Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 036-2025, 046-2025, 047-2025, 049-2025, 091-2025

Ashish Patel
Niravkumar Patel
University of Saskatchewan
Ministry of Health

July 7, 2025

Summary: In 2024, a 4th year University of Saskatchewan (U of S) student who was enrolled in the College and Nutrition Doctor of Pharmacy program (PharmD) snooped into the personal health information of 114 individuals at Hill Avenue Drugs Pharmacy during their experiential learning rotation (rotation) that year. This led eHealth Saskatchewan (eHealth) to audit the student's access to the Ministry of Health's (Health) Pharmaceutical Information Program (PIP) during their rotation at Shoppers Drug Mart #2466 (Shoppers) in 2021 and 2022. eHealth provided the PIP audit reports to Health, which confirmed the student had improperly accessed PIP in their second rotation in July of 2022. Health confirmed with the current pharmacist at Shoppers that the majority of the student's unauthorized accesses were *not* on a need-to-know basis. In other words, the student inappropriately accessed personal health information in PIP. Health proactively reported the snooping to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

The Commissioner made several findings, including that 70 privacy breaches occurred in total, that Health's notice to the affected individuals was inadequate, and that the U of S's current method of evaluating students' ability to maintain privacy and confidentiality is insufficient.

The Commissioner made several recommendations, including: 1) Health contact the affected individuals and offer an apology and acknowledgment of the breach including a right to complain to OIPC; 2) U of S apply increased rigour in evaluating student access to personal health information to ensure privacy and confidentiality; 3) Health ensure the current pharmacist/owner of Shoppers has established policies and procedures to maintain administrative, physical and technical safeguards to protect

personal health information in accordance with the *Joint Service & Access Policy* and section 16 of HIPA; and 4) Health require PIP users to take PIP training on an annual basis.

I BACKGROUND

[1] On September 6, 2024, the Office of the Information and Privacy Commissioner (OIPC) issued Investigation Report 179-2024 into a matter involving a 4th year student enrolled into the College of Pharmacy and Nutrition, Doctor of Pharmacy (PharmD) program at the University of Saskatchewan (U of S). The student was completing an experiential learning rotation (rotation) at Hill Avenue Drugs Pharmacy in Regina. In that case, it was found that during the period May 6th to June 25th, 2024, the student had inappropriately accessed the personal health information of 114 individuals in the Ministry of Health's (Health) Pharmaceutical Information Program (PIP) by means of the eHealth Saskatchewan's (eHealth) electronic Health Record (eHR) Viewer. The Hill Avenue Drugs Pharmacy proactively reported this privacy breach to this office the day after the discovery, June 26, 2024.

[2] As a result of the breaches discussed in Investigation Report 179-2024, Health requested, and received, an audit report from eHealth regarding the same student's earlier rotations at Shoppers Drug Mart #2466 (Shoppers) in Regina during 2021 and 2022. Health received the audit report on October 29, 2024. It was then learned that the student had begun to snoop on the personal health information of individuals even before the matters discussed in Investigation Report 179-2024. Those matters form the basis of this Investigation Report.

[3] The student's first rotation spanned from September 14, 2021 to January 16, 2022. The second rotation, that is the subject matter of this report, involved 26 days from June 27, 2022, to July 22, 2022. The audit report revealed the student inappropriately accessed the PIP database during the second rotation. At the time of the student's rotations, the proprietor of Shoppers was 102089349 Saskatchewan Ltd. The majority shareholder of 102089349 Saskatchewan Ltd. was Ashish Patel. As of the date of this investigation, the

proprietor of Shoppers was Yavit Pharmacy Ltd. The majority shareholder of Yavit Pharmacy Ltd. is Niravkumar Patel.

[4] On January 15, 2025, Niravkumar Patel confirmed the inappropriate nature of the student's accesses with Health during the second rotation.

[5] In total, the student made 70 inappropriate accesses, or snoops, into the personal health information of 51 individuals.

[6] On February 5, 2025, the Health proactively reported this matter to OIPC.

[7] On April 29, 2025, OIPC notified Health, U of S, Ashish Patel, Niravkumar Patel and the student that OIPC was undertaking an investigation. OIPC invited all parties to provide a submission.

[8] On May 2, 2025, U of S provided a submission to OIPC.

[9] On May 5, 2025, Health provided its submission to OIPC.

[10] On May 27, 2025, Ashish Patel provided a submission to OIPC.

[11] On May 29, 2025, Niravkumar Patel provided a submission to OIPC.

[12] The student did not provide a submission.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction to investigate this matter and which Acts are engaged?

[13] Based on the nature of the various organizations involved in this matter, the application of *The Health Information Protection Act* (HIPA) and/or T*he Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) must all be considered.

a. Is HIPA engaged?

[14] HIPA is engaged when three elements are 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 HIPA is engaged.

i. First element – personal health information

[15] For the first element, PIP allows users to view the following types of information with respect to the citizens of Saskatchewan:[1]

- Medication profiles;
- Allergy/intolerance information; and
- Prescriptions (past and present).

[16] The information on PIP constitutes "personal health information" pursuant to section 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;

[1] See eHealth's webpage *Pharmaceutical Information Program* (PIP) at https://www.ehealthsask.ca/services/pip.

(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;

[17] The first element is present for HIPA to be engaged.

ii. Second element – trustees

[18] For the second element, OIPC must determine if Health, Ashish Patel and Niravkumar Patel qualify as trustees under HIPA.

Health

[19] In past reports, OIPC found that Health is the trustee responsible for PIP pursuant to section 2(1)(t)(i) of HIPA, which provides: [2]

2(1) In this Act:

...
(t) **"trustee"** means any of the following that have custody or control of personal health information:

(i) a government institution;

Ashish Patel

[20] Ashish Patel, a pharmacist licensed pursuant to *The Pharmacy and Pharmacy Disciplines Act,* was the majority shareholder of 102089349 Saskatchewan Ltd. during the time of the students' second rotation (June/July 2022). The corporate entity, 102089349 Saskatchewan

[2] See OIPC Investigation Report H-2010-001 at paragraph [89]; OIPC Investigation Report 042-2017 at paragraph [2]; OIPC Investigation Report 103-2018, 105-2019, 106-2019 at paragraph [30]; OIPC Investigation Report 179-2024 at paragraph [40].

Ltd., was the proprietor of Shoppers, according to a "Proprietor Pharmacy Permit" issued by the Saskatchewan College of Pharmacy Professionals (SCPP) from December 1, 2021 to December 1, 2022. Therefore, Ashish Patel qualifies as a trustee pursuant to section 2(1)(t)(ix), (xii) and (xv) of HIPA, which provides:

> **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;

[21] With regard to section 2(1)(t)(xv) of HIPA, section 4(b) of *The Health Information Protection Regulations, 2023* (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;

[22] In essence, Ashish Patel was a pharmacist and the manager of Shoppers during the material time. As such, they qualify as a trustee in this matter pursuant to section 2(1)(t) (ix), (xii) and (xv) of HIPA and section 4(b) of HIPA Regulations.

Niravkumar Patel

[23] Niravkumar Patel, a pharmacist licensed pursuant to *The Pharmacy and Pharmacy Disciplines Act*, is the majority shareholder of Yavit Pharmacy Ltd. Yavit Pharmacy Ltd is the current proprietor of Shoppers, according to a "Proprietary Pharmacy Permit" issued by the Saskatchewan College of Pharmacy Professionals (SCPP) for the time period December 1, 2024 to November 30, 2025. Therefore, Niravkumar Patel qualifies as a trustee pursuant to sections 2(1)(t) (ix) and (xii) of HIPA.

[24] Since Health, Niravkumar Patel and Ashish Patel qualify as trustees, the second element is present for HIPA to be engaged.

iii. Third element – the trustees must have custody or control over the personal health information

[25] For the third pillar of analysis, this office must determine whether the trustees had custody or control of the personal health information in issue. "Custody" is the physical possession of a record by a trustee combined 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.[3]

[26] In past reports, OIPC found that Health has custody and control of the personal health information in PIP.[4] Therefore, there will be a finding that Health has custody and control of the personal health information in PIP.

[27] Further, as OIPC has found in past investigation reports, whenever a pharmacist views personal health information in the PIP database, that is considered a "disclosure" by Health and a "collection" by the pharmacist.[5]

---

[3] See OIPC Investigation Report 306-2019 at paragraphs [15] to [16].

[4] See OIPC Investigation Report H-2010-001 at paragraph [8]; OIPC Investigation Report 282-2016 at paragraph [10]; OIPC Investigation Report 179-2024 at paragraph [18].

[5] See OIPC Investigation Report H-2010-001 at paragraph [89].

[28] In this case, when the student was completing the second rotation at Shoppers, they were an "employee" of Ashish Patel, as defined by section 2(1)(b) of the HIPA Regulations.

[29] When the student accessed personal health information in the PIP database at Shoppers during their second rotation in June/July 2022, they were collecting personal health information on Ashish Patel's behalf. Therefore, Ashish Patel had custody with a measure of control over the personal health information at issue.

[30] Therefore, there will be a finding that Ashish Patel had custody and control over the personal health information.

[31] Since Health has custody and control over the personal health information and Ashish Patel also had custody and control, then the three elements are present for HIPA to be engaged.

[32] Since Niravkumar Patel became the proprietor of Shoppers long after the student had completed the second rotation, then Niravkumar Patel did not have custody or control over the personal health information at issue. However, Niravkumar Patel assisted Health in its investigation of this matter and must be considered in terms of preventing similar privacy breaches in the future.

b. Is LA FOIP engaged?

[33] U of S is not a trustee as defined by section 2(1)(t) of HIPA; however, it is a "local authority" as defined by section 2(1)(f)(xi) of LA FOIP.

[34] U of S had a role in the placement of the student at Shoppers. Since the U of S is a local authority, LA FOIP is engaged for this aspect of the analysis.[6]

[35] Both HIPA and LA FOIP are engaged. OIPC has jurisdiction to undertake this investigation.

[6] See OIPC Investigation Report 179-2024.

2. Did privacy breaches occur?

[36] A privacy breach occurs when personal health information is collected, used and/or disclosed without authority under HIPA.

[37] As noted above, a pharmacist "collects" personal health information when they view information in the PIP database. Section 2(1)(b) of HIPA defines "collect" as:

> **2**(1) In this Act:
>
> ...
> (b) **"collect"** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;

[38] When a trustee collects personal health information, they must do so in accordance with the "need-to-know principle" as set out in section 23 of HIPA. The need-to-know principle provides that trustees, *and their employees*, 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. Section 23 of HIPA provides, in part:

> **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.

[39] Further, 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.

[40] The U of S submission stated that the student's second rotation involved 26 days, between June 27, 2022, to July 22, 2022. However, according to the PIP audit report, the student continued accessing PIP up to, and including, July 25, 2022. July 25, 2022, is a significant date. This was the date the student was formally disconnected from the PIP database.

[41] Health received confirmation from Niravkumar Patel that there were 70 audit breach events. In each audit breach event the student inappropriately accessed the profiles of 51 individuals. In some instances, the student accessed the personal health information of some individuals more than once.[7] The audit report revealed that these individuals were not clients of Shoppers. Neither did they receive medication from Shoppers during the time period of the audit report. Without a doubt, the student lacked a legitimate business purpose and did not possess a valid need-to-know basis to access the profiles of the 51 snooped individuals. The student's actions constitute a clear violation of sections 23 and 24 of HIPA. Each of the 70 audit events is a privacy breach. There will be a finding that 70 privacy breaches occurred by means of unauthorized snooping.

[7] Of the 51 individuals whose privacy was violated in June/July 2022, the student continued to snoop on the personal health information of some of the same individuals during their later placement at Hill Avenue Drugs in 2024 – 28 people in all. The second snoop breach at Hill Avenue Pharmacy occurred when the student was enjoying a 4th year U of S College of Pharmacy placement in 2024.

3. Did U of S and the trustees (Health and Ashish Patel) respond to the privacy breaches appropriately?

[42] There are several determinants of whether a local authority or a trustee's response to a privacy breach is appropriate. Sections 6-7 and 7-7 of OIPC's *Rules of Procedure* sets out these considerations as follows:

a) Was the breach contained;

b) Were the affected individuals notified;

c) Was the breach investigated; and

d) Were appropriate steps taken to prevent future breaches.

[43] This office must now consider the role played by the U of S, Health and Ashish Patel with respect to the student's rotation and the provision of access to the PIP database.

U of S Role in Student Privacy Training

[44] U of S requires students of the PharmD program to engage the following:

- Register as an intern with the Saskatchewan College of Pharmacy Professionals.
- Sign an annual confidentiality agreement.
- Review the Experiential Learning Handbook and sign a self-declaration on a yearly basis indicating they have understood the contents of the handbook.
- Complete PIP training.
- Complete the PHAR 112.1 Pharmacy Law course. This course outlines pharmacists' professional, ethical and legal obligations within provincial and federal frameworks, including the duty of patient confidentiality and the privacy of personal health information. This must be completed in the first year of the PharmD program.

- Become familiar with and adopt the competencies outlined the Association of Faculties of Pharmacy Canada (AFPC) *Educational Outcomes* and the National Association of Pharmacy Regulatory Authorities (NAPRA) *Professional Competencies for Canadian Pharmacists at Entry to Practice*.

- Become familiar with and adopt the *Procedures for Concerns with Pharmacy and Nutrition Student Professional Behaviour*.

- Complete self-assessments at the mid-point and end of placements, which requires the student to address whether they personally maintained privacy and confidentiality "at all times".

[45] U of S also has a *Student Placement Agreement* with Shoppers, effective November 14, 2016. This agreement sets out the responsibilities of U of S and Shoppers regarding the placement of students, so students can gain structured and professional practice experience. However, the agreement is seriously defective in that it did not speak to the responsibilities or obligations of either the U of S or the trustee in the event of a privacy breach. This issue is discussed later in this ruling.

Health and Ashish Patels' Roles in Access to PIP

[46] PIP is accessed via a web-based application. To access the personal health information of a citizen of Saskatchewan contained within the PIP database, the user must be linked to a "User Organization".[8] Once associated with a User Organization, the user is then presented with a "patient confirmation screen". The patient confirmation screen appears and allows the user to search for individuals. Once at that screen, users *must* provide a legitimate reason for accessing a patient's medication profiles.

[47] The *Joint Service & Access Policy* (JSAP) is a policy document between Health and eHealth Saskatchewan (eHealth). This policy sets out the responsibilities for organizations using PIP and the rules for the collection, use and disclosure of personal health information contained in PIP. Section 5.1.4 of JSAP establishes eHealth as Health's information management service provider (IMSP) for PIP.

[8] Schedule A of the JSAP defines "User Organization" as "a clinic, pharmacy, RHA or other organization outside the Ministry with user rights into PIP".

[48] eHealth's website provides that individuals who wish to register for a PIP user account must first complete training modules. These modules include privacy and security training. The modules must be completed prior to registration for a PIP user account. In order to complete registration, the individual must sign a self declaration that they have viewed the required privacy and security training videos. Once registered, a User Organization must link the individual's PIP account to their organization so that the user can gain access to the personal health information in the PIP database.

[49] Ashish Patel signed a JSAP confirmation document on November 6, 2019. This signified that Ashish Patel reviewed and accepted the JSAP and that Shoppers is a registered User Organization.

[50] The student completed the privacy and security training modules on September 4, 2021 and registered for a PIP user account on that date. Ashish Patel linked the student's PIP user account to Shoppers on June 27, 2022. Ashish Patel unlinked the student's PIP user account on July 25, 2022, three days after the completed their rotation.

[51] What follows is an analysis of the response to the breach.

(a) Containment of the Breach

[52] Upon learning that a privacy breach has occurred, a local authority or trustee should immediately take steps to contain the breach. These steps will depend entirely on the nature of the breach, but they may 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.

[53] OIPC applies a standard of reasonableness to assess the containment of a breach. The institution must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals within a reasonable consideration.[9]

[54] The privacy breaches in this matter went undetected for two years. It was not until June 26, 2024, when the student was placed at Hill Avenue Drugs Pharmacy, that the pharmacist there learned of the privacy breaches at that location and swiftly revoked the student's access to PIP.[10] When Health and eHealth audited the student's past accesses to PIP the disturbing privacy breaches that form the subject matter of this report came to light.

[55] Logic dictates that the revocation of the student's access to PIP must result in a finding that the privacy breaches were contained thanks to the swift action of the Hill Avenue Pharmacist. It must also be noted that the offending student was not allowed to continue in the PharmD program and received a failing grade. Still, the fact that the student's snooping went undetected for two years is an issue that must be addressed by means of recommendations dealing with future prevention.

(b) Notification of Affected Individuals

[56] It is best practice for local authorities and trustees to inform affected individuals as soon as possible when personal information and/or personal health information has been breached. This is an obvious and crucial step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps they deem necessary to protect themselves.[11] An effective notification should include:[12]

[9] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [23].

[10] The student's inappropriate accesses into PIP and the eHR Viewer while at Hill Avenue Drugs Pharmacy is discussed in Investigation Report 179-2024.

[11] *Ibid*, at paragraph [34].

[12] See OIPC Investigation Report 179-2024 at paragraph [73].

- 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 OIPC.
- Recognition of the impacts of the breach on affected individuals and an apology.

[57] On February 5, 2025, Health notified 48 of the 51 affected individuals of this privacy breach by letter. Health indicated that 3 affected individuals were deceased and it did not have information regarding next of kin or personal representatives.

[58] This office's review of the Health letter reveals that it contains helpful information, including instruction on how to access the audit report. The audit report would reveal details of the privacy breach.

[59] Unfortunately, the letter does not inform individuals of their right to complain to OIPC. During this investigation, this office asked Health why it did not inform all the affected individuals of their right to complain. Health indicated that it did not do so because that information "was provided in the previous letter regarding the Hills Avenue Breach". This is unsatisfactory. Not all of the 51 affected individuals were involved in the subsequent snooping breaches at the Hill Avenue Drugs Pharmacy. Sadly, 23 affected individuals were never informed of their statutory right to complain to this office and to have input towards an investigation and review.

[60] Most distressingly, the letter from Health does not include an apology. Failure to include an acknowledgement of the tremendous negative impact of these breaches upon the citizens of Saskatchewan only amplifies the public's loss of trust in the provincial government's failure to safeguard their precious personal health information.

[61] There will be a finding that Health's notice to the affected individuals was inadequate. There will be a recommendation that Health contact the affected individuals once again to inform them of their right to complain to OIPC as well as to recognize the impact of these privacy breaches in the form of an apology.

(c) Investigation of the Breach

[62] Local authorities and trustees *must* conduct an investigation in the wake of a privacy breach. This is effected to learn the root of the breach and to prevent a future occurrence. The investigation must address the incident on a systemic basis and include a root cause analysis. Local authorities must consider their "duty to protect" pursuant to section 23.1 of LA FOIP. This section of the legislation requires local authorities to establish policies and procedures to maintain administrative, technical and physical safeguards. Section 23.1 of LA FOIP provides:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[63] Trustees must consider their "duty to protect" pursuant to section 16 of HIPA, which requires trustees to establish policies and procedures to maintain administrative, technical and physical safeguards.[13] 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.

[64] We now review the safeguards that U of S, Health, and Ashish Patel had in place at the time of the snooping.

U of S

[65] Earlier in this Investigation Report, OIPC summarized U of S's role in setting out its privacy expectations in the experiential learning program. Based on a review of materials, including the *Experiential Learning Handbook*, it is evident that U of S explicitly communicates to their students that personal health information must be accessed only on a need-to-know basis.

[66] However, OIPC has identified three areas in which U of S can improve its safeguards. The first is with respect to the university's confidentiality agreements.

[13] See OIPC Investigation Report 253-2024, 033-2025 paragraph [40] and OIPC Investigation Report 179-2024 at paragraph [83].

[67] U of S provided OIPC with copies of the confidentiality agreements signed by the student throughout their time in the PharmD program. The confidentiality agreements were signed by the student on August 27, 2021, June 14, 2022, March 29, 2023, August 28, 2023, and April 29, 2024.

[68] These confidentiality agreements are comprehensive, and the preamble admirably states the law in this province. But there is one defect. Because the agreements were created by the Saskatchewan Health Authority (SHA) for SHA employees, they are generic. There should be a provision in the signed part of the agreement that describes the student's placement. To be truly effective, the party signing this agreement must self-identify and proclaim that it is their individual placement that is subject to a confidentiality agreement.[14] There will be a finding that the U of S confidentiality agreement is insufficient for experiential learning rotations.

[69] U of S provided OIPC with a blank copy of its new *Experiential Learning Student Privacy and Confidentiality Pledge*. This pledge is specific to a student's experiential learning rotations. In its submission, U of S indicated that U of S has now implemented its *Experiential Learning Student Privacy and Confidentiality Pledge* and students are currently required to review it and sign. There will be a finding that U of S has taken the appropriate step of requiring students to review and sign the *Experiential Learning Student Privacy and Confidentiality Pledge*.

[70] The second area where improvement is needed is with respect to the university's role in supervising students and ensuring they observe the health privacy laws of this province. The U of S provided this office with the student's self-assessment in this case. The self-assessment included the following statement: "Privacy and confidentiality are maintained at all times". The student responded with a simple "Yes". We now know nothing could have been further from the truth. The student was allowed to self-regulate and, in this case, that was a privacy disaster.

[14] See Saskatchewan Health Authority's Policy Directive Number SHA-07-003.

[71] U of S clearly needs to be more involved in its supervision and evaluation of students during their experiential learning rotations. In its submission, U of S indicated that it updated its preceptor training modules to include a reminder that preceptors now must regularly audit student access to PIP. This is a positive step forward. However, we do not think it is enough.

[72] There will be a finding that the U of S current method of student evaluation in the PharmD program is insufficient. There will be a recommendation that U of S become much more involved in its program of student evaluation in the PharmD program. This could include the university college requiring pharmacists to obtain PIP audits throughout the rotation of every student. A regular audit would allow a sponsoring pharmacist to be assured of the legitimacy of a student's access for the entire duration of a rotation. Students would know that they were being audited. Had a measure such as this been in place in this case, there would likely be no need to cite the names of two independent pharmacists in this Investigation Report.

[73] This office previously found deficiencies in the *Student Placement Agreement* between the U of S and the pharmacist at Hill Avenue Pharmacy Drugs in 2024. Specifically, the agreement failed to clearly spell out the roles of the pharmacy or the U of S in the event of a student violation of HIPA during the course of a placement. In that investigation, OIPC recommended that U of S amend its *Student Placement Agreement* to clearly spell out how privacy breaches will be handled in the future and the expectations/responsibilities of U of S and the trustee. In that matter U of S indicated to OIPC that it would review and revise student placement agreements going forward to clarify expectations with respect to student supervision and the protection of privacy.

[74] Needless to say, the *Student Placement Agreement* with Shoppers does not speak to the roles and responsibilities of U of S and Shoppers if and when a student violates HIPA. OIPC expects that as a part of its response to OIPC's previous recommendation, that U of S is currently reviewing and revising its *Student Placement Agreement* with Shoppers.

[75] It should be noted that the U of S *Student Placement Agreement* with Shoppers was dated November 14, 2016 and signed by the pharmacist/owner of Shoppers at that time (who was not Ashish Patel). In effect, this agreement was a nullity at the time of the privacy violation. There will be a recommendation that if U of S continues to place students at Shoppers, all *Student Placement Agreements* are signed by the current pharmacist/owner of Shoppers at the time of the student's learning rotation.

Health and Ashish Patel

[76] Earlier, OIPC described the JSAP, which is a document between Health and eHealth setting out the responsibilities for organizations using PIP and the rules for the collection, use and disclosure of personal health information in PIP. Representatives of User Organizations must also sign a JSAP confirmation document indicating they accept the JSAP. Ashish Patel signed the JSAP confirmation document on November 6, 2019.

[77] Section 5.1.1 of the JSAP sets out the responsibilities for User Organizations, including establishing written policies and procedures to maintain safeguards to protect personal health information. It says:

> **5.1.1 User Organization Responsibilities**
>
> Each User Organization shall:
>
> (a) appoint a User Organization Representative who will be responsible for privacy for PIP, and a User Organization Approver (who may be the same individual as the User Organization Representative) who will be responsible to manage and designate Users and User roles for the User Organization;
>
> (b) provide eHealth and the Ministry with the contact information for its User Organization Representative and (where applicable) its User Organization Approver;
>
> (c) with respect to PIP Data within its custody or control or within systems within its custody or control. establish written policies and procedures to maintain administrative, technical and physical safeguards that will:

> (i) protect the integrity, accuracy and confidentiality of the information;
>
> (ii) protect against any reasonably anticipated:
>
> 1. threat or hazard to the security or integrity of the information;
>
> 2. loss of the information; or
>
> 3. unauthorized viewing, use, disclosure, modification or deletion of the information; and
>
> (iii) otherwise ensure compliance with HIPA by its employees;
>
> (d) comply with all applicable laws including without limitation HIPA and, where applicable, PIPEDA. It is important to note that the Saskatchewan Office of the Information and Privacy Commissioner has stated as follows:
>
> > (A) trustee cannot rely on the provisions in HIPA for collection, use and disclosure of personal health information without express or implied consent in sections 26, 27 and 28 unless that trustee has first satisfied the general duties in sections 9, I 0. 16, 19, 23.1
>
> It is the responsibility of each User Organization to ensure it has authority and consent to collect, use, disclose and enter PIP Data as outlined in this Policy.

[78] OIPC asked Ashish Patel to provide copies of policies and procedures and any details that illustrated the student understood their obligations under HIPA. Ashish Patel provided OIPC with the following:

- A version of Saskatchewan of College of Pharmacy Professionals' (SCPP) *Supervision of Pharmacy Interns* policy dated May 2, 2025 (which cannot be the version in effect when the student was completing their placement). In Investigation Report 179-2024 at paragraph [61], OIPC quoted a version of this policy dated September 14, 2021, which is likely the version of the document in effect when the student was working their experiential learning rotation at Shoppers. This version of the document provided that the responsibility for supervising interns is the responsibility of the pharmacy manager (which was Ashish Patel).

- A copy of SCPP's *Accessing PIP and eHR Viewer* general guidance document, dated September 6, 2023. This document provides that HIPA authorizes access to personal health information on a need-to-know basis.

[79] Ashish Patel clearly relied on the U of S to ensure students were signing "confidentiality documents". In so doing, there was a total abdication of responsibility when it came to the protection of the personal health care information of the citizens of Saskatchewan. He submitted:

> I have attached the SCPP policy for pharmacy intern students. I contacted the University of Saskatchewan for providing confidentiality documents every student has to sign before starting an internship so the University has forwarded to your office for his internship documents. Shoppers have a policy and procedure to sign confidentiality documents for employees but not for interns as pharmacy interns are not set up in shoppers HR portal.
>
> -Usask pharmacy placement program has all documentation for orientation list ,confidentiality agreement.

[80] Ashish Patel failed to establish independent policies and procedures unique to the pharmacy in order to maintain administrative, physical and technical safeguards of personal health information pursuant to the JSAP or section 16 of HIPA. There will be a finding that Ashish Patel failed to provide adequate safeguards in the supervision of this student. And in so doing, Ashish Patel also failed to ensure the confidentiality of the personal health information of the citizens of Saskatchewan.

[81] Section 7.3 of the JSAP provides that Health may suspend of terminate a user or User Organization's access to PIP:

> 7.3 **Suspension or Termination by Ministry.**
>
> If the Ministry believes that a User or User Organization has not complied with the privacy laws applicable to it or with the terms of this Policy, the Ministry may suspend the User/User Organization's right to collect or use information within PIP under this Policy in whole or in part.
>
> The Ministry shall inform the applicable User/User Organization of any suspension, and shall provide the User/User Organization an opportunity to make representations to the Ministry. The Ministry may then reinstate the User/User Organization's rights under this Policy or, if it appears to the

> Ministry that the User/User Organization will not or cannot comply with its obligations, the Ministry may terminate the User/User Organization's permission to collect or use PIP Data from PIP.

[82] As a side note, Ashish Patel is no longer the pharmacist at Shoppers. However, there will be a recommendation that Health ensure that the current pharmacist/owner of Shoppers has established policies and procedures to maintain administrative, physical and technical safeguards to protect personal health information in accordance with JSAP and section 16 of HIPA. Further, if Ashish Patel is the pharmacist/owner at another pharmacy in this province, there will be a recommendation that Health ensure that Ashish Patel has established policies and procedures to maintain administrative, physical and technical safeguards, in accordance with JSAP and section 16 of HIPA.

(d) Prevention of Future Breaches

[83] The most important aspect of responding to a privacy breach is the implementation of measures that seek to prevent future breaches. Prevention steps include strategies such as adding/enhancing safeguards, providing additional training, monitoring or auditing systems and users, and providing additional training.[15]

[84] In Investigation Report 179-2024, this office recommended that U of S, Health and eHealth each review their understanding of their own responsibility for the supervision of students and the protection of personal health information in PIP. Each of these parties has a different role to play in the event of a privacy breach on the part of a student placed in an establishment such as a pharmacy with a PIP database. OIPC recommended that these understandings be converted into formal agreements, policies and/or procedures. U of S, Health and eHealth all indicated to OIPC that they would comply with the recommendation.

[85] In its submission, U of S provided OIPC with the following update:

[15] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [50]; see also OIPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.

> Updated contracts are in the approval stages and will be implemented for the upcoming year clearly identifying who is responsible for protecting the PI/PHI as the trustee, and responsibility in management of privacy breaches.

[86] This is a positive step in responding with clarity and surety to privacy breaches and we commend U of S on this development.

[87] Health submitted the following with respect to future access to PIP by this student:

> A note was placed on the student intern's profile in eHealth's account management system to indicate that any clinical application request by the Intern must be assigned to the Privacy, Access and Patient Safety Unit at eHealth for review. Should the Intern go back to work in the Saskatchewan health sector and request PIP access, a thorough review will occur that would include retaking any PIP and privacy training, as well as, reviewing and acknowledging the PIP JSAP. The individual may also be subject to additional monitoring/auditing of their PIP use to ensure compliance with the JSAP.

[88] Further, Health submitted it would be reviewing its PIP training to ensure it is sufficient and that it was committed to exploring the requirement of annual privacy training in connection with PIP and PIP users. In Investigation Report 179-2024, OIPC noted that ongoing training is a requirement of section 5 of the HIPA Regulations, which provides:

> **5** To ensure compliance with the Act by its employees, a trustee that has custody or control of personal health information must:
>
> (a) provide orientation and ongoing training for its employees about the trustee's policies and procedures respecting the protection of personal health information; and
>
> (b) ensure that each of its employees signs a pledge of confidentiality that includes an acknowledgement that the employee:
>
> (i) is bound by the trustee's policies and procedures mentioned in clause (a); and
>
> (ii) is aware of the consequences of breaching those policies and procedures.

[89] We commend Health on its efforts in this area. There will be a formal recommendation that Health require PIP users to undergo PIP privacy training on an annual basis.

[90] Niravkumar Patel is now the pharmacist at Shoppers. Shoppers has not engaged any student interns since new management came on board. There will be a recommendation that should Shoppers and Niravkumar Patel assume responsibility for student interns as a part of the U of S experiential learning program, policies and procedures that maintain administrative, physical and technical safeguards to protect personal health information pursuant to section 16 of HIPA must be in place. There is a further recommendation that Shoppers and Niravkumar Patel provide training on the policies and procedures pursuant to section 5 of HIPA Regulations upon the reception of a student intern.

III FINDINGS

[91] Since both HIPA and LA FOIP are engaged, OIPC has jurisdiction to undertake this investigation.

[92] Seventy privacy breaches occurred in this matter.

[93] The privacy breaches have been contained.

[94] Health's notice to the affected individuals was inadequate.

[95] U of S has taken the appropriate step of requiring students to review and sign the Experiential Learning Student Privacy and Confidentiality Pledge.

[96] U of S' current method of evaluating students' ability to maintain privacy and confidentiality in the PharmD program is insufficient.

[97] Ashish Patel failed to provide adequate safeguards in the supervision of students in his employe and failed to ensure the confidentiality of the personal health information of the citizens of Saskatchewan that was available on PIP.

IV RECOMMENDATIONS

Re: Notification of Affected Individuals

[98] I recommend that within 30 days of the issuance of this Investigation Report, Health contact the affected individuals once again to inform them of their right to complain to OIPC as well as to recognize the impacts of the privacy breach in the form of an apology.

Re: Prevention of Future Similar Breaches

[99] I recommend that U of S apply more rigour in evaluating the student's ability to maintain privacy and confidentiality. This could include requiring pharmacists to obtain PIP audits of every student throughout the rotation at a pharmacy so that the pharmacist can ensure the student's access is on a need-to-know basis for the entire duration of a rotation.

[100] I recommend that if U of S continues to place students at Shoppers for the experiential learning rotations, that it ensures it has Student Placement Agreements signed with the pharmacist/owner of Shoppers at the time of the student's rotation.

[101] I recommend that Health ensure that the current pharmacist/owner of Shoppers has established policies and procedures to maintain administrative, physical and technical safeguards to protect personal health information in accordance with JSAP and section 16 of HIPA.

[102] If Ashish Patel is the pharmacist/owner at another pharmacy, I recommend that Health ensure that Ashish Patel has established policies and procedures to maintain administrative, physical and technical safeguards, in accordance with JSAP and section 16 of HIPA.

[103] I recommend that Health require PIP users to take PIP training on an annual basis.

[104] I recommend that should Niravkumar Patel accept student interns as a part of the U of S experiential learning program, that policies and procedures that maintain administrative, physical and technical safeguards to protect personal health information pursuant to section 16 of HIPA are in place.

[105] I recommend that should Niravkumar Patel/Shoppers accept student interns in the future, that they provide training on such policies and procedures pursuant to section 5 of HIPA Regulations.

Dated at Regina, in the Province of Saskatchewan, this 7th day of July, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner