Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 034-2025[1]

## Neighbourly Pharmacy Incorporated (Pharmasave #424 and Pharmasave #425)

**December 5, 2025**


**Summary:** Neighbourly Pharmacy Incorporated (Neighbourly) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). The privacy breach occurred when the pharmacist/ manager (former manager) used the point-of-sale system (Kroll) to access personal health information for the purpose of creating a bogus refund and pocketing the refund for personal use. The Commissioner opened a file and issued an Investigation Report pursuant to *The Health Information Protection Act* (*HIPA*).

The Commissioner made the following findings:
(1) A privacy breach occurred when the former manager used personal health information for an unauthorized purpose;
(2) Neighbourly took reasonable steps towards containment but should have identified and itemized the affected individuals sooner than it did;
(3) On the facts of this case, there is no need to provide notice to the affected individuals;
(4) The root cause of this privacy breach was the former manager who failed to follow all professional obligations and who failed to adhere to the corporate administrative safeguards that were in place at the material time;
(5) Deficiencies in the technical safeguards in place at the two pharmacies were a contributing factor to the privacy breach but not the root cause;
(6) Neighbourly had appropriate administrative safeguards in place to prevent the privacy breach, had they been followed;
(7) Neighbourly has properly addressed the deficiencies in the technical safeguards in the two pharmacies since the occurrence of the privacy breach.


[1] This Investigation Report also involves IPC Files 092-2025 and 094-2025.

The Commissioner had no overall recommendations as a result of this investigation.

The Commissioner did not recommend that this matter be referred to the Attorney General of Saskatchewan for consent to prosecute pursuant to section 64 (offence provision) of *HIPA*. For the detailed reasons explained below, this privacy breach was the result of the combination of many factors. The former manager was terminated from their employment. Neighbourly proactively reported this breach to OIPC and both the former manager and Neighbourly co-operated with OIPC in this investigation. There was no harm to the public and the likelihood of a public interest in the prosecution of this matter is negligible.

TABLE OF CONTENTS

## I BACKGROUND

[1] On February 12, 2025, Neighbourly Pharmacy Incorporated (Neighbourly) contacted the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) to report a privacy breach. The breach occurred at Pharmasave #424 (OIPC File 034-2025) and Pharmasave #425 (OIPC File 092-2025) both pharmacies in Moose Jaw.

[2] On January 22, 2025, an eyewitness employee at one of the Moose Jaw pharmacies reported to Neighbourly that they had witnessed the pharmacist/manager (herein referred to as "former manager") "stealing money from the till". On January 23, 2025, the District Operations Director for Neighbourly reviewed surveillance footage for the pharmacy and confirmed that the former manager had indeed been captured on video pocketing money from the till. Neighbourly advised of the following:

> [The] Pharmacy manager accessed patient files to reprint old prescription receipts. No patient profiles were altered. The receipts were used in the Point of Sale system to manipulate the system to pay cash out to the manager. This occurred over the course of the past year at 2 Pharmasave locations in the city of Moose Jaw. While accessing patient files was not the intended motive, it was determined that by reprinting receipts the manager accessed files for patients [they were] not currently providing care for.

[3] The point-of-sale system used by Neighbourly is called "Kroll". Among other things, Kroll's database contains customer profiles of the customers who attend the pharmacies for medical prescriptions over the years. Neighbourly provided OIPC with a spreadsheet containing data that supported the allegation that the former manager issued refunds by first inappropriately accessing customer profiles in Kroll between January 14, 2023, and January 22, 2025. Once the former manager accessed the customer profiles, a receipt was re-printed and used to create a bogus refund. The former manager then pocketed the refund for personal use. The stolen funds were those of Neighbourly.

[4] Neighbourly explained that by accessing the customer profiles in Kroll, the former manager was then able to use the individual identities of 66 different customers to process 89 monetary refunds which approximated $3,082.35 in overall lost funds to Neighbourly.

[5] Neighbourly confirmed that customer profiles in Kroll were not modified or altered and the manipulations of Kroll occurred during work hours and when the pharmacies were closed. Neighbourly added that the former manager printed hard copy receipts to generate the cash refunds, using current and past customer prescription receipt information on Kroll. Some of the customers were deceased at the material time and many had long since ceased doing business at the pharmacies so their contact data was out of date.

[6] Neighbourly reported the former manager to the Saskatchewan College of Pharmacy Professionals (College). The College notified eHealth Saskatchewan (eHealth) to suspend the former manager's accesses to the eHR Viewer (Viewer) and the Pharmaceutical Information Program (PIP) database which is connected to the Kroll in house point-of-sale system.[2]

[7] On May 25, 2025, this office notified Neighbourly that OIPC would be undertaking an investigation into the privacy breach that occurred at both Pharmasave #424 and Pharmasave #425.[3]

[8] Neighbourly provided its completed *Privacy Breach Investigation Questionnaire* and supporting documentation on June 19, 2025.

[9] On May 29, 2025, OIPC also provided the former manager with an opportunity to provide a submission (OIPC File 094-2024), which they did through legal counsel on July 10, 2025.

[2] In November 2025, Neighbourly worked with the Ministry of Health and eHealth Saskatchewan to confirm that the breaches in the Kroll database were not linked in any way, and there were no related and unauthorized intrusions onto the Viewer and/or PIP databases. Since there is no allegation that the former manager ever improperly accessed Viewer/PIP, this is a non-issue in this Investigation Report.

[3] OIPC provided notice to Neighbourly that an investigation would commence pursuant to sections 42(1)(c) (application for a review where the person believes there has been a contravention of *HIPA*) and 52 of *HIPA* (Commissioner's powers to investigate).

## II DISCUSSION OF THE ISSUES

### 1. Jurisdiction

[10] The *Health Information Protection Act* (*HIPA*)[4] is engaged when three elements are present: 1) there is personal health information; 2) there is a trustee; and 3) the trustee has custody or control of the personal health information.

#### *a. First element – personal health information*

[11] To generate prescription receipts, the former manager needed to access each customer's profile in Kroll.[5] Within Kroll, access may be had to a customer's basic demographic information (e.g., name, address, date of birth, sex)[6], Health Services Number (HSN), prescription history and other "clinical data" such as "medical conditions, allergies, potentially lab work, other documents from external sources such as clinicians, medication profile, etc."[7] These categories all qualify as personal health information pursuant to sections 2(1)(m)(i), (ii), (iii), (iv)(A) and (v) of *HIPA* as follows:

> **2**(1) In this Act:
>
> …
> (m) "personal health information" means, with respect to an individual, whether living or deceased:

[4] *The Health Information Protection Act*, SS 1999, c. H-0.021, as amended.

[5] Kroll is part of *TELUS Health and Payment Solutions Limited Partnership*.

[6] OIPC considered this information to be "registration information" and it includes data elements that a trustee uses to register a patient for a service at paragraphs [18] to [20] of Investigation Report 014-2023, 015-2023.

[7] OIPC concluded that medication profile information that includes data such as prescription information or allergy/intolerance information is "personal health information", see paragraphs [15] and [16] of OIPC Investigation Report 036-2025, et al. OIPC also has concluded that "personal health information" can include demographic information, such as name, date of birth, sex and health card number at paragraphs [12] and [15] of OIPC Investigation Report 398-2019, et al.

> (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
>
> …
>
> (v) registration information;

[12] Therefore, the personal health information of the Neighbourly patient/customers was involved in this matter.

***b. Second element - trustees***

[13] On its website, Neighbourly advertises a personal approach to community healthcare and describes itself as "Canada's largest and fastest growing network of community pharmacies". [8]

[14] Section 2(1)(t)(xv) of *HIPA* lays out that trustees include those as provided for in section 4(b) of *The Health Information Protection Regulations, 2023* (*HIPA Regulations*).[9] These sections lay out:

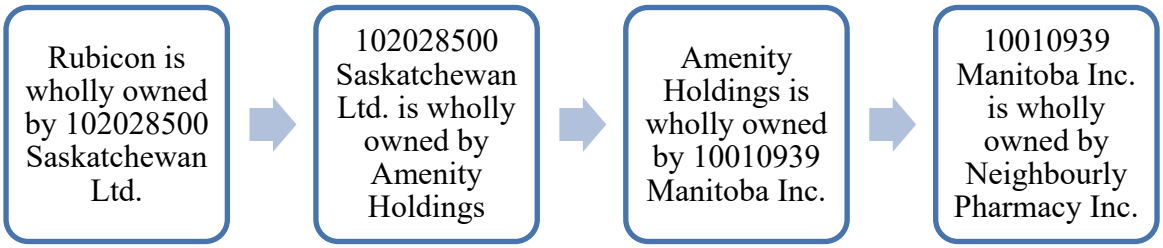
> ***HIPA***
>
> **2**(1) In this Act:
>
> ...

[8] See the Neighbourly website webpage: *Our Story | Neighbourly Pharmacy*.

[9] *The Health Information Protection Regulations, 2023*, c. H-0.021 Reg 2 (August 1, 2023), as amended by Saskatchewan Regulations 68/2023.

> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> …
> (xv) any other prescribed person, body or class of persons or bodies;
>
> ***HIPA Regulations***
>
> **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;

[15] In determining whether a trustee relationship was at play, the specific corporate entity that was subject to the provisions of HIPA in this matter must be identified. Neighbourly provided copies of the pharmacy permits for each pharmacy. Those permits listed the proprietor for each pharmacy as "Rubicon Pharmacies Permit Corp." ("Rubicon"). Neighbourly explained that Rubicon is wholly owned by 102028500 Saskatchewan Ltd., which is wholly owned by Amenity Holdings Incorporated (Amenity Holdings).[10] Amenity Holdings is wholly owned by 10010939 Manitoba Incorporated (Manitoba Inc.), which is wholly owned by Neighbourly Pharmacy Operations (a.k.a. Neighbourly Pharmacy Inc.)[11] Neighbourly considers itself to the "ultimate parent company." The following graphic may assist in understanding the corporate relationships in this matter:




[10] An Information Services Corporate Registry (ISC) search verified the connection between Rubicon Pharmacies Permit Corporation and Saskatchewan Ltd. On the same entity profile, the Amenity Holdings Inc. is listed as a shareholder.

[11] A search of *Manitoba Companies Online* verified that 10010939 Manitoba Incorporated is currently inactive and has been amalgamated with Neighbourly Pharmacy Operations (registry number 10185079) which is currently active. The address for Neighbourly Pharmacy Operations entity profile is the same as Neighbourly Pharmacy Incorporated (Neighbourly).

[16] We know that personal health information was accessed by the former manager from Kroll where the personal health information was stored in both pharmacies. Neighbourly confirmed that the former manager would have signed an agreement with TELUS Health and Payment Solutions Limited Partnership (TELUS), which created and managed Kroll.

[17] Section 2(1)(j) of HIPA defines "information management service provider". This term is important in the Saskatchewan legislation because TELUS was, in fact, an information management service provider to Neighbourly by virtue of its management of Kroll which it contracted out to Neighbourly. Section 2(1)(j) provides as follows:

> **Interpretation**
> **2**(1) In this Act:
>
> …
> (j) **"information management service provider"** means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf;

[18] A copy of the TELUS agreement confirms the nature of the relationship between TELUS and Neighbourly. While not binding on this office, it is important to note that TELUS viewed Neighbourly as a "trustee" under *HIPA*:

> A. TELUS has agreed to provide the applicable pharmacy management software solution and related services to Custodian(s) (also known as "trustee(s)" under the applicable Canadian health privacy legislation), including any related pharmacy patient portal solution, as applicable (hereinafter collectively referred to as "PMS Services"), pursuant to the applicable software license and other services agreement(s) ("PMS Agreement(s)") executed concurrently with or subsequently after this IMA. Please note that TELUS might have entered into the PMS Agreement(s) with a different legal entity than the Custodian(s)identified herein.
>
> …
> D. Pursuant to the applicable Canadian health privacy legislation, the Custodian(s) enter(s) into this IMA with TELUS in order to provide Personal Health Information to TELUS and allow TELUS to Process

> Personal Health Information that is in the custody or under the control of the Custodian(s) with or without the consent of the individuals/patients who are the subjects of the Personal Health Information, as applicable, for the purpose of providing the PMS Services in accordance with the PMS Agreement(s).

[19] The former manager was, at the material time, named as a director of Rubicon as of May 2020.[12] Section 9-1(1) of *The Business Corporations Act, 2021 (BCA)* [13] describes the role of a director as follows:

> **9-1**(1) Subject to any unanimous shareholder agreement, the directors of a corporation shall:
>
> (a) exercise the powers of the corporation directly or indirectly through the employees and agents of the corporation; and
>
> (b) direct the management of the business and affairs of the corporation.

[20] The former manager had authority to act on behalf of, and to bind, Neighbourly in signing the TELUS agreement as a director pursuant to section 9-1(1) of *BCA*. Neighbourly is the trustee by way of section 2(1)(t)(xv) of *HIPA* and section 4(b) of *HIPA Regulations* as outlined in paragraph [14] above. We conclude that the trustee is Neighbourly and it was bound by the former manager who entered into the contractual relations with TELUS on behalf of Neighbourly. Therefore, the second element of the jurisdictional test is met.

### *c. Third element – the trustees must have custody or control over the personal health information*

[21] "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,

[12] OIPC confirmed this fact from the ISC search of the entity profile for Rubicon Pharmacies Permit Corp.

[13] *The Business Corporations Act, 2021*, SS 2021, c 6, as amended.

regulating and administering its use, disclosure or disposition. Custody is not a requirement for control to be present.[14]

[22] The agreement that the former manager signed with TELUS provided that the control and custody of the personal health information always resided with the Custodian (Neighbourly):

> …
> 2.4 The PHI Processed by TELUS based on this IMA is considered to continue in the custody or under the control of the Custodian(s) for the purposes of the applicable Canadian health privacy legislation.[15]

[23] We conclude that since the former manager had authority to act on behalf of Neighbourly and entered into contractual relations with TELUS on behalf of Neighbourly, Neighbourly is not only a trustee for the purposes of *HIPA* but the custodian of the personal health information in this matter as well. The care and control of the personal health information in Kroll was always with Neighbourly.

[24] As the three elements are present, *HIPA* is engaged and this office has jurisdiction to undertake this investigation pursuant to the jurisdiction afforded by PART VI and PART VII of *HIPA*.

**2. Did a privacy breach occur?**

[25] A privacy breach occurs when personal health information is collected, used and/or disclosed without authority under *HIPA*. As noted above, the former manager accessed the personal health information of 66 customers in Kroll to reprint receipts, create a refund, and then to pocket the refund. This access constitutes a "use" under HIPA.[16]

[14] OIPC Investigation Report 036-2025 et al. at paragraph [25].

[15] PHI: Personal Health Information; IMA: Information Manager Agreement.

[16] "Use" in *HIPA* includes reference to, or manipulation of, personal health information by the trustee that has custody or control of the information but does not include disclosure to another person or trustee.

[26] Sections 23(1) and (2) of *HIPA* provides that personal health information can only be used under conditions that are deemed to be "reasonably necessary":

> **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.
>
> [Emphasis added]

[27] As a result, sections 26(1) and (2) of *HIPA* places restrictions on how a trustee may use personal health information, with consent being the prime criterion for legal use:

> **26**(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (2) A trustee may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
>
> (b) for the purposes of de-identifying the personal health information;
>
> (c) for a purpose that will primarily benefit the subject individual; or
>
> (d) for a prescribed purpose.

[28] While the former manager accessed (used) the customer profiles of 66 individuals there was no alteration or inappropriate disclosure of the personal health information. Neighbourly confirmed that the sole purpose of the access was to re-print the receipts which were then used in the pharmacy refund process for the financial benefit of the former manager. The former manager's submission confirmed there was no motive to snoop or access personal health information for any other reason than to commit theft.

[29] None of the conditions as stated in section 26 were present for the use of the personal health information in this matter. There is a finding that a privacy breach occurred when the former manager used personal health information for an unauthorized purpose.

**3. Did Neighbourly properly respond to the privacy breach?**

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

a) Has the trustee contained the breach as soon as possible?

b) Has the trustee notified all affected individuals as soon as possible?

c) Has the trustee investigated the breach?

d) Has the trustee taken concrete steps to prevent future breaches?

***a) Containment of the Breach***

[31] 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.[17]

[32] Neighbourly originally investigated the former manager for theft. This led to the discovery that the former manager had also committed the privacy breach. Neighbourly explained:

> …The individual accessed the pharmacy's main prescription filling database which we are not able to audit as [they] did not do a transaction, [they] only reprinted labels.

[33] When Neighbourly discovered the former manager's fraudulent activity, it shut down the theft immediately by revoking the former manager's access to Kroll. The former manager was then placed on leave and an internal investigation concluded with termination of

[17] *Supra,* footnote 14 at paragraph [53].

employment on February 6, 2025. Without a doubt, the effective and immediate actions on the part of Neighbourly stopped the illegal behaviour from continuing.

[34] Neighbourly did not itemize the 66 affected individuals as part of its early investigation. That measure occurred later. Itemizing the full scope of a privacy breach is an essential aspect of containment. [18] A trustee must know the identity of and number of possible complainants and the scope of the breach, such as whether the breach spread further than the pharmacy into the eHealth databases. Notice must then be addressed. It is impossible to furnish a proper notice if the number, identity of the affected individuals and scope of the breach remain unknown.

[35] Neighbourly finally itemized the affected individuals when it confirmed to this office that the former manager had not accessed the broader eHealth databases.[19] The investigation also revealed that 11 of the 66 affected individuals had their personal health information accessed twice in the refund scam. This phase of the investigation was at the request of OIPC and happened 10 months after the proactive report. Neighbourly is still credited for stopping the breach and for the eventual creation of a list of affected individuals. There is a finding that Neighbourly took reasonable steps towards containment, but it should have identified and itemized the affected individuals sooner than it did.

***b) Notification of Affected Individuals***

[36] It is best practice for trustees to inform affected individuals *as soon as possible* when personal health information has been breached. This is an obvious step that invokes the principles of fairness. Affected individuals should be informed of the possible risks so they

[18] In OIPC Investigation Report 154-2022 at paragraphs [30] to [31] and [49] to [50], OIPC spoke to the importance of keeping an inventory of records, which is helpful in the context of trying to contain a privacy breach.

[19] Neighbourly took the step of itemizing affected individuals when it investigated, using data it obtained from eHealth, whether the former manager also accessed PIP and the Viewer. However, this measure was taken 10 months after notifying OIPC of the privacy breach.

can take any remedial steps they deem necessary to protect themselves. An effective notification should include:[20]

- A general description of what occurred.
- A detailed description of the personal health information involved (e.g., name, health number, medical record information, etc.).
- A description of the types of harm that may result from the breach.
- Steps the trustee has taken to mitigate the harm and prevent future breaches.
- If necessary, actions that affected individuals can take to mitigate any harms from the breach.
- Contact information of an individual within the organization who can answer questions and provide information.
- A notice that individuals have the right to complain to OIPC.
- Recognition of the impacts of the breach on affected individuals and an apology.

[37] Neighbourly decided not to provide notice to the affected individuals in this case. Its reasons are as follows:

> As (1) no patient profiles were altered or modified, (2) no patient information was disclosed or shared with others, and (3) the sole purpose of accessing the patient profiles was for the pharmacy manager to print receipts to issue refunds for [their] own financial benefit, we did not believe there was harm to the affected individuals.
>
> …
> We do not believe that there was risk to the affected individuals as no PI or PHI was disclosed as part of this breach.

[38] Regarding risk*, HIPA* does not have a requirement that trustees take reasonable steps to notify affected individuals of a *real risk of significant harm* when a breach occurs. Before deciding to not provide notice, however, OIPC recommends that trustees first take steps to

[20] *Supra,* footnote 14 at paragraph [56].

assess what possible harms may exist.[21] This can inform a trustee's decision whether to provide notice. This office has historically recommended that trustees provide notice of a privacy breach to affected individuals, even if any resulting harm is not obvious or if it is assessed that there is no perceivable risk of harm.[22] Affected individuals must be allowed to determine for themselves what risk they have undergone and they must then be free to take whatever steps necessary to protect themselves.

[39] A privacy breach always carries the risk of identity theft and fraud.[23] Notice must be given when personal information has been breached *and* when there is a real risk of significant harm. The motivation behind the former manager's fraudulent scheme was to obtain funds from Neighbourly to fund his addiction and hide his addiction from his family. Personal health information in this matter only sufficed to permit a re-printing of the medication prescriptions to allow for refunds. There was never a real risk of significant harm for identity theft or any of the other risks that come from traditional snoopers. Still, at the phase of discovery by a trustee – affected individuals need to be identified so that they may address personal risk if their information has been put at jeopardy. Again, that was not the case here.

[40] The former manager's submission to this office confirmed that the entire fraudulent scam was to reprint prescriptions and access a refund from Neighbourly's cash on hand. The former manager has fully assumed responsibility for this behaviour. There was a confirmation that no personal health information was ever accessed or even required beyond the prescription aspect of the refund in the carrying out of this fraudulent scheme.

---

[21] The Office of the Privacy Commissioner of Canada offers a risk assessment tool that organizations can use to determine if a privacy breach poses a real risk of significant harm.

[22] OIPC Investigation Report 253-2024, 033-2025 at paragraph [35]. See also OIPC Investigation Report 193-2024, 043-2025 at paragraphs [47] to [49]. Notice must be given when personal information has been breached *and* when there is a real risk of significant harm. As will be argued later in this report, the motivation behind the former manager's fraudulent scheme was to obtain funds from Neighbourly. Personal health information in this matter only sufficed to allow for a re-printing of the medication prescriptions to allow for refunds. There was never a real risk of significant harm for identity theft or any of the other risks that come from traditional snoopers.

[23] The *Canadian Anti-Fraud Centre* provides information on identity theft.

Neighbourly explained that some of the customers (affected individuals) are now deceased, and others have not attended either pharmacy in years. In this instance, requiring Neighbourly to provide notice to the affected individuals in this matter is a "make work" proposition at best and serves no purpose in law. There is a finding that, on the facts of this case, there is no need for Neighbourly to provide notice to the affected individuals. A recommendation for notice will not follow but that is because this is a most unusual case.

### *c) Investigation of the Breach*

[41] Trustees must investigate in the wake of a privacy breach to learn the root cause and to prevent a future occurrence. An investigation should address the incident on a systemic basis and include a root cause analysis.[24]

[42] Section 16 of *HIPA* places on a trustee a "duty to protect" personal health information by establishing policies and procedures to maintain administrative, technical and physical safeguards as follows:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[43] Section 23(2) of *HIPA* further informs the policies and procedures that a trustee must establish:

[24] *Supra,* footnote 14 at paragraph [62].

> **23**(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.

[44] Neighbourly established the following timeline of events in its investigation:

- On January 22, 2025, the former manager was witness to be inappropriately accessing Kroll, or the personal health information contained within, to commit theft.
- On January 23, 2025 authorities from Neighbourly viewed videotape surveillance evidence and found evidence of the theft.
- On January 24, 2025 the former manager was placed on suspension pending an investigation conducted by Neighbourly.
- Neighbourly interviewed the former manager on February 4, 2025, and terminated their employment on February 6, 2025.
- The matter was proactively reported to OIPC by Neighbourly on February 12, 2025.

[45] Given the timelines, Neighbourly took timely action to address the privacy breaches and complete its investigation. Neighbourly is to be commended for its proactive report to this office and for working with us to resolve this unfortunate occurrence.

[46] Investigating a privacy breach to identify the root cause is key to understanding what happened to prevent similar breaches from occurring in the future.[25] Neighbourly addressed its administrative, technical and physical safeguards in relation to this privacy breach in its written submission.

### *i. Administrative Safeguards*

[47] Administrative safeguards include fundamental corporate documents that preserve the security of personal health information. They can include policies and procedures

[25] OIPC Investigation Report 291-2018 at paragraph [20].

regarding privacy, security of the premises and they will almost always require employee oaths/affirmations that the polices will be honoured by the employee.[26]

[48] Neighbourly had several administrative safeguards in place at the time of the privacy breach. The first was the *Store Operator Agreement*[27], which defined confidential information as "information owned, possessed or controlled by the employer." This agreement explained that confidential information was information stored in "databases, customer lists… and other information not available to the public in general without restriction…". It was abundantly clear to all employees that the information within Kroll was personal health information, that it was confidential in nature and only to be accessed on a need to know basis.

[49] Another administrative safeguard in place was the *Confidentiality and Privacy Policy,*[28] which stated that as a "condition of employment", employees are prohibited from "disclosing company confidential and proprietary information." It contained a term that employees are only to use "personal information for the purposes for which it was collected" and not to use it for "any personal benefit or profit." Upon assuming the position, the former manager had formally agreed to abide by these policies.

[50] Neighbourly also provided OIPC with the following policies, procedures or guidance documents that are currently in place and were in place at the time of this matter which were also fully ignored by the former manager:

- *Reference Manual – Community Pharmacy Privacy Office* - document from the Saskatchewan College of Pharmacy Professionals (College) that describes the duties of a pharmacy privacy officer;

[26] OIPC Investigation Report 065-2025 at a paragraph [31].

[27] Counsel for the former manager provided this document to OIPC along with the formal written submission. This document outlines the former manager's terms of employment and formal duties.

[28] This document indicates that it was in effect as of January 1, 2021, the time the former manager was employed.

- *The Health Information Protection Act (HIPA) Founding Principles* – document from the College that outlines the 12 founding principles found at the beginning of *HIPA*;

- *Reference Manual – Privacy Toolkit for Community Pharmacies* – document from the College that outlines what is required to meet compliance with *HIPA* and, where applicable, the federal *Personal Information Protection and Electronic Documents Act*;

- *Code of Ethics and Business Conduct 2025* (Neighbourly) – organizational document that outlines code of ethics for pharmacies and business conduct. A section addresses confidentiality;

- *Confidentiality and Privacy Policy 2021* (Neighbourly) – as previously discussed in this Investigation Report, a document that outlines, as a condition of employment, the privacy obligations of each pharmacist; and

- *Schedule A – Job Description* (Neighbourly) – document that outlines the responsibilities of a pharmacy manager.

[51] The former manager paid little heed to the many administrative safeguards that were in place at the instance of Neighbourly. The root cause of this privacy breach was the former manager who failed to follow their professional obligations and who failed to adhere to the administrative safeguards that were in place at the material time and there is a finding to this effect.

### *ii. Technical Safeguards*

[52] Technical safeguards involve access controls on electronic storage, and the security of physical premises. They often involve use of individual/unique usernames and passwords to permit access.[29]

[53] Neighbourly identified two issues with its technical safeguards at the time the former manager committed the privacy breach: (1) Kroll was configured such that it could be accessed via the shared usernames of employees; and (2) access to the pharmacies were facilitated with door security codes sourced from the license numbers of employees at these

[29] *Supra,* footnote 26 at a paragraph [31].

two pharmacies. Access to the pharmacies could be effected in off hours by means of another employee's access code. In its submission to this office, it was noted that the former manager "may have sometimes used a colleague's [license] number to enter the store during closed hours." Neighbourly also confirmed that the time clock on the security system was not accurate. Deficiencies in the technical safeguards in place at the two pharmacies were a contributing factor to the privacy breach but not the root cause and there is a finding to this effect.

#### *iii. Physical Safeguards*

[54] Physical safeguards include measures such as locked cabinets/bins, locked doors and video security cameras.[30]

[55] Neighbourly was able to immediately investigate the privacy breach because of its use of video surveillance cameras in the pharmacies. Video surveillance cameras are essential in terms of the security and physical safety of a pharmacy. In this unique case, video surveillance was not a deterrent and did not prevent the privacy breach.

### *d) Prevention of Future Breaches*

[56] The most important aspect of responding to a privacy breach is the implementation of measures after the fact 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.[31]

#### *i. Administrative Safeguards*

[57] We commend Neighbourly for its immediate removal of the former manager's access from Kroll upon discovery of the privacy breach and for placing the offender on suspension

[30] OIPC Review Report 166-2021 at paragraph [28].

[31] *Supra,* footnote 14 at paragraph [83].

pending the results of the in-house investigation. These actions effectively addressed the immediate threat to personal health information at the pharmacies.

[58] Neighbourly also provided a document it distributed to Saskatchewan pharmacy managers regarding the amended *HIPA Regulations* that came into effect on August 1, 2023. This document outlines the need for pharmacy managers to undertake the following to comply with the amendments:

i. Need to provide orientation and ongoing training to new staff regarding HIPA;

ii. Need to have employees sign a pledge of confidentiality to acknowledge they are bound by policies and procedures and aware of the consequences for breaching them;

iii. Need to have written retention and destruction policies; and

iv. Need to have written agreements with IMSPs such as Kroll, including an updated IMSP agreement and confidentiality pledge.

[59] Upon review of all documentation provided by Neighbourly, it is apparent that this organization goes to great effort to ensure pharmacy managers and employees have knowledge of, and are compliant with, *HIPA* and *HIPA Regulations*. There is a finding that Neighbourly had appropriate administrative safeguards in place at the time of the privacy breach which should have been preventative had they been followed. Hopefully these policies and procedures stand testament that current and future pharmacy managers are aware of their obligations under *HIPA* and especially to the use of personal health information in Kroll.

### *ii. Technical Safeguards*

[60] Neighbourly outlined that it undertook the following since this incident with the former manager:

…

> (1) All staff that have access to use the till/point-of-sale system, now have their own unique username and passwords, to limit multiple individuals accessing the till under the same username.
>
> (2) Security codes have been reset to individual numbers (not license numbers) to limit employees using other employees' security codes.
> …

[61] This office has found in past privacy breach investigations that it is impossible for an organization to properly investigate a privacy breach is if system users share log-on credentials.[32] It is also impossible to review or audit system activity if staff do not have their own credentials.

[62] As we have previously noted, the privacy breaches in this matter were facilitated by lax security measures with online access to Kroll and the physical premises. Neighbourly has adequately addressed these lapses in security. Going forward Neighbourly should take measures to ensure that employees understand that passwords *must* be unique and of an appropriate length to stave off future unauthorized access. These security requirements must be captured in corporate policies and procedures.[33]

[63] There is a finding that Neighbourly had appropriate administrative safeguards in place at the time to prevent the privacy breach that occurred had they been followed.

[64] There is a finding that Neighbourly has properly addressed the deficiencies in the technical safeguards in place at the two pharmacies since the occurrence of this privacy breach.

## 4. Should prosecution be recommended under section 64 of *HIPA*?

[65] We now address whether we will recommend the matter to the Attorney General of Saskatchewan for consent to prosecute pursuant to section 64 of *HIPA*. In a publication entitled, *Detecting and Deterring Unauthorized Access to Personal Health Information*

[32] OIPC Investigation Report 108-2018 at paragraph [42].

[33] The Government of Canada offers information on the use of strong password protection.

(January 2015), former Information and Privacy Commissioner of Ontario, Brian Beamish, advocated for an increase in prosecutions of those who access personal health information without cause. The public naming of those who commit privacy breaches and the referral of the matter to the Attorney General of Saskatchewan for consent to prosecute represents the community's zero tolerance for violations of *HIPA*. We affirm that the unauthorized access and use of personal health information in Saskatchewan is unacceptable and will not be tolerated.[34]

[66] A contravention of *HIPA* in the Province of Saskatchewan subjects the wrongdoer to the offence provisions laid out in sections 64(1)(a) and (3.2) of *HIPA*, which provide:

> **64**(1) No person shall:
>
> (a) knowingly contravene any provision of this Act or the regulations;
>
> …
>
> (3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.
>
> (4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General of Saskatchewan.

[67] The former manager has confirmed a breach of the personal health information of 66 customers of the pharmacy for their own personal gain. For sections 64(1)(a) and (3.2) of *HIPA* to apply, the contravention would have to be proven as being wilful and committed with full knowledge. This office defines these terms as follows:[35]

- A person who acts *knowingly* understands that the social harm will almost certainly be a consequence of the action but acts with other motives and does not care about whether the social harm occurs.

[34] OIPC Review Report 103-2025, 104-2025 at paragraph [77].

[35] OIPC Investigation Report 193-2024, 043-2025 at paragraph [154], which considered these definitions from *Black's Law Dictionary* (12th Ed., 2024).

- A voluntary act becomes *wilful*, in law, only when it involves conscious wrong or evil purpose on the part of the actor, or at least inexcusable carelessness, whether the act is right or wrong.

[Emphasis added]

[68] Legal counsel for the former manager provided a written submission to this office and co-operated fully in our investigation. It has been submitted, and we have accepted, that these violations of *HIPA* were not committed knowingly or wilfully because the former manager was subject to an active addiction at the material time. With the former manager's concession of full responsibility, the explanation for the reasons behind the theft and fraudulent behaviour, we will neither name the former manager nor will there be a recommendation that this matter be referred to the Attorney General of Saskatchewan for consent to prosecute. We note that Neighbourly chose not to refer this matter to the authorities as well.

## III FINDINGS

[69] *HIPA* is engaged and this office has jurisdiction to undertake the investigation.

[70] A privacy breach occurred when the former manager used personal health information for an unauthorized purpose.

[71] Neighbourly took reasonable steps towards containment but it should have been identified and itemized the affected individuals sooner than it did.

[72] On the facts of this case, there is no need for Neighbourly to provide notice to the affected individuals.

[73] The root cause of this privacy breach was the former manager who failed to follow their professional obligations and who failed to adhere to the administrative safeguards that were in place at the material time.

[74] Deficiencies in the technical safeguards in place at the two pharmacies were a contributing factor to the privacy breach but not the root cause.

[75] Neighbourly had appropriate administrative safeguards in place to prevent the privacy breach had they been followed.

[76] Neighbourly has properly addressed the deficiencies in the technical safeguards in the two pharmacies since the occurrence of this privacy breach.

## IV RECOMMENDATION

[77] Because of the unique nature of the facts behind this privacy breach, the quick response on the part of Neighbourly and the effective investigation that took place on the part of Neighbourly in conjunction with this office, we have no overall recommendations. Administrative and technical security safeguards must always be in place in a pharmacy. Such measures will, unfortunately, never stop behaviour that is contrary to *HIPA* when an employee fails to follow them.

Dated at Regina, in the Province of Saskatchewan, this 5th day of December, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner