Office of the Information and Privacy Commissioner for Nova Scotia

INVESTIGATION REPORT IR18-02

Drug Information System Privacy Breaches

Sobeys National Pharmacy Group

Catherine Tully
Information and Privacy Commissioner for Nova Scotia
August 1, 2018

TABLE OF CONTENTS

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Catherine Tully

INVESTIGATION REPORT IR18-02

August 1, 2018

Sobeys National Drug Pharmacy Group

Commissioner's Message

In our modern world, the delivery of health care is increasingly tied to electronic health records. The advent of electronic health records is intended to improve health care for citizens. But the increasing use of interoperable health databases by a multitude of health care providers also increases the risks of authorized users intentionally using their access for unauthorized purposes. These interoperable databases are rich with detailed personal health information. The temptation to "snoop" is difficult for some individuals to resist. Custodians of electronic health records must anticipate and plan for the intentional abuse of access privileges by authorized users.

This is a case of a pharmacist accessing highly sensitive personal health information over a two-year period to satisfy personal curiosity. Prescription history and medical conditions contain intimate details of a person's personal life and are among the most sensitive personal health information a custodian keeps about an individual. Access to this information for purposes not related to providing health care is a serious invasion of an individual's personal life and an abuse of authorized user access privileges.

During the course of this investigation, we discovered that the governance and monitoring of broad access, multi-custodian, electronic personal health information databases is a critical vulnerability in the province. There is an urgent need to strengthen and clarify the responsibilities for and monitoring of interoperable health information databases to protect the privacy of Nova Scotians' health information.

The circumstances of this breach illustrate that organizations which have been granted access to public health databases must have in place privacy breach management protocols and an effective technical auditing capacity in order to ensure that they can identify these type of "snooping" breaches and properly contain and manage the risks that result from this type of misuse.

Further, this investigation highlights a significant shortcoming in our health privacy law – the very short time limit for prosecution of offences. The current time limit defaults to six months

from the date of the offence because the *Personal Health Information Act* does not specify a time limit. These types of offences are often discovered well after the initial snooping began and investigations to determine whether an offence has occurred also take some time. Two years is the typical time limit for other provincial offences. While not a specific recommendation of this report, I have written directly to the Minister of Health and Wellness to recommend that the law be amended to lengthen the timelines for prosecution of offences under the *Personal Health Information Act*.

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Executive Summary

[1] In August of 2017, concerns about a registered pharmacist's use of the provincial Drug Information System (DIS) surfaced at the provincial College of Pharmacists who prompted the Department of Health and Wellness (DHW) to conduct an audit of user activity. From this initial audit, the DHW conducted an investigation along with Sobeys National Pharmacy Group (Sobeys) which employed the pharmacist as its manager at a rural pharmacy. The investigation led to the termination of the pharmacist's employment and the eventual notification of 46 individuals that the pharmacist manager (pharmacist) had inappropriately accessed their personal health information contained in the DIS.

[2] Both the DHW and Sobeys are custodians of personal health information within the meaning of the *Personal Health Information Act* (*PHIA*) and their responsibilities in relation to the DIS are set out in a User Agreement and policies. Both custodians had policies in place that clearly prohibit authorized users of the system from accessing and using personal health information for unauthorized purposes, that is, purposes outside of the provision of their professional services.

[3] On learning of the situation from the DHW, the Office of the Information and Privacy Commissioner (OIPC) immediately initiated a privacy investigation on December 20, 2017. Our investigation revealed that, over a two-year period, a pharmacy manager employed by Sobeys had inappropriately viewed the personal health information of 46 individuals. These individuals included the pharmacists' doctor, co-workers, former classmates, her child's girlfriend and her parents as well as teachers in her child's school among others. In order to gain access to some of the personal health information, the pharmacist created false profiles and falsely claimed that individuals had consented to the creation of the records. Further, the evidence established that the pharmacist used and shared the personal health information and continued to do so even after she was dismissed by the pharmacy.

[4] The initial investigation of the privacy breaches conducted by the DHW in conjunction with Sobeys was inadequate in a number of areas. As a result of the inadequate investigation, the DHW did not sufficiently canvass the risks associated with the breaches and did not sufficiently contain the breaches. Our investigation and analysis as it relates to the DHW is contained in the companion report IR18-01.

[5] Our investigation revealed that Sobeys did not sufficiently communicate with the DHW and did not correctly identify the full scope and nature of the breaches as they related to its own electronic health information system. Several of Sobeys' employees gave evidence that although they were aware of the unauthorized accesses by the pharmacist for some time, they hesitated to report the violations because the pharmacist was their supervisor. They feared they would not be believed and they may suffer some form of retaliation by the pharmacist.

[6] During the course of this investigation, we discovered that the governance and monitoring of broad access, multi-custodian, electronic personal health information databases is a critical vulnerability in the province. There is an urgent need to strengthen and clarify the

responsibilities for and monitoring of interoperable health information databases to protect the privacy of Nova Scotians' health information.

[7] Key findings in this investigation are:

- Sobeys failed to act in a timely fashion to properly and thoroughly investigate and contain these privacy breaches.
- The breaches have not yet been adequately contained because 28 false profiles continue to exist on the Sobeys' local system.
- Sobeys has several effective administrative safeguards including policies, training and monthly tips to staff.
- Sobeys took a number of effective steps to remediate the work environment following these breaches.
- Sobeys does not have adequate technical auditing capacity to detect unauthorized access by authorized users of its system.

[8] In summary, I make eight recommendations:

1. Sobeys develop and implement a privacy breach management protocol and provide training on the protocol to management within six months.
2. Sobeys immediately notify the 28 individuals whose personal information was improperly copied into its POS system.
3. Sobeys delete all false profiles from the POS system after providing a copy of the record to affected individuals.
4. Sobeys update, within 45 days, its Operational Standards for pharmacies in Nova Scotia and information brochures intended for Nova Scotian customers to include a correct reference to Nova Scotia's *Personal Health Information Act* and the privacy complaints process.
5. Sobeys make documenting the reason for DIS access for non-dispensing situations mandatory for all pharmacy staff.
6. Sobeys require all pharmacy staff to read this report.
7. Sobeys improve its Quality Improvement Audit process by doing it more frequently, involving more management and non-management staff and including a regular review of the audit logs for the POS system.
8. Sobeys obtain and implement the technical auditing capacity to regularly conduct proactive user activity audits of its POS system within six months.

1.0 Introduction and Purpose of the Report

1.1 Introduction

[9] This is the second of two investigation reports that arose out of the same series of events.

[10] On December 20, 2017, the Department of Health and Wellness (DHW) notified this office of a series of privacy breaches involving the province's Drug Information System (DIS). The DHW reported that the series of breaches were intentionally committed by an authorized user of the DIS, a registered pharmacist employed as a pharmacy manager by the Sobeys National Pharmacy Group (Sobeys) within the province.

[11] In its preliminary breach report to this office, the DHW indicated that the pharmacist had viewed a number of individuals' records in the DIS without authorization. The DHW initially reported that there was no malicious intent and that the pharmacist had used the system to look up cell phone numbers of people she[1] knew. In total, the DHW reported that it planned to give 39 affected individuals notice of the privacy breach within a few days. As a result of this investigation, the DHW eventually notified seven more affected individuals, bringing the total number of affected individuals to 46.

[12] Based on the information provided to this office on December 20, 2017, I notified the DHW and Sobeys that I had initiated two simultaneous investigations - one for each of the two custodians under the provisions of s. 92(2)(b) of the *Personal Health Information Act (PHIA)*. Both organizations cooperated in the conduct of these investigations. This report describes our investigation into Sobeys' conduct.

1.2 Jurisdiction

[13] Pursuant to *PHIA* s. 92(2)(b), the Commissioner may "initiate an investigation of compliance if there are reasonable grounds to believe that a custodian has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention."

[14] The DIS is a database containing personal health information as defined in s. 3(r) of *PHIA*. The DIS receives and stores personal health information collected by health care providers and simultaneously provides access to information stored within the database to health care providers. The relationships and data flows are complex, involving multiple layers of technology operated by multiple responsible parties. The technology platforms 'talk' to each other in the background to provide the end-user with a seamless application and easy access to information.

[1] Throughout this report, I use the pronoun "she" for both women and men in order to protect the identity of individuals. To be clear, the use of the term "she" is not meant as an indication of the gender of any of the individuals discussed.

[15] The DHW is a custodian within the meaning of s. 3(f)(ii) of *PHIA* and unequivocally confirms itself as the custodian of the health information stored within the DIS. Sobeys is a custodian within the meaning of s. 3(f)(i) of *PHIA* in that it provides direct health care services to patients through a team of regulated health care professionals and unregulated staff at its pharmacy locations. Sobeys operates its own electronic health records system that interfaces with the DHW network.

[16] Pursuant to *PHIA* s. 38(1)(u), a custodian may disclose the personal health information of an individual without the individual's consent to the DHW "for the purpose of creating or maintaining an electronic health record." This section of *PHIA* allows for the creation of multi-custodian health information databases, where information collected by one custodian is held and managed by the DHW and made available to many other custodians and regulated health professionals, according to the associated user agreements and technical provisions.

[17] Both custodians have responsibilities under *PHIA* in relation to their organizations' information practices and electronic systems.

[18] Section 65 of *PHIA* requires a custodian to implement, maintain and comply with information practices that:

- meet the requirements of this Act and the Regulations;
- are reasonable in the circumstances; and
- ensure that personal health information in the custodian's custody or under its control is protected against theft or loss of information, and unauthorized access to or use, disclosure, copying or modification of the information.

[19] The *PHIA* Regulations require a custodian to implement additional safeguards for personal health information held in an electronic information system, including requirements to implement safeguards to protect network infrastructure, hardware and software to ensure security and authorized access.[2]

[20] The existence of multi-custodian electronic databases adds a layer of complication to the responsibilities set out under *PHIA*. This breach investigation highlights the need for setting clear lines of responsibility in order to ensure that the personal health information of Nova Scotians is adequately protected in these modern-day databases.

2.0 Background

2.1 The Drug Information System – DIS

[21] The interrelationship between the DIS and Sobeys local POS system is described in detail in Investigation Report IR18-01.

[2] *Personal Health Information Act* Regulation, N.S. Reg. 217/2012 as amended, s. 10.

[22] The important factors for the purposes of this investigation are first that the DIS profile includes personal health information contributed to the database by authorized users across the province including:

- identifier information such as name, date of birth, gender;
- prescription history;
- prescription monitoring program alerts;
- allergies;
- adverse reactions;
- medical conditions;
- immunization history;
- services provided;
- observations; and,
- notes.

[23] A second important fact is that pharmacy users of the DIS, such as the pharmacist in this case, access the DIS through their local pharmacy system, known as the POS system. In order to access the DIS the local POS system must have a user profile for the customer or patient. If users want to access DIS data about an individual who is not a customer and so does not have a POS system profile, they must access a different provincial database, the Client Registry, and search for the person they are interested in. Once found, the profile in the Client Registry must be "synched" to the POS system. This draws in the name and address information into the POS system and creates a new POS profile. From there, the user can then access the DIS data on the provincial network.

2.2 Chronology of events

[24] Investigation Report IR18-01 contains the detailed chronology of events in this matter. For the purposes of this report the key events are described below.

[25] As a result of our investigation noted above, we determined that the following series of events occurred.

[26] A registered pharmacist, employed as a pharmacy manager at a branch of Sobeys, was granted access to the DIS on June 8, 2015, when the Sobeys pharmacy branch was connected to the network.

[27] Between 2015 and the fall of 2017, the pharmacist accessed the DIS and/or the Client Registry to obtain personal information of individuals who were either not clients of the local pharmacy or who were not receiving or requesting any service from the pharmacy at the time of the access.

[28] The audit reports established that the unauthorized accesses occurred between October 2015 and August 2017, affecting 39 individuals. For 28 of the 39 affected individuals, the pharmacist also created false POS profiles in order to access the DIS information of those 28 individuals who were not customers of the pharmacy.

[29] The types of access by the pharmacist as recounted by witnesses included looking up DIS information (such as prescriptions and medical conditions in particular) of:

- her child's girlfriend and her parents;
- her child's friends and acquaintances;
- an individual she had been involved in a car accident with;
- her child's teachers and former teachers;
- her former teacher (deceased);
- relatives (including deceased relatives);
- her and her family's health care providers;
- a former high school classmate who had recently suffered a significant illness; and
- co-workers.

[30] Several witnesses gave evidence that although they were aware of the unauthorized accesses by the pharmacist for some time, they hesitated to report the violations because the pharmacist was their supervisor. They feared they would not be believed and may suffer some form of retaliation.

[31] The Nova Scotia College of Pharmacists sent an investigator to conduct a site visit of the Sobeys pharmacy where the pharmacist worked on August 22, 2017.

[32] On August 23, 2017, one pharmacy employee had a conversation with the Sobeys district manager for her branch in which she communicated that a pharmacy employee had knowledge of a 'questionable lookup' on the DIS made by the pharmacist, that she had discussed it with a relief pharmacist a month prior, and that an inspector from the Nova Scotia College of Pharmacists had made a visit to the pharmacy.

[33] The DHW received an email from the Nova Scotia College of Pharmacists on August 28, 2017 asking the DHW to conduct an audit of user activity within the DIS for a particular user: the pharmacist. In response to this request, the DIS audit specialist initially identified eight individuals whose DIS profiles where accessed by the pharmacist in the prior month that could not be explained by the logged activity in the DIS.

[34] This initial audit information was then provided to Sobeys on September 11, 2017 to solicit any information from the pharmacy's local POS system that could explain the DIS access. Sometimes the local POS system contains information that would explain why a pharmacist accessed a person's profile. For example, the pharmacist may have provided pharmacy advice, over-the-counter medication sales or may have administered an immunization which is logged in the local POS system but not in the DIS. After searching the local POS system, the Sobeys district manager, along with a corporate human resources representative, questioned the pharmacist on September 15, 2017. Based on her responses, Sobeys immediately terminated the pharmacist's employment.

[35] Following its meeting with the pharmacist, the Sobeys district manager also met briefly with employees who worked at the local pharmacy and were supervised by the pharmacist. Employees disclosed some of their concerns about the pharmacist's behaviour to the district

manager and one employee submitted to the district manager a handwritten sheet of paper containing personal health information created by the pharmacist after accessing the Client Registry and/or the DIS in January 2017.

[36] On September 20, 2017, Sobeys director of quality and regulatory provided the DHW with a formal response with notes about each of the eight affected individuals from the POS system as well as from the interview with the pharmacist. The notes confirm that five of the eight were not patients at the local pharmacy and six of the eight accesses were not associated with any valid pharmacy business. The recorded rationale for the accesses provided by the pharmacist was a range including: to obtain an address, to obtain a phone number, a response to an undocumented doctors' office query, and that she could not recall or may have selected the wrong name. Two of the eight accesses were validated by the local POS system information. The DHW determined that the six invalid access events were privacy breaches.

[37] On September 20, 2017, the DHW initiated a broader audit of the pharmacist's activity in the DIS by requesting a full User Access Review Report from the Nova Scotia Health Authority's FairWarning team for the entire period the pharmacist had access to the DIS, which was from June 8, 2015 to September 15, 2017.

[38] The DHW identified an additional 67 potentially unauthorized accesses. The results were again provided to Sobeys to determine if any information from the pharmacy's local POS system could explain the identified DIS access events. By November 8, 2017, the DHW, with information from Sobeys, had identified an additional 33 individuals whose DIS profiles had been accessed with no documented clinical reason either in the DIS or in the local POS system. The total period of the unauthorized access was October 2015 to August 2017 and the total number of affected individuals identified in the two audit exercises was 39 people.

[39] On December 18, 2017, Sobeys notified the DHW that a pharmacy employee had supplied a copy of a statement the now dismissed pharmacist had prepared for one of the affected individuals to sign. The statement was a declaration of consent for the former pharmacy manager (pharmacist) to have accessed the DIS profile, including the date of access, and described purported authorized reasons for the access. Our investigation confirmed that the pharmacist arrived at the individual's home requesting that she sign the document. The individual refused and provided it to the pharmacy employee who in turn supplied it to Sobeys. Sobeys provided a copy of the document to the DHW.

[40] The DHW sent breach notification letters to 39 affected individuals on December 22, 2017.

[41] On December 20, 2017, the DHW notified my office of these privacy breaches. Based on the fact that the pharmacist's employment and access to the DIS was terminated by that time, the DHW and Sobeys reported that the immediate cause of the privacy breaches was contained.

[42] Following an interim recommendation by my staff on March 1, 2018, Sobeys undertook additional investigation actions to re-interview its staff from the local pharmacy and gather documentation about the privacy breaches in its possession. A summary of the additional investigation actions confirmed that the staff supervised by the former pharmacy manager

(pharmacist) had longstanding concerns about her behaviour related to compliance with a number of corporate policies and they confirmed direct observations of and conversations with the former pharmacy manager regarding her access to and use of the DIS for reasons other than providing clinical services to patients. It also confirmed that individuals whose profiles were inappropriately accessed and who were not clients of the pharmacy had false profiles created within the POS system.

[43] This investigation confirmed significant details of the circumstances, scope and nature of several of the privacy breaches:

- An employee reported that the pharmacist had encouraged her to use the network access to obtain contact information to send birthday greetings to known individuals.
- An employee witnessed the pharmacist access the DIS in March 2017 and then call her spouse on the phone to discuss what she had discovered. The employee heard the pharmacist say that their child cannot see this person because of the medications she and her parent were on.
- An employee observed the pharmacist look up DIS profiles after a Prescription Monitoring Profile alert was received in January 2017. The employee observed the pharmacist make notes about what was viewed and then call her spouse on the phone to determine if the subject of the alert was someone known to them socially.
- An employee found the notes made by the pharmacist following an apparent unauthorized access and kept the evidence, eventually providing it to the district manager in September 2017.
- An employee observed the pharmacist look up an individual in the DIS whom she had been in a motor vehicle accident with; several staff at her child's school; her child's therapist; and her family doctor.
- An employee reported that she was consulted by the pharmacist to assist in fabricating reasons for her access of the DIS in response to audit activity by the College of Pharmacists.
- An employee expressed concern that, although it was not directly witnessed, the pharmacist had also viewed the DIS profiles of other employees at the corporate location, including the employees supervised by the pharmacist.
- An employee reported that the pharmacist solicited her to obtain patient contact information from the local POS system after her termination.
- An employee confirmed her spouse was approached by the pharmacist at their home with a document the pharmacist had prepared for signature that claimed the individual had consented to the access and fabricating a reason for the access. This employee also had second hand knowledge that the pharmacist had approached up to a dozen other affected individuals in a similar manner.

[44] In total, the evidence establishes that 46[3] individuals' personal health information was accessed on the DIS by the pharmacist without authorization. Of those, 28 were not customers

[3] Thirty-nine originally confirmed by the DHW in conjunction with Sobeys; 1 identified after Sobeys re-interviewed its employees; 4 identified by OIPC investigation as being validated without merit; 2 identified by OIPC investigation as evidence supports the conclusion despite not being captured in the DHW audit.

of Sobeys and so the pharmacist created records in the Sobeys POS system for those 28 individuals without authorization.

[45] Following my interim recommendation on March 29, 2018, the DHW took additional steps to contain the breaches by sending a letter to the pharmacist directing her to cease and desist using or discussing any information gained from the inappropriate access of the DIS, to destroy any copies in her possession or provided to others, and to provide the DHW with a list of individuals to whom information from the DIS was shared.

[46] On May 22, 2018, following my interim recommendation, Sobeys shared the results of its additional investigation results with the DHW, including the identity of one additional affected individual and evidence that the pharmacist had improperly used the DIS data of the affected individuals.

3.0 Issue

[47] The issue in this investigation was did Sobeys take reasonable steps in response to the privacy breaches as required by ss. 61 and 62 of *PHIA*?

4.0 Analysis and Findings

4.1 Did Sobeys take reasonable steps in response to the privacy breaches as required by ss. 61 and 62 of *PHIA*?

[48] *PHIA* requires that health custodians protect the confidentiality of personal health information and that they do so by implementing practices that are reasonable in the circumstances.[4]

[49] When we evaluate the reasonableness of security of personal information following a privacy breach, we consider whether the health custodian followed best practices in managing the breach. These best practices are known as the "four key steps" which include:[5]

1. Contain the breach and conduct an investigation
2. Evaluate the risks
3. Notification
4. Prevention

---

[4] *PHIA* ss. 61 and 62. For a detailed discussion of the meaning of "reasonable security" see Investigation Report IR18-01 at para 66.

[5] This practice is articulated by the OIPC in our guidance document "Key Steps to Responding to Privacy Breaches" available on our website at https://foipop.ns.ca/. It follows the same approach other jurisdictions use. See, for instance: the Office of the Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches": https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf; the Office of the Information and Privacy Commissioner for British Columbia, "Privacy Breaches: Tools and Resources": https://www.oipc.bc.ca/guidance-documents/1428; the Office of the Information and Privacy Commissioner of Alberta, "Key Steps in Responding to Privacy Breaches" https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf; and the Office of the Information and Privacy Commissioner of Ontario, "Privacy Breach Protocol: Guidelines for Government Organizations": https://www.ipc.on.ca/wp-content/uploads/Resources/Privacy-Breach-e.pdf.

Step 1: Contain the breach and conduct an investigation

[50] Sobeys did not immediately begin an investigation upon the district manager receiving information from a pharmacy employee about the pharmacist's questionable access of the DIS on August 23, 2017. Instead, Sobeys' investigation was prompted by its receipt of the first batch of audit results from the DHW. After determining that there was no documentation in the system to explain the access, Sobeys interviewed the pharmacist.

[51] During the interview meeting on September 15, 2017, the pharmacist provided answers in six of eight instances that Sobeys considered to be departures from known and acknowledged corporate policies and Sobeys immediately terminated the pharmacist's employment. Sobeys immediately secured the pharmacist's keys to the pharmacy and deactivated her passcodes and POS system login credentials. These prompt actions contained the immediate cause of the privacy breaches and prevented further unauthorized use of the DIS.

[52] Sobeys provided specific answers to the DHW questions about the instances of access provided by the DHW audit logs but did not volunteer any information about the relationships between the pharmacist and affected individuals or what was observed by pharmacy employees and shared with the district manager in September 2017, nor from the initial employee concerns raised in August 2017.

[53] In its summary of additional investigation steps provided to this office in April 2018, Sobeys confirmed that the sheet containing personal health information from the DIS created by the pharmacist and left in the pharmacy was given to the district manager by a pharmacy employee in September 2017. It was "misplaced and believed to have been inadvertently destroyed, however, in moving offices this month it was located." Sobeys did not carefully preserve evidence of the pharmacist's use of the DIS information supplied to it by its employee nor did it adequately protect the personal health information contained in that evidence.

[54] Sobeys' management staff confirmed that they did not find the pharmacist credible in her accounts of accessing the DIS during the September 15, 2017 interview. Sobeys' management staff also confirmed that they received some information from other employees in September 2017 and shared that information with the director of quality and regulatory but not in a formal way. During our interview with the director of quality and regulatory on March 1, 2018, she indicated general knowledge of the key steps to privacy breach management.

[55] In December 2017, Sobeys developed a key message for any individuals who might inquire about the matter and provided those messages to pharmacy staff who may need to respond to inquiries. A similar key message was issued to the OIPC at the outset of this investigation. The statement was: "We do not have evidence that [the pharmacist] did more with the information than view it."

[56] As of the end of September 2017, Sobeys did have in its possession information about some of the relationships between the pharmacist and affected individuals. It also had possession of a sheet of paper containing an individual's personal health information created by

the pharmacist, had knowledge that at least five false profiles had been created within the local POS system and had possession of knowledge of some of the pharmacy employees' concerns and some of their observations related to the purposes behind the pharmacist's unauthorized accesses to the DIS.

[57] The evidence established that Sobeys had sufficient information in its possession by the end of September 2017 to determine on a reasonable basis that the pharmacist's actions went beyond viewing the information and that the circumstances required additional investigation to fully ascertain the scope and nature of the breaches. Sobeys had sufficient information to know that there was a real risk that the pharmacist could further use or disclose the information, and further, that the pharmacist was not innocently viewing records; she was actively searching for information about targeted individuals with whom she had some pre-existing relationship. This should have prompted Sobeys to conduct an immediate investigation into the circumstances of these breaches to better understand the risks. On March 1, 2018, I made a recommendation to Sobeys that it conduct a more thorough investigation into the circumstances and it did so.

[58] On December 18, 2017, Sobeys notified the DHW of the pharmacist's attempt to contact at least one affected individual and that it suspected that the pharmacist would attempt to contact other affected individuals in a similar manner. By doing so, Sobeys appeared to understand that the behaviour was problematic and thought the DHW would accelerate its notification plans as a result. The pharmacist's actions were a continued breach of the privacy of affected individuals whom she contacted following her dismissal from Sobeys. Sobeys did not recognize this as a continued breach of the individuals' privacy that required containment.

[59] Further, Sobeys did not provide us with any breach management protocol or investigation strategy document specific to the investigation of privacy breaches. Sobeys' evidence was that its Privacy Breach Protocol is contained in its Privacy Operational Standards. The Privacy Operational Standards contains a section on Privacy Breaches and Complaints that provides general guidance to employees to use the online Quality Related Event reporting tool and states that the pharmacy manager will investigate. The Privacy Operational Standards does not address breach containment, investigation, risk assessment or notification procedures, nor does it address how a breach will be dealt with if it is caused by the pharmacy manager. My office has published guidelines on the management of privacy breaches. These guidelines, known as the *"*Key Steps to Responding to Privacy Breaches",[6] provide guidance on how to manage a privacy breach.

[60] **Finding #1**: I find that Sobeys failed to act in a timely fashion to properly and thoroughly investigate and contain these privacy breaches.

[61] The recommended solution to this problem is tied to the risk assessment phase of breach management and is discussed below.

---

[6] Key Steps to Responding to Privacy Breaches, available on the OIPC website: https://foipop.ns.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf

[62] With regard to the 28 instances where the individuals were not already clients of the pharmacy, the pharmacist was prompted by the system to create local profiles in the POS system in order to access the DIS profiles of those individuals. The creation of these false profiles is a separate breach of those individuals' privacy by creating a new health record at a pharmacy that is unrelated to the provision of health services. The record itself is clearly personal health information and contains information about the individual drawn from the provincial Client Registry.

[63] In 13 instances, the profiles created indicate that the privacy consent from the individual is "unknown". This is a system generated default when the pharmacy employee who created the profile failed to enter the consent status of the individual. In two instances, the pharmacist actively entered consent information into the profile, which are believed to be false entries.

[64] In another 13 instances, the profiles created indicate that the privacy consent from the individual was "verbal". The evidence establishes that these 13 "verbal consents" were created on March 8, 2017 as a result of a technical choice during a system transition. This compounds the confusion and falsity of the profiles.

[65] The existence of these records may cause confusion if it is thought to be a true record of providing health services from that location. If an individual were to attend that pharmacy in the future, it may be quite shocking to find that a profile already exists. Another user of the local POS system may access the profile and erroneously believe that services were provided there or that the consent statements they contain are accurate. Sobeys took no steps to contain this aspect of the breaches, having failed to assess these acts as separate and distinct privacy breaches.

[66] **Finding #2:** The breaches have not yet been contained while the 28 false profiles exist in Sobeys POS system.

[67] The recommended solution to this problem is tied to the required notification and is discussed below.

Step 2: Evaluate the risks

[68] The next step in appropriately managing a privacy breach is to evaluate the risks. To evaluate the risks associated with this series of breaches, it is necessary to evaluate a number of factors including the nature of the personal information involved, relationship between the parties, containment efforts, cause and extent of the breaches and foreseeable harm from the breaches.

[69] I completed a thorough evaluation of the risks relevant to these privacy breaches in Investigation Report IR18-01. I adopt that assessment here and conclude that the risks associated with these breaches were high.

[70] It bears repeating in the context of this investigation report that the risk of authorized users engaging in unauthorized access of personal health records is a significant and foreseeable risk for any health information custodian. Even despite professional ethical standards, policies and

training, some individuals continue to operate with a total disregard for the privacy of the individuals served by the health care system. Trust for custodians and the health care system in general is damaged when custodians do not appreciate the constant risk from authorized users abusing their authority. As electronic records and broad access to health information proliferates, the nature of this risk continues to augment.

[71] Sobeys' evidence was that it expects and assumes that regulated pharmacists will comply with their professional ethical standards as regulated by the College of Pharmacists and that intentional privacy breaches are rare and unusual. This investigation demonstrates that despite the safeguards provided by a regulated health profession or appropriate employment policies, the risk of privacy breaches from authorized users cannot be underestimated.

[72] **Finding #3:** I find that at the time of the discovery of these breaches, Sobeys did not properly assess the risk of unauthorized access by authorized users.

Recommendation #1: Breach Management Protocol
I recommend that, within six months, Sobeys:

i. Develop and implement a privacy breach management protocol consistent with the OIPC's *Key Steps to Responding to Privacy Breaches* guidance.
ii. Include in the protocol an informed assessment of the risk of unauthorized access by authorized users.
iii. Provide training to its National Pharmacy Group corporate leadership and district managers in *PHIA* privacy breach containment and investigations to equip them with sufficient knowledge and understanding to adequately contain, investigate and assess the risk of a privacy breach in a timely manner.

Step 3: Notification

[73] The third step in managing a privacy breach is to determine whether notification is appropriate and necessary. Section 69 of *PHIA* requires the custodian to notify individuals at the ***first reasonable opportunity*** if the custodian believes on a reasonable basis that, as a result of the breach, there is potential for harm or embarrassment to the individual.

[74] The DHW took the lead on notifying affected individuals of the privacy breaches involving the DIS and did so on December 22, 2017.

[75] However, Sobeys made no attempt to contact the 28 individuals who were affected by the separate privacy breaches concerning the creation of false local profiles in the Sobeys POS system. Sobeys was aware of the content of the DHW's notification letters and should not have relied on this as providing this specific sub-set of affected individuals with appropriate notification of the breaches of its system. Sobeys failed to appreciate that its own electronic system had also been breached. In this circumstance, it would make sense to separately inform the affected individuals of how the false profiles came to be created with reference to the DHW notification and to notify of steps taken to mitigate or delete them.

[76] *PHIA* requires that health custodians notify affected individuals where the custodian has a reasonable basis to believe that the information has been subject to unauthorized access, use, disclosure, copying or modification. In this case, the pharmacist engaged in unauthorized copying of personal health information from the provincial Client Registry into Sobeys' POS system.

[77] **Finding #4:** I find that Sobeys was not in compliance with *PHIA* when it failed to provide notification to 28 individuals of the privacy breaches within its local POS system.

Recommendation #2: Breach Notification
I recommend that Sobeys immediately notify the 28 individuals whose personal information was improperly copied into the Sobeys POS system. A confidential hard copy of each profile should be provided to each affected individual with the breach notification letter.

Recommendation #3: Delete False Local POS System Profiles
I recommend that Sobeys take immediate steps to contain the breaches resulting from the false local profiles created in the Sobeys POS system by deleting those profiles. Before deleting the POS system profiles, Sobeys should prepare one confidential hard copy of each profile to be provided to each affected individual.

Step #4: Prevention

[78] The final step in managing a privacy breach is to develop strategies to prevent a future occurrence. Strategies should address both the immediate causes of the present breach and should improve the public body's ability to detect and manage future breaches.

[79] Typically, prevention strategies will address privacy controls in all of the following areas:

1. Physical controls
2. Administrative and personnel controls
3. Technical controls

[80] The information practices required of a custodian must be reasonable in the circumstances and must ensure that personal health information in the custodian's custody or under its control is protected against theft or loss and unauthorized access, use, disclosure, copying or modification.

Physical controls

[81] Physical safeguards by Sobeys were not a factor in this investigation and were not reviewed.

Administrative and personnel controls

[82] The administrative safeguards we reviewed in this investigation included: Sobeys Privacy Management Framework, Policies and Processes, Ongoing Staff Training, Workplace Culture, and Continuous Quality Improvement Audit – Pharmacy.

Sobeys privacy management framework

[83] Sobeys' privacy management framework operates under the general oversight and guidance of Sobeys' chief privacy officer. It is a national program of "…policies and procedures designed to comply with all applicable federal and provincial privacy legislation across Canada."

[84] The chief privacy officer position is a member of the corporate senior executive and the Audit Committee of the Board of Directors receives quarterly information about privacy breaches. The individuals responsible for implementation and adherence are senior level executives.

[85] There appears to be a commitment to be responsive to privacy issues as they arise. For example, the chief privacy officer described that a gap analysis is conducted "…any time an incident occurs at a Sobeys Pharmacy, a sector trend is noticed which has privacy relevance, a change in privacy legislation…or they become aware of incidents occurring at non-Sobeys pharmacies involving a privacy issue."[7]

[86] In response to this series of breaches, Sobeys identified and took the following corrective actions:[8]

1. Remediation of the work environment at the local pharmacy and additional training provided to staff regarding the Sobeys ethics reporting line.
2. Discussions with pharmacy staff.
3. Recommunication of expectations regarding accessing provincial health records in the form of quality communications and a strongly worded human resources memorandum.

[87] Sobeys also identified additional preventative measures it is undertaking to implement:

1. Improved auditing by producing a report to be provided to district managers to help identify higher risk access activities.
2. Increased frequency of continuous improvement audits to twice yearly, with one audit to be completed with a staff pharmacist (non-manager).
3. Discussions on privacy, requirements and expectations included in Sobeys Pharmacy Manager Meetings (scheduled for June 2018).
4. All Nova Scotia pharmacy staff members required to review and re-complete the DIS Confidentiality Oath as part of the 2018 annual policy review and acknowledgement process on an annual basis.

[7] Sobeys chief privacy officer statement, May 22, 2018.
[8] Sobeys chief privacy officer statement, May 22, 2018.

[88] Our investigation identified two areas where Sobeys' pan-Canadian approach to its pharmacy privacy responsibilities loses the nuance and prescriptive detail of the provincial personal health information legislation which can be misleading.

[89] First, Sobeys' policy documentation and information directed toward staff emphasizes the *Personal Information Protection and Electronic Documents* Act (*PIPEDA*) as the applicable legislation. In its Privacy Operational Standards policy document, under Privacy Laws and Consent, the first reference is to the federal *PIPEDA* legislation. The policy states, "Most provinces also have legislation specific to protecting personal health information." However, the actual provincial legislation and specific implications are not identified in the policy document.

[90] In its Pharmacy Quality – Weekly Reminder, there are some excerpts from the Privacy Operational Standards policy document relating to accessing patient information. Under the Reference Documents supplied with the Weekly Reminder, there is a link to the federal *PIPEDA* legislation and a statement, "Provincial Practice Directions/Standards (see your provincial website for standards)". There is no mention of provincial personal health information legislation in this Weekly Reminder.

[91] Sobeys, as a commercial enterprise, is subject to the federal *PIPEDA* legislation when it collects, uses and discloses personal information generally. However, Nova Scotia's *PHIA* legislation, along with other provincial personal health information legislation, has been designated by the federal Governor in Council as "substantially similar" to *PIPEDA* legislation. As such, the *PIPEDA* legislation does not apply to the personal health information aspect of the enterprise in Nova Scotia. It is explicitly the Nova Scotian legislation that applies to the custodian of personal health information in this province, even though *PIPEDA* applies to other aspects of the commercial enterprise.

[92] By not explicitly and accurately signaling to employees the correct applicable laws, Sobeys glosses over the nuance and details specific to the regulation of personal health information, including the prosecutable offences in relation to accessing and handling of personal health information that are a feature of *PHIA* in Nova Scotia.

[93] Personal health information is a specific type of personal information subject to a statutory regime specifically designed for the health care context. The federal Governor in Council "substantially similar" scheme does not leave open to the corporate entity to choose which law it cares to apply.

[94] The second significant area in which Sobeys' national approach is misleading is with its notification to patients about privacy, personal health information practices and information about complaints procedures. Section 68 of *PHIA* requires a custodian to make available to the public a written statement providing a description of the custodian's information practices, contact information and how to request access to or correction of personal health information.

PHIA specifically requires the public written statement to include information about how to "…make a complaint under this *Act* to the custodian and to the Review Officer."[9]

[95] Sobeys' public notification statement is in the form of a brochure. The brochure covers the information required, except that where it directs patients about inquiries or complaints to an oversight body, it directs them to the Privacy Commissioner of Canada (the Commissioner responsible for *PIPEDA* legislation). When we inquired about this, the Sobeys corporate representative held the view that this brochure appropriately directs individuals on the basis that if individuals called the Privacy Commissioner of Canada they would likely be re-directed to the appropriate privacy commissioner for their province or territory and that it is unreasonable to suggest that Sobeys should produce different versions of its brochure relevant to each jurisdiction in which it operates pharmacies.

[96] Not only is this not in compliance with *PHIA*, this approach risks that an individual patient may not persevere through the challenge of being incorrectly directed in the first instance by the Sobeys' notification.

[97] **Finding #5:** Sobeys' pan-Canadian approach to its pharmacy privacy program is inaccurate and not in compliance with Nova Scotia's health privacy legislation.

Recommendation #4: Apply Provincial Health Privacy Law
I recommend that within 45 days, Sobeys:

i. Correctly reference the applicable personal health information laws within its Privacy Operational Standards for pharmacies, as well as within any staff training materials.
ii. Produce and distribute a public information brochure in Nova Scotia that correctly identifies the applicable legislation and that correctly directs people with privacy complaints or questions to the Office of the Information and Privacy Commissioner for Nova Scotia.

Policies and processes

[98] Sobeys has implemented two relevant policies: the Privacy Operational Standards and the Code of Business Conduct and Ethics. Together, these policies set out the foundation for Sobeys expectations of its staff relating to privacy and conduct. On May 31, 2017, Sobeys National Pharmacy Group circulated a memorandum to all pharmacies operating under its banner to implement harmonized alignment of standards and procedures as the National Pharmacy Group.

[99] The current Privacy Operational Standards document outlines anticipated and acceptable circumstances for accessing patient electronic health records, making note that provincial drug information systems may require a specific additional oath or pledge. The policy clearly states: "These standards supplement and reinforce any provincial regulations governing privacy and the use of electronic drug information systems/electronic health records" and, "It is not permissible or acceptable to access a patient's EHR outside the course of providing care."

[9] *PHIA*, s. 68(d). Note that the Information and Privacy Commissioner for Nova Scotia serves as the "Review Officer" for the purposes of *PHIA*.

[100] The Code of Business Conduct and Ethics provides employees with clear statements about what constitutes unethical behaviour, which includes violations of corporate polices and operational standards. The Code also outlines the consequences of unethical behaviour and multiple mechanisms for reporting ethical concerns, including anonymous reporting.

[101] Along with the implementation of harmonized policies and standards, the National Pharmacy Group implemented a requirement that all pharmacy staff confirm their understanding and acknowledgement of the policies by June 30, 2017. All members of the local pharmacy staff at issue in this investigation signed the acknowledgement, including the pharmacist, on June 27, 2017.

[102] Previous to this harmonized policy statement, Sobeys pharmacies had a similar process of requiring employees to sign an acknowledgement of policies. The pharmacist previously signed an acknowledgement of the policies in place at the time on June 26, 2015, which included the following policies: a Code of Behaviour, Protecting Patient and Corporate Information, Privacy Operational Standards and Accessing Electronic Health Records.

[103] **Finding #6:** Sobeys policies provide adequate administrative safeguards by explicitly prohibiting employees from accessing patient personal health information outside of the provision of health care services and by providing employees clear ethical rules and reporting mechanisms, with one identified area of improvement noted in the below section. Sobeys practice of requiring employees to regularly acknowledge the Privacy Operational Standards is a best practice to ensure employees are aware of the policies.

Ongoing staff training

[104] Sobeys has implemented a program of Quality - Weekly Reminders and Monthly Quality Tips to operationalize its policies. This ongoing program is designed to highlight aspects of the policies, to inspire conversation at local pharmacies and to clarify areas where they may have received questions or identified issues. On April 22, 2017, the Weekly Reminder took excerpts from page 6 of the Privacy Operational Standards, including the statement that it is not permissible or acceptable to access a patient's electronic health record (EHR) outside the course of providing care.

[105] In response to this series of breaches, on December 2, 2017, Sobeys circulated a Monthly Quality Tip about accessing electronic health records which states: "Access to the EHR is balanced with regulations to protect patient privacy. Be familiar with your provincial PHIA requirements as well as corporate privacy operational standards." In addition, it states: "It is prudent for pharmacy staff to ensure there is pharmacy care activity documented in conjunction with access to a patient's provincial record." The tip provides guidance to take additional steps to document the reason for the access for over-the-counter or non-dispensing situations. Its conclusion is, "These practices ensure that you can demonstrate compliance with privacy practices if audited."

[106] Sobeys developed an online policy training module and required all pharmacy staff to complete it as part of its rollout of the updated and harmonized policies.[10] Sobeys now requires an annual renewal of the online training module and written acknowledgement of policies.[11] The pharmacist completed the online training module in February 2017.

[107] **Finding #7:** Sobeys' ongoing training and program of Monthly Tips and Weekly Reminders is an effective strategy to emphasize and revisit policy documents and messages with employees.

Recommendation #5: Document Reasons for DIS Access
I recommend that Sobeys make documenting the reason for DIS access for over-the-counter or non-dispensing situations a required privacy operational standard.

Workplace culture
[108] In response to this series of privacy breaches, Sobeys identified a concerning workplace culture of staff not disclosing their knowledge of the privacy breaches earlier.

[109] Our investigation identified two elements present in the workplace that contributed to employees not disclosing their knowledge of the pharmacist's behaviour. First, there was a perception that the pharmacist was knowledgeable and respected, which contributed to a sense that an employee that came forward would not be believed or would be at risk of retribution if the behaviour could not be proved. The second is that an inexperienced employee was not sufficiently confident in her understanding of the Privacy Operational Standards to challenge the supervisor, although when an occasion arose, that employee discussed some of her observations with a relief pharmacist who confirmed that the behaviour as described was not appropriate.

[110] The relief pharmacist, an experienced regulated pharmacist, admitted during our investigation that she did not believe the pharmacy employee because she had known the pharmacy manager (pharmacist) for a long time and respected her. She did not report the matter to Sobeys.

[111] The employees described a difficult work environment as their discomfort with the behaviour grew but they were not certain how to address it. One employee eventually called in an anonymous tip to the DHW rather than report the behaviour to her employer.

[112] Sobeys identified three steps of corrective action: remediating the work environment at the local pharmacy, initiating discussions with pharmacy staff and recommunicating expectations regarding accessing provincial health records.

[113] The supervisory dynamic as a deterrent to employees recognizing and reporting unauthorized access of health records cannot be underestimated. The challenge is even more pronounced in a small workplace where there are few staff and the identity of the reporting employee is difficult to protect. In a rural community, where there may be few other

[10] Sobeys letter to the OIPC, Feb 1, 2018.
[11] Sobeys chief privacy officer statement, May 22, 2018.

employment opportunities, the risk to an employee coming forward including facing retribution, losing her employment, or being forced to continue in the work environment due to lack of other options, is significant.

[114] **Finding #8:** Sobeys' corrective actions to remediate the work environment, discuss the issues with staff and recommunicate the expectations and anonymous reporting procedure, are appropriate remedial steps.

Recommendation #6: Build Employee Confidence in the Workplace
I recommend that Sobeys:

i. Require all of its pharmacy staff and management in Nova Scotia to read this report.
ii. Specifically discuss with employees how the supervisory dynamic deterred the employees coming forward sooner in this case and emphasize the corporate commitment to address issues that are reported regardless of whether the individual is a supervisor or a long-term, respected employee.

Continuous Quality Improvement Audit

[115] The pharmacy's Continuous Quality Improvement Audit contains 20 questions to be answered by a district manager on a site visit, including ensuring that the personal health information brochure is readily available, that top fax numbers are pre-programmed to reduce the potential of misdirected faxes, that staff are aware of the location of "privacy tools and information on the pharmacy web portal" and that staff understand their responsibility to report "Quality Related Events" (QRE) on a dashboard. It also includes a requirement to check that the pharmacy manager at the pharmacy being visited by the district manager has followed up on all QRE as required by Sobeys policy.

[116] A Continuous Quality Improvement Audit was conducted for the local Sobeys pharmacy as required, but did not identify any issues in this pharmacy. Sobeys' corrective action included an effort to increase the frequency of continuous improvement audits to twice yearly, with one audit to be completed with a staff pharmacist (non-manager).

[117] Sobeys' corrective action is intended to improve the Continuous Quality Improvement Audit to address that it failed to identify any issues at this pharmacy. However, the identified corrective action to the Continuous Quality Improvement Audit is not sufficient to address the root cause of the audit's failure in this case.

[118] Our investigation revealed that the audit process, as implemented at this local pharmacy, involved filling out the check-boxes based on a relatively short meeting with the pharmacist. A more frequent but similar check-box exercise may not produce better results. Furthermore, depending on the size of the pharmacy, another regulated pharmacist may not be able to provide the most relevant information. In this case, the non-regulated pharmacy staff had the most information and insights about the pharmacist's behaviour because they were more likely to be working at the same time as the pharmacist.

[119] **Finding #9:** Sobeys' Continuous Quality Improvement Audit provides an appropriate framework for a regular audit process, but its implementation is perfunctory and does not

sufficiently record evidence of the pharmacy's compliance. The identified corrective action does not address the workplace culture issues that contributed to the audit's failure at this pharmacy.

Recommendation #7: Strengthening the Continuous Quality Improvement Audit
I recommend that Sobeys improve its Continuous Quality Improvement Audit process by:

i. Conducting three Continuous Quality Improvement Audits per year and involve a non-pharmacist in the completion of at least one audit per year.
ii. Adding a question to the Continuous Quality Improvement Audit for all staff that asks them to identify any privacy compliance concerns or recommendations.
iii. Adding a regular review of the proactive monitoring logs to the Continuous Quality Improvement Audit process (once the POS system has an adequate proactive user activity monitoring program - see recommendation 8 below).

Technical controls

[120] The technical safeguards that we reviewed in this investigation were user activity logs and the auditing of logs. The DHW has a proactive user activity audit program in place but it did not successfully identify the pharmacist's activities over the two years that she abused her authorized access. Over the period of the pharmacist's unauthorized accesses, Sobeys did not have any kind of user activity audit program in place.

[121] Auditing offers an electronic footprint of what a user did or accessed and can be a powerful source of evidence of a privacy breach. However, the information coming from an audit tool needs to be calibrated. Although a powerful technological requirement for any custodian, it cannot supply all of the safeguards alone. The details of user activity data, configurations and use of the tool are also important considerations.

[122] Sobeys conducts annual audits of access control[12] to ensure that users are granted appropriate system access. Prior to this investigation, Sobeys had not implemented any form of proactive auditing of its user activity. Sobeys communicated during this investigation that the POS system it uses does not have a proactive auditing functionality.

[123] Sobeys confirmed that user access profiles which report user activity can be done by patient name, but it is cumbersome and not useful as a tool to monitor authorized user activity. The district manager confirmed that no regular proactive user access monitoring is currently being done by Sobeys.

[124] The DIS User Agreement with the DHW requires a user organization to "…monitor access of its staff to the DIS to ensure proper access, use, and disclosure of personal health information in the DIS." Proactive monitoring of user activity is widely acknowledged as a reasonable and necessary technical safeguard to address the general risk of unauthorized access

[12] This is an audit to ensure that employees have the access necessary for their roles and any employees who have left the organization have their access terminated.

by authorized users and is a significant trend in the electronic health records field.[13] Proactive user activity monitoring typically takes the form of periodic review of users' total activity according to set criteria, as well as system generated automatic alerts to pre-programmed suspicious activity.

[125] Sobeys has since determined that it can develop a report of "non-transactional" activities, that is, look-up activities that are not associated with pharmacy transactions which, according to Sobeys, can be used on a regular basis to identify trends and assess adherence to access and documentation standards. At the time of writing this report, Sobeys was reviewing and refining this report with a view to implementing it at the pharmacy district manager level as an additional component of its existing Continuous Quality Improvement Audits twice per year.

[126] The report of "non-transactional" activities is an example of suspicious user behavior, but the proposed report incorporated into a twice per year Continuous Quality Improvement Audit, is not an automatic system-generated alert program. As proposed, this report offers a regularized selective user activity audit and is an improvement over Sobeys' current status. Other types of suspicious user behaviour include looking up: family members or individuals with the same last name, co-workers and individuals who are famous or have notoriety in the community.

[127] **Finding #10:** I find that Sobeys is not in compliance with the DIS User Agreement requirement to conduct regular auditing of user activity and does not have reasonable technical security in place capable of the timely identification of unauthorized access by authorized users.

Recommendation #8: Strengthening Technical Auditing
I recommend that within six months, Sobeys obtain and implement the technical auditing capacity to regularly conduct proactive user activity audits of its POS system, including at a minimum, flagging same name lookup, employee lookup, and activity in the POS system not associated with dispensing.

5.0 Summary of Findings and Recommendations

[128] I find that:

#1: I find that Sobeys failed to act in a timely fashion to properly and thoroughly investigate and contain these privacy breaches.

#2: The breaches have not yet been contained while the 28 false profiles exist in Sobeys POS system.

---

[13] BC Investigation Report F06-01; Ontario Order MC09-9; BC Investigation Report F06-01; 2013-IR-02, 2013 CanLII 82405(AB OIPC); Order H2016-06(Re), 2016 CanLII 104927 (AB OIPC); Order H2014-02 (Re), 20104 CanLII 41751 (AB OIPC); Eastern Health (Re), 2016 CanLII 85236; A Public Hospital, 2017 CanLII 88475 (ON IPC); London Health Sciences Centre (Re), 2017 CanLII 31432 (ONIPC); Group Health Centre (Re), 2017 CanLII 87957 (ON IPC); Heartland Regional Health Authority (Re), 2015 CanLII 85349 (SK IPC); Regina Qu'Appelle Regional Health Authority (Re), 2013 CanLII 5640 (SK IPC); L&M Pharmacy Inc (Re), 2010 CanLII 17914 (SK IPC);Manitoba Ombudsman Case 2014-0500.

#3: I find that at the time of the discovery of these breaches, Sobeys did not properly assess the risk of unauthorized access by authorized users.

#4: I find that Sobeys was not in compliance with *PHIA* when it failed to provide notification to 28 individuals of the privacy breaches within its local POS system.

#5: Sobeys' pan-Canadian approach to its pharmacy privacy program is inaccurate and not in compliance with Nova Scotia's health privacy legislation.

#6: Sobeys policies provide adequate administrative safeguards by explicitly prohibiting employees from accessing patient personal health information outside of the provision of health care services and by providing employees clear ethical rules and reporting mechanisms, with one identified area of improvement noted in the below section. Sobeys practice of requiring employees to regularly acknowledge the Privacy Operational Standards is a best practice to ensure employees are aware of the policies.

7: Sobeys' ongoing training and program of Monthly Tips and Weekly Reminders is an effective strategy to emphasize and revisit policy documents and messages with employees.

#8: Sobeys' corrective actions to remediate the work environment, discuss the issues with staff and recommunicate the expectations and anonymous reporting procedure, are appropriate remedial steps.

#9: Sobeys' Continuous Quality Improvement Audit provides an appropriate framework for a regular audit process, but its implementation is perfunctory and does not sufficiently record evidence of the pharmacy's compliance. The identified corrective action does not address the workplace culture issues that contributed to the audit's failure at this pharmacy.

#10: I find that Sobeys is not in compliance with the DIS User Agreement requirement to conduct regular auditing of user activity and does not have reasonable technical security in place capable of the timely identification of unauthorized access by authorized users.

[129] I recommend that:

#1: Breach Management Protocol
Within six months, Sobeys:

i. Develop and implement a privacy breach management protocol consistent with the OIPC's *Key Steps to Responding to Privacy Breaches* guidance.
ii. Include in the protocol an informed assessment of the risk of unauthorized access by authorized users.
iii. Provide training to its National Pharmacy Group corporate leadership and district managers in *PHIA* privacy breach containment and investigations to equip them with sufficient knowledge and understanding to adequately contain, investigate and assess the risk of a privacy breach in a timely manner.

#2: Breach Notification
Sobeys immediately notify the 28 individuals whose personal information was improperly copied into the Sobeys POS system. A confidential hard copy of each profile should be provided to each affected individual with the breach notification letter.

#3: Delete False Local POS System Profiles
Sobeys take immediate steps to contain the breaches resulting from the false local profiles created in the Sobeys POS system by deleting those profiles. Before deleting the POS system profiles, Sobeys should prepare one confidential hard copy of each profile to be provided to each affected individual.

#4: Apply Provincial Health Privacy Law
Within 45 days, Sobeys:

i. Correctly reference the applicable personal health information laws within its Privacy Operational Standards for pharmacies, as well as within any staff training materials.
ii. Produce and distribute a public information brochure in Nova Scotia that correctly identifies the applicable legislation and that correctly directs people with privacy complaints or questions to the Office of the Information and Privacy Commissioner for Nova Scotia.

#5: Document Reasons for DIS Access
Sobeys make documenting the reason for DIS access for over-the-counter or non-dispensing situations a required privacy operational standard.

#6: Build Employee Confidence in the Workplace
Sobeys:

i. Require all of its pharmacy staff and management in Nova Scotia to read this report.
ii. Specifically discuss with employees how the supervisory dynamic deterred the employees coming forward sooner in this case and emphasize the corporate commitment to address issues that are reported regardless of whether the individual is a supervisor or a long-term, respected employee.

#7: Strengthening the Continuous Quality Improvement Audit
Sobeys improve its Continuous Quality Improvement Audit process by:

i. Conducting three Continuous Quality Improvement Audits per year and involve a non-pharmacist in the completion of at least one audit per year.
ii. Adding a question to the Continuous Quality Improvement Audit for all staff that asks them to identify any privacy compliance concerns or recommendations.
iii. Adding a regular review of the proactive monitoring logs to the Continuous Quality Improvement Audit process (once the POS system has an adequate proactive user activity monitoring program - see recommendation 8 below).

#8: Strengthening Technical Auditing
Within six months, Sobeys obtain and implement the technical auditing capacity to regularly conduct proactive user activity audits of its POS system, including at a minimum, flagging same name lookup, employee lookup, and activity in the POS system not associated with dispensing.

6.0 Conclusion

[130] While Sobeys has in place some effective administrative safeguards, this investigation highlighted a number of shortcomings in Sobeys' privacy management program. Sobeys must take immediate steps to adequately notify affected individuals, contain the breach of its own system and develop the technical capacity to proactively conduct audits of user access to its system.

[131] We will publish Sobeys' response to these recommendations and investigators from my office will follow up regularly with Sobeys to ensure that all implementation measures are completed.

7.0 Acknowledgements

[132] I would like to thank the many people who cooperated with this investigation from the Department of Health and Wellness and staff and management at Sobeys. The purpose of these investigation reports is to ensure that any lessons to be learned from a privacy breach are shared for the benefit of Nova Scotians and for the education of all health information custodians.

[133] I would also like to thank Janet Burt-Gerrans, Senior Investigator, who lead this investigation and contributed to the drafting of this report.

August 1, 2018

Catherine Tully
Information and Privacy Commissioner for Nova Scotia