Pharmacy Manager (valid 12/01/2023 to 11/30/2024). Above, the policy indicates that providing supervision is by default the pharmacy manager. The policy was in place when the student was at the pharmacy so Mr. Gilbertson should have been aware of the responsibility, he had for supervision of the student which included their access to personal health information in PIP and the eHR Viewer.

[63] For future placements, the U of S should be clearer in its *Student Placement Agreements* about responsibility and supervision in terms of breaches under HIPA as noted earlier in

this Investigation Report. Further, eHealth should be setting students up under the appropriate APO that is responsible for supervision and communicating as such to the site for the eHR Viewer.

[64] I recommend the U of S, Health, and eHealth review the current understanding of responsibility for supervision, protection of personal health information in the systems and the roles of each party in the event of a privacy breach. The understandings should be in writing in either agreements or policies and procedures, so all parties are clear.

4. Were the privacy breaches appropriately handled?

[65] In circumstances where a trustee proactively reports a privacy breach to my office, my office will consider whether the trustee appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the trustee took the privacy breach seriously and appropriately addressed it. My office recommends four best practice steps be taken when a trustee discovers a breach of privacy has occurred. These are:

- Contained the breach (as soon as possible)
- Notified affected individuals (as soon as possible)
- Investigated the breach
- Taken steps to prevent future breaches

(*Rules of Procedure*, updated August 2023 at p. 34)

[66] I will consider the appropriateness of the handling of the matter by all four parties against these four best practice steps.

Contained the breach (as soon as possible)

[67] Upon learning that a privacy breach has occurred, a trustee should immediately take steps to 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 to personal health information.
- Correcting weaknesses in physical security.

[68] Effective and prompt containment reduces the magnitude of a breach and the risks involved with personal health information being inappropriately accessed.

[69] On June 24, 2024, staff of Hill Avenue Drugs Inc., claim to have overheard the student speaking to himself while in front of his computer. According to the submission from Mr. Gilbertson, the student was overheard saying "Oh – he is still alive". When the student was asked who the student was reviewing, the student quickly shut down several patient searches. On June 25, 2024, Mr. Gilbertson was advised. Mr. Gilbertson conducted an audit of the student's searches, and it appeared several searches were of patients that were not with Hill Avenue Drugs Inc. Mr. Gilbertson contacted the U of S on June 25, 2024, and the student was removed from the site the same day.

[70] The U of S contacted Health and eHealth to revoke the student's access to PIP and the eHR Viewer. Both were revoked June 26, 2024, and June 27, 2024, respectively. However, the parties were unable to determine if the student made paper copies of the records accessed.

[71] On June 26, 2024, the U of S and Mr. Gilbertson notified my office.

[72] All parties acted swiftly and removed the student from the pharmacy and revoked access to the systems within a reasonable timeline. This stopped additional breaches from occurring. I find that all parties responded appropriately to contain the breaches.

Notified affected individuals (as soon as possible)

[73] Notifying an individual that their personal health information was inappropriately accessed is important for several reasons. Not only do individuals have a right to know, but they also need to know to protect themselves from any potential harm that may result from the inappropriate access. Unless there is a compelling reason not to, trustees should always notify affected individuals. An effective notification should include:

- A description of what happened (a general description of what happened).
- A detailed description of the personal health information involved (e.g., name, medical record, etc.).
- A description of the types of harm that may possibly come to them because of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to change a health services number).
- Contact information of an individual within the organization who can answer questions and provide information.
- A notice that individuals have a right to complain to the IPC.
- Recognition of the impacts of the breach on affected individuals and an apology.

(*Privacy Breach Guidelines for Trustees,* updated August 2022, p. 4)

[74] In addition to notifying individuals, trustees may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee professions.

[75] On July 11, 2024, eHealth, Health, and Mr. Gilbertson mailed joint notification letters to 109 affected individuals (five letters were not sent as individuals were deceased and no next of kin contact information was available). The U of S provided an additional letter that was included in the joint notification which included an apology from the U of S.

[76] Normally, my office would recommend that notification to affected individuals only come from the responsible trustee. However, in this case, due to the involvement of all of the parties and the roles of Health and eHealth with PIP and the eHR Viewer, it was appropriate for a joint notification letter with a supplement from the U of S.

[77] My office reviewed the template for the three different notification letters. The three types were one for those only affected by PIP access, one for those only affected by eHR Viewer access, and one for those affected by access to both systems. All three template letters contained the elements noted above. The letters also contained a form and process to request audit reports of who has accessed the individuals' personal health information in PIP and/or the eHR Viewer.

[78] The notification letters were sent out very quickly after the breaches were contained. This is positive. I also note that my office has received no formal complaints from any affected individuals.

[79] I also note that the parties notified my office and engaged my office early in the process for guidance.

[80] Mr. Gilbertson and the U of S notified the Saskatchewan College of Pharmacy Professionals (SCPP) as the regulatory body. All PharmD students/interns must be registered with SCPP.

[81] Based on the above, I find that notification to affected individuals was appropriately handled.

[82] There is one exception to this finding. Mr. Gilbertson advised my office that he contacted a known friend of one of the affected individuals who then contacted the affected individual via text message. This was inappropriate and would constitute a breach of privacy for that affected individual. The third party did not have a need-to-know that this individual was

the victim of a privacy breach. In future, Mr. Gilbertson should contact all affected individuals directly instead.

Investigated the breach

[83] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The investigation should address the incident on a systemic basis and should include a root cause analysis. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred which helps inform how to prevent future breaches at step 4.

[84] A root cause analysis should include a consideration of section 16 of HIPA, which sets out the trustee's duty to protect personal health information. For LA FOIP, the equivalent obligations are found in section 23.1.

[85] Unfortunately, I find that the parties did not investigate the breaches beyond a conclusion that the root cause of the breaches was snooping and the student not following clear expectations or their training. While this was definitely a root cause, none of the parties appear to have considered other significant factors at the level of how access was provisioned to the student, the extent of the student's access to these systems or who was responsible for supervision. My office had to request this information from the parties after the fact, which I address in the third discussion issue above in this Investigation Report. Further, some of the parties did not appear to have considered obligations under section 16 of HIPA. If it was considered, it was not provided to my office.

[86] In conclusion, I find that the parties did not fully investigate the root causes of these breaches. In the future, I recommend the parties consider the broader issues when dealing with cases of snooping in systems. To only focus on the actions of the snooper, opportunities for improvement and to prevent future breaches may be missed. To view snooping in isolation from the environment that may have provided the opportunity to snoop would be shortsighted. I will address this further in the next section.

Taken steps to prevent future breaches

[87] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone but a trustee can learn from one and improve its practices. To avoid future breaches, a trustee should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[88] In its submission to my office, the U of S indicated that no changes at the University level would occur in terms of its policies and procedures. It did indicate it would provide stronger messaging and communication about the expectations at the start of the academic year for all students. It may also explore changes to its policy around dismissal from the program for intentional privacy breaches. It should be noted that the student's PharmD rotation was immediately terminated, a failing grade was awarded and the student has not been allowed to continue on in the PharmD program. These are appropriate steps by the U of S. I also recommend the U of S work with Health and eHealth to ensure that it has no role in the provisioning of access to PIP and the eHR Viewer for students. In addition, it clarifies the supervision expectations of students in its *Student Placement Agreements*, which should include how privacy breaches involving students will be handled.

[89] eHealth indicated it would work with the U of S to establish a process to conduct random user audits for students approved for eHR Viewer access. Further, a note was placed on this student's profile to indicate that any clinical application request by the student must be assigned to the eHealth Privacy Unit for review. eHealth recommends retraining for the student and a reread and acceptance of the terms of the site's JSAP should a request be received for access for the student. The student would also be subject to additional monitoring of their eHR Viewer use to ensure compliance in the future if access is given.

[90] Health indicated that it would be reviewing the current PIP training content to ensure it is sufficient. Health will also explore requiring PIP users to revisit the privacy training on an annual basis. As it currently stands, students only have to take the *PIP Basic User Training*

once and not each time they are linked to a new organization. This student took the *PIP Basic User Training* on September 4, 2021. Ongoing training is a requirement of section 5 of the HIPA Regulations. Health did not indicate that it would establish a process to conduct random user audits for students approved for PIP access. I recommend it do so.

[91] Mr. Gilbertson advised that his pharmacy has an *Employee Privacy* Pledge that all hired staff sign. Going forward, Mr. Gilbertson advised that he intends to have students also review and sign this pledge. He provided a copy of the pledge to my office. My office reviewed it, and it contains the elements required by subsection 5(b) of the HIPA Regulations. He also indicated that he will be informing future students of what the pharmacy experienced and that he will be reviewing student access to PIP during their rotation. Further, Mr. Gilbertson indicated that if breaches of this nature occur again with future students, his pharmacy will not participate in student placements from the U of S.

[92] All of the above steps being taken by the parties are positive. In particular, the random user audits of future students as noted by eHealth. I recommend Health and eHealth get this in place as soon as possible for both PIP and the eHR Viewer. In my office's Investigation Reports H-2010-001 involving L & M Pharmacy, the former Commissioner recommended random audits be done on a sustained basis of activities in PIP. I have also previously recommended eHealth proactively conduct random audits on users of the eHR Viewer to ensure compliance with HIPA (see for example paragraph [130] of Investigation Report 161-2018).

[93] In summary, the parties need to go further with preventative measures. Some additional recommendations are:

- The U of S work with Health and eHealth to ensure that it has no role in the provisioning of access to PIP and the eHR Viewer for students. In addition, it clarifies the supervision expectations of students in its *Student Placement Agreements*, which should include how privacy breaches involving students will be handled.

- Health and eHealth establish a process to conduct random user audits for students approved for PIP and eHR Viewer access as soon as possible.

[94] In conclusion, I find that the parties have not sufficiently set out a plan for prevention in terms of future students accessing personal health information in PIP and the eHR Viewer.

III FINDINGS

[95] I find that HIPA is engaged for the aspects of this investigation involving Mr. Gilbertson, Health and eHealth.

[96] I find that HIPA is engaged for the aspects of this investigation involving Mr. Gilbertson, Health and eHealth.

[97] I find that only LA FOIP, and not HIPA, is engaged for the aspects of the investigation involving the U of S and its role in placement of the student.

[98] I find I have jurisdiction to undertake this investigation.

[99] I find that there were 371 privacy breaches impacting 114 individuals.

[100] I find that Mr. Gilbertson is not in compliance with section 16 of HIPA.

[101] I find that the parties did not appropriately handle the privacy breaches in accordance with the four best practices steps. Specifically, investigating the breaches for root causes and setting out a comprehensive plan for prevention.

IV RECOMMENDATIONS

[102] I recommend that within 30 days of issuance of this Investigation Report, the U of S amend its *Student Placement Agreement* with Mr. Gilbertson and all trustees going forward so it spells out how privacy breaches will be handled and what the expectations/responsibilities of the U of S and the trustee are in such situations.

[103] I recommend that within 30 days of issuance of this Investigation Report, Mr. Gilbertson develop policies and procedures in compliance with section 16 of HIPA. Said policies and procedures should include supervision and auditing of student access in PIP and the eHR Viewer on site.

[104] I recommend that, going forward, eHealth provide access to the eHR Viewer only under the APO associated to the site rather than the U of S (except hospital-based rotations).

[105] I recommend that within 30 days of issuance of this Investigation Report, the U of S, Health, and eHealth review the current understanding of responsibility for supervision, protection of personal health information in the systems and the roles of each party in the event of a privacy breach with future placements. The understandings should be in writing in either agreements or policies and procedures, so all parties are clear.

Dated at Regina, in the Province of Saskatchewan, this 6th day of September, 2024.

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