Office of the Information and Privacy Commissioner for Nova Scotia

INVESTIGATION REPORT IR18-01

Drug Information System Privacy Breaches

Department of Health and Wellness

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 IR18-01

August 1, 2018

Nova Scotia Department of Health and Wellness

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 Nova Scotia 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 record. 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.

[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 would suffer some form of retaliation. Our investigation and analysis as it relates to Sobeys is contained in the companion report IR18-02.

[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] Some key findings in this investigation are:

- A pharmacist engaged in unauthorized access to sensitive personal health information over a two-year period. In that time, she accessed the personal health information of 46 individuals for personal reasons. In doing so she created falsified pharmacy records.
- The DHW does not have an adequate or effective breach investigation protocol. As a result, the DHW failed to identify all affected individuals and failed to provide notification "at the first reasonable opportunity" as required by law.
- While there are some effective administrative safeguards in place, they were not effectively used and are not sufficient to protect Nova Scotians from this type of "snooping" behaviour.
- The DHW has failed to adequately audit the organizations who have been granted access to the Drug Information System.
- The DHW does not have sufficient safeguards in place to protect the database content of its broadly defined electronic health information systems.

[8] In summary, I make 10 recommendations:

1. The DHW develop and implement an effective investigation protocol for the DIS that ensures the DHW takes the lead and has authority to determine corrective action.
2. The DHW re-contact all 46 affected individuals to determine if the pharmacist has been in contact with them since April 2018. If so, the DHW must take further legal action to prevent the ongoing unauthorized use or disclosure of the personal health information.
3. The DHW revise its Privacy Breach Protocol to prescribe that where a user is found to have breached the privacy of any individual(s) via one of the electronic databases, detailed audits of that user's activity in other implicated databases are automatically conducted.
4. The DHW revise its Privacy Breach Protocol to clarify that notification at the first reasonable opportunity requires that notification occur within days and to ensure that notification letters include clear and specific information regarding the breach.
5. The DHW establish a protocol for investigating anonymous tips on its Health Privacy 1-800 line.
6. The DHW amend the DIS User Agreement to make it mandatory that user organizations monitor and audit their own systems and to make the type and frequency of the DHW monitoring of user organization audits and audit capacity explicit.
7. The DHW conduct training for all users of the DIS on the use of DIS notations – to ensure any use of the DIS not associated with prescription activity is explained.
8. The DHW update its Privacy Policy to reflect current positions and to remove ambiguity about agency status of individuals not employed by the DHW.
9. The DHW develop more robust and systematic auditing policies and practices.
10. The DHW amend *PHIA* to add provisions that assign responsibilities for interoperable health databases in use in Nova Scotia to prescribed entities.

1.0 Introduction and Purpose of the Report

1.1 Introduction

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

[10] 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.

[11] 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 the conduct of the DHW. The companion report describes our investigation into the conduct of Sobeys.

1.2 Jurisdiction

[12] 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."

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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]

[19] 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.

1.3 Investigative process

[20] Upon initiation of this investigation, our first step was to notify the custodians of our intent to conduct two separate but simultaneous and linked investigations.

[21] We obtained and reviewed the DHW's policies, procedures, user agreements, privacy impact assessment for the DIS, inventory of personal health information contained in the DIS and records related to the discovery and investigation of the privacy breaches. We also obtained

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

and reviewed policies, procedures, computer system user manuals and records related to the discovery and investigation of the privacy breaches from Sobeys.

[22] Following the review of the documents, we interviewed the DHW's director of privacy and access, the drug information system director, and the drug information system audit specialist.

[23] Following the review of documents, we interviewed the following staff from Sobeys:

- chief privacy officer,
- national director of regulatory and quality,
- legal counsel,
- pharmacy district manager, and
- local pharmacy employees.

[24] In response to information received from the local pharmacy employees, on March 1, 2018, I made an interim recommendation that Sobeys re-interview its employees and gather further evidence in its possession regarding potential further use and/or disclosure of the information taken from the DIS system as a result of these unauthorized accesses. I further recommended that Sobeys communicate the outcome of these interviews to the DHW. On March 29, 2018, I made an interim recommendation that the DHW take additional steps to contain the breaches by writing to the pharmacist to direct that she destroy all copies of any records she had maintained and that she not further use or disclose any information obtained as a result of the unauthorized viewings of DIS data. Both Sobeys and the DHW accepted and implemented my interim recommendations.

[25] Following receipt of the breach notification letters issued by the DHW, 11 individuals contacted the DHW seeking further information. Six requested they be sent the forms to request a record of user activity and four forms requesting records of user activity were received and actioned by the DHW. In order to understand the effect of the breach on individuals and to obtain information about the possible reasons for the unauthorized viewing, OIPC investigators contacted three individuals who obtained their record of user activity. Only one individual responded and was interviewed by OIPC investigators.

2.0 Background

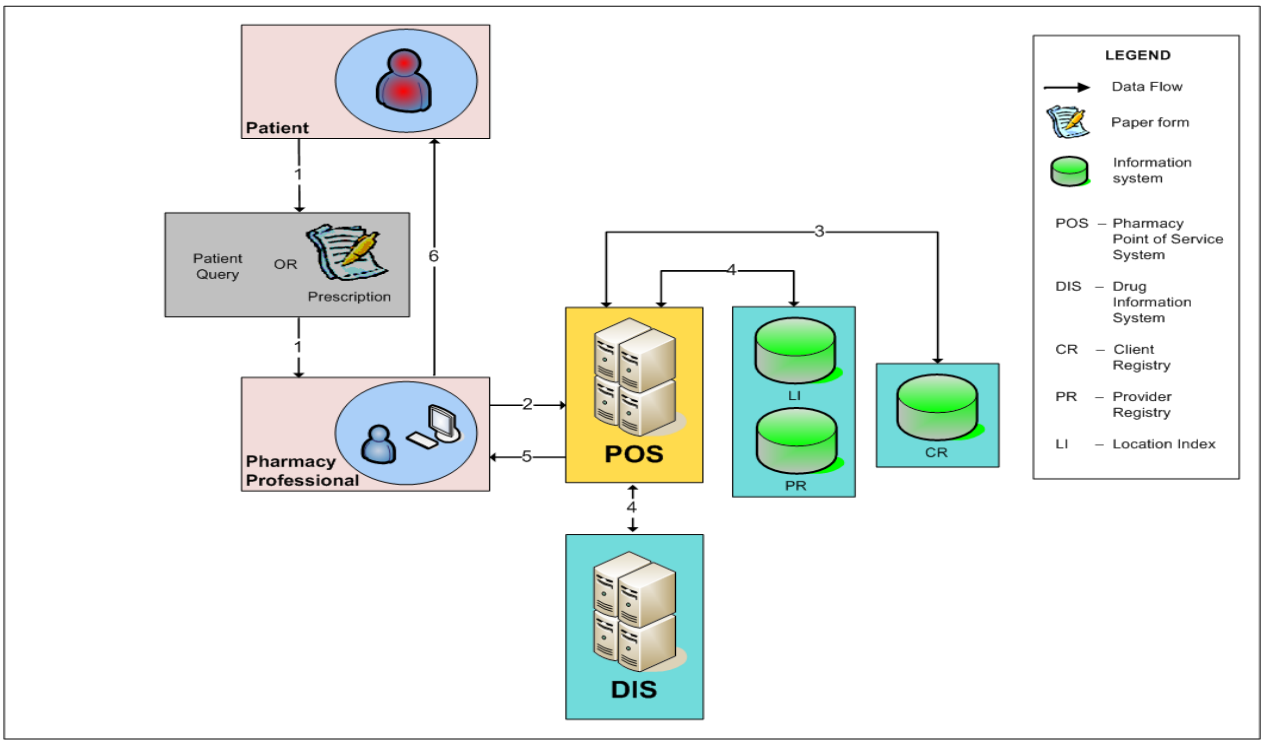
2.1 The Drug Information System – DIS

[26] Central to this investigation is the provincial Drug Information System. The DIS is a multi-user access database operated by the DHW and used by approximately 11,000 authorized users including pharmacists in community pharmacies across the province. Once granted access, a user of the DIS can access the DIS profile of any person in Nova Scotia.[3] Regulated

[3] The DIS also contains records for anyone who filled a prescription in Nova Scotia including those from out of province.

dispensing pharmacists in Nova Scotia are required to record all dispensed prescriptions in the DIS.[4]

[27] The following diagram[5] illustrates a simplified version of key technology points that are relevant in this case.



[28] The 'POS' box in the centre illustrates the local pharmacy's electronic records that exist as a local database and platform for access that interfaces with the DHW's systems. There are multiple pharmacy platforms in use by different pharmacies in Nova Scotia. By logging into the POS system, individual pharmacy users can access a locally created and stored client profile which may include information 'synched' from provincial databases as well as notes and other fields of information populated at the local level. Once into the POS system, the user has access to a tab menu called "Network". Clicking on this tab opens a menu that triggers connections with two separate provincial systems. One is the provincial Client Registry indicated on the diagram as a green cylinder called CR. The other is the DIS indicated on the diagram as a set of filing cabinets called DIS.

[4] Section 36(2) of the *Registration, Licensing and Professional Accountability Regulations* pursuant to the *Pharmacy Act* S.N.S 2011, c.11. Certified dispensers and pharmacy technicians have the same responsibility.
[5] PIA Stream 1 - (Community) Pharmacy p. 16, March 11, 2013, PNNS0102-022A.

[29] The DIS profile includes the following personal health information:

- 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.

a. The relationship between the local POS system and the DIS

[30] Through the Network menu functions the local POS user can query the DIS database for the client's DIS profile. In other words, pharmacy employees using a local POS system must access the DIS via their local POS system. They must have a local client profile created in their own system before they can access that person's DIS profile.

[31] If there is no local client profile in the POS system, users click on the Network tab in the local POS and search for the name of the individual they want to add to their local POS system. That search takes place within another provincial database – the Client Registry (indicated as the green cylinder CR in the diagram above). Once the patient or client is identified by the local user, the information can be "synched" with the user's local POS system. This creates a local client profile which is populated with basic data such as name and contact information.

[32] To access a patient's DIS information, the local user must first open the local POS client profile. From there the local user clicks on the Network tab. This sends a series of query messages to the DIS database. The database returns the results of the query messages and displays them on the local user's screen. It is at this point that the user can see the type of data listed above from the DIS – such as prescriptions, prescription history and medical conditions. The information from the DIS always remains stored in the DIS database and is not imported or 'synched' to the local system.

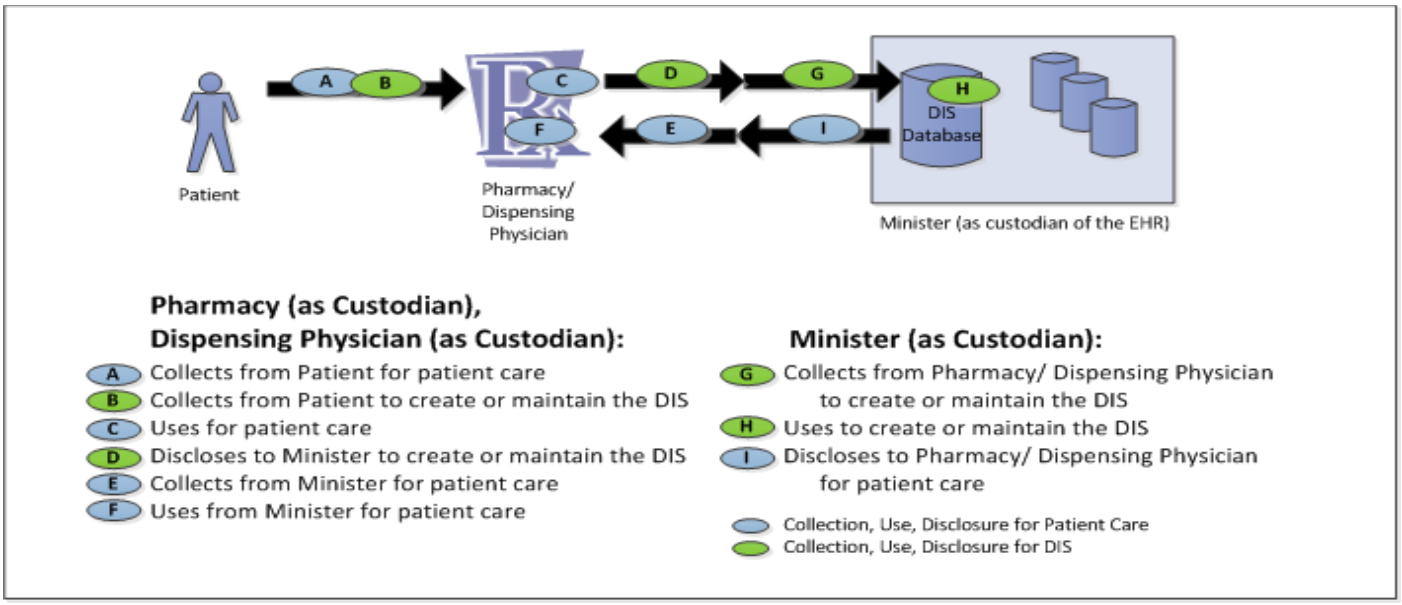
b. Auditing access to the DIS

[33] In addition to the above diagram of data information flows is the DIS logging activity which logs all user activity touching the DIS. The logging activity connects to a complicated array of technical architecture behind the scenes, involving data stored at two major data centres, the Capital District Health Authority data centre (now Nova Scotia Health Authority) and the province's information technology data centre, operated by the provincial government. Certain fields from the activity logs feed into an audit software platform called FairWarning which produces reports for audit purposes. The FairWarning software, reports and processes are administered by the Nova Scotia Health Authority.

c. Relationship between the DHW and pharmacies

[34] The DHW completed a privacy impact assessment (PIA) for the DIS in March 2013. The system went 'live' with the first pharmacy connected in November 2013 and a broader rollout

beginning January 2014. The PIA describes the relationship between the DHW and the pharmacy as a 'custodian' to 'custodian' relationship where the custodians interface and where each maintains independent responsibilities for the collection, use and disclosure of personal health information. The following diagram demonstrates the relationships. [6]



[35] The terms and conditions of the relationship between the two custodians takes the form of the "Drug Information System Joint Service and Access Policy". Pharmacy custodians can gain access for their employee users by signing the Confirmation of Acceptance of the policy. These two documents are referred to throughout this investigation report as the User Agreement. Sobeys signed its User Agreement in June 2014.

2.2 Chronology of events

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

[37] 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.

[38] Witnesses gave evidence that 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. Witnesses based their observations on the fact that they overheard the pharmacist on the telephone discussing the information accessed on a number of occasions and on the fact that the pharmacist also occasionally discussed these accesses with pharmacy employees.

[6] PIA Stream 1 - (Community) Pharmacy p. 16, March 11, 2013, PNNS0102-022A.

[39] From its investigation, the DHW established that the unauthorized accesses occurred between October 2015 and August 2017, affecting 39 individuals.[7] For 28 individuals, the pharmacist also created false POS profiles in order to access the DIS information of those 28 individuals who were not existing customers of the pharmacy. We interviewed one of the 28 individuals added to the system whose POS record indicated that she had provided verbal consent to the access of her personal health information. Her evidence was that she had never been a customer of the pharmacy, had never spoken to the pharmacist or any pharmacy employee and had no knowledge of why a customer profile had been created for her nor why the pharmacist would access her DIS profile. She also confirmed that she had never provided verbal consent to the pharmacist for any reason. However, she did recognize the pharmacist's name as a former high school classmate.

[40] The pharmacy has no other records or evidence supporting the existence of a customer relationship with those individuals. The only plausible reason for the creation of POS profiles in those instances was to facilitate access to personal health information.

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

[42] A review of the information the DHW provided regarding the 39 individuals who were originally notified of the breaches confirms that two individuals were deceased at the time of the DIS access by the pharmacist and five were under the age of 18 at the time of the DIS access.

[43] The DHW received a phone call on the Health Privacy 1-800 line[8] from a pharmacy employee on May 29, 2017 inquiring about how to make an anonymous report about suspicious use of the DIS by a pharmacist. The DHW phone log documented the received call and that the individual was concerned about being named because of fear of reprisal since the pharmacist was her supervisor. The caller left her first name and home phone number. The 1-800 call log indicates that DHW staff returned the call but there is no indication that a message was left. The evidence of the pharmacy employee was that she never received a return call.

---

[7] The OIPC investigation prompted additional analysis which identified additional affected individuals as outlined below and as referenced in the recommendations. The total final count of affected individuals is 46.

[8] The 1-800 line is answered by staff from the Health Privacy Office. The importance of this incident is further discussed in the prevention strategies section at paras 157-161.

[44] On August 14, 2017, a Nova Scotia College of Pharmacists (College) inspector called the pharmacy to arrange a site visit which took place on August 22, 2017. Our investigation failed to identify the exact catalyst for the visit, although it appears that the College was likely acting on a tip.

[45] Witnesses gave evidence that the pharmacist was concerned about the upcoming College site visit and discussed with a pharmacy employee that she was considering going on sick leave or adding notations to the files, and solicited the employee to assist in developing reasons for some of her DIS accesses.

[46] On August 23, 2017 one pharmacy employee had a conversation with the Sobeys district manager responsible for her branch in which she communicated ethical concerns she had regarding the pharmacist's use of the DIS and informed her of the recent Nova Scotia College of Pharmacists site visit.

[47] 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 initiated an audit of user activity for the period August 1 – 31, 2017. This initial audit identified eight individuals whose DIS profiles where accessed by the pharmacist but could not be explained by the logged activity in the DIS. The DIS audit specialist made this determination based on audit criteria which identifies suspicious behaviour as including logged access to a DIS profile without accompanying activity to dispense a prescription or other updates to the DIS profile within a prescribed period of time before or after the date of access.

[48] 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.

[49] Following her 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 to the district manager some of their concerns about the pharmacist's behaviour 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.

[50] 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 six invalid access events were privacy breaches.

[51] It is important to recall at this point that if an individual is not a client of the local pharmacy, and so has no record in the local POS system, the only way that a user can make a query into the DIS is to first create a client record in the POS system by getting the name and address information from the Client Registry (using the Network button in the POS system). There is no need to enter the DIS to get address or phone number information as all of that information comes from the Client Registry and is added to the local POS system when the user "synchs" the record to create the POS client record. Therefore, the pharmacist's claim that she was in the DIS looking up contact information was not believable. Furthermore, the number of steps involved in getting to the DIS profile, particularly for an individual not already a pharmacy client, are so extensive it renders a mistakenly selected name highly implausible as an explanation.

[52] To be clear, even if the pharmacist had genuinely been looking up contact information, using a sensitive health information system as a personal phone book would not have been an authorized access and would have been considered a privacy breach.

[53] 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.

[54] Once again, the audit process involved identifying instances where the DIS was accessed without corresponding dispensing activity logged in the DIS within a prescribed period of time before or after the DIS access. The results that fit the criteria identified 67 new individuals. 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. Sobeys provided the DHW with information related to valid or invalid access. By November 8, 2017, the DHW, in conjunction with 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.

[55] The DHW began drafting its notification letters to affected individuals on November 15, 2017. By December 14, 2017, the letters and mailing addresses were finalized and the letters were mailed to affected individuals on December 22, 2017. Six letters were returned to the DHW for incorrect or out-of-date addresses. On January 23, 2018, the DHW set a schedule to check its databases for updated contact information after six months. By the time of publication, DHW had reduced the number of individuals who have not yet received notice to two.

[56] 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.

[57] 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, Sobeys and the DHW reported that the immediate cause of the privacy breaches was contained.

[58] In January 2018, the DHW received follow-up inquiries from eight affected individuals shortly after they received the notification letters. Several requested specifically to know who had accessed their personal health information. One affected individual described that she had been approached by a local pharmacist from a pharmacy where she is not a customer. She found this strange and concerning. Having later received the notification from the DHW, she thought it was related and that the DHW should know. The DHW offered to produce records of user activity[9] for anyone who called seeking additional information.

[59] 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 thought to be 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. The employees identified one additional affected individual who was not identified by the DHW audit exercise.

[60] The investigation also 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.

---

[9] A record of user activity is a report produced by a custodian who maintains personal health information using an electronic information system. The custodian is required by s. 63 of *PHIA* and corresponding Regulation 10, to maintain information about who accessed an electronic health record, what was accessed, including the date and time of access for a minimum of one year after each access, and to produce a report of accesses upon the request of the individual whose health record it is.

- An employee observed the pharmacist look up personal health information 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.

[61] 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.

[62] 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 was continuing to improperly use the DIS data of the affected individuals.

[63] Our investigation identified six further individuals whose personal health information was accessed without authority. In total, the evidence establishes, on a balance of probabilities, that 46[10] individuals' personal health information was accessed on the DIS by the pharmacist without authorization.

[10] Discussed further below. In summary, 39 unauthorized accesses were originally confirmed by DHW in conjunction with Sobeys; 1 identified after Sobeys re-interviewed its employees; 4 identified by the OIPC investigation as the DHW accepted Sobeys' validation without basis; 2 identified by the OIPC investigation because other evidence identified the access as suspicious but the audit criteria was too loose to capture them.

[64] Our investigation also identified that the pharmacist's unauthorized activity in the DIS caused the creation of 28 patient profiles in the local POS system for individuals who were not customers of the pharmacy.

3.0 Issues

[65] There are two issues:

1. Did the Department of Health and Wellness take reasonable steps in response to the privacy breaches as required by ss. 61 and 62 of *PHIA*?
2. Does the Department of Health and Wellness have reasonable security and information practices in place for the DIS in compliance with ss. 61, 62 and 65 of *PHIA*?

4.0 Analysis and Findings

4.1 What is "reasonable security"?

[66] I have discussed the meaning of "reasonable security" in Nova Scotia's privacy laws on several occasions.[11] Below, I have summarized 12 factors commonly considered when evaluating the reasonableness of a custodian's security. I adopt these considerations in the analysis that follows.

1. **Contextual:** Reasonable security is contextual. Overwhelmingly, what is clear in the case law is that reasonable security is intended to be an objective standard measured against the circumstances of each case.
2. **Sensitivity:** The more sensitive the information, the higher the security standard required. Personal health information is frequently among the most sensitive and can require a higher level of rigor to achieve reasonable security.[12]
3. **Not technically prescriptive:** Reasonable security is not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect privacy vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.[13]
4. **Foreseeability:** Reasonable security must take into account the foreseeability of the breach and the harm that would result if the breach occurred. The higher the risk of a breach, the higher the security standard will be.[14]
5. **Trust:** For public sector health custodians such as the DHW, reasonable security also includes reasonable assurances to the public that the government is taking privacy protections seriously. Where government organizations hold personal information, the public has an increased level of trust that their personal information is being protected.

---

[11] NS Investigation Reports IR17-01 and IR16-02, for example. In both reports, I noted that the summary of considerations supplied above are consistent with every other jurisdiction in Canada.
[12] *Electronic Health System (Re),* 2010 BCIPC 13 (CanLII) at para 130.
[13] *Electronic Health System (Re),* 2010 BCIPC 13 (CanLII) at para 129.
[14] BC Investigation Report F06-01; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order H2005-IR-001.

This creates a high standard for government organizations to ensure security measures are in place.

6. **Industry standards**: Industry standards, codes of practice or established user agreements can illuminate security requirements provided that following those practices reaches the contextual standards of reasonableness. If the industry standard is less than the contextual evidence demonstrates reasonable security requires, the industry standard is not sufficient. Simply accepting that a third party or contractor will follow industry standards or established user agreements does not demonstrate reasonable security.[15]
7. **Cost:** The cost of implementing a new security measure may be a factor but it is on an extreme scale – reasonable security does not require a health custodian to ensure against a minute risk at great cost. A health custodian cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable security in another.[16]
8. **Life cycle:** Reasonable security applies to the entire life cycle of the records.
9. **Format:** The medium and format of the records will dictate the nature of the physical, technical and administrative safeguards.
10. **Timing:** Reasonableness requires a proactive and speedy response to known or likely risks.[17] Time is of the essence in any privacy breach. The safeguards must ensure that should a privacy breach occur, the custodian and the individual will learn of the breach and have response measures in place quickly and efficiently.[18]
11. **Documentation:** Procedures for establishing reasonable security must be documented, and health custodians must be prepared to respond to the idea that employees won't always follow the documented procedures.[19]
12. **User logs:** Cases dealing with intentional unauthorized access and use of personal health information by authorized users highlight the need for technical infrastructure to log user access of electronic systems and the need for an ongoing program of proactive auditing to address the general risk of intentional abuse of access by authorized users.[20]

4.2 Did the Department of Health and Wellness take reasonable steps in response to the privacy breaches as required by ss. 61 and 62 of *PHIA*?

[67] *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.[21]

---

[15] Ontario Order MC09-9; BC Investigation Report F06-01.
[16] BC Investigation Report F06-01.
[17] BC Investigation Report F06-01; Alberta Order P2013-04; BC Investigation Report F12-02.
[18] Alberta Order H2005-IR-001.
[19] Alberta Order H2005-IR-0010; Ontario Order HO-001; BC Investigation Report F06-01; Alberta Order P2010-008.
[20] 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 CaLII 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.
[21] *PHIA* ss. 61 and 62.

[68] 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:[22]

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

Step 1: Contain the breach and conduct an investigation

Investigation strategy

[69] The pharmacist's access to the DIS was terminated on September 15, 2017 when her employment with Sobeys was terminated and user access was revoked. The DHW's steps to contain the breaches consisted of the audit process in collaboration with Sobeys to determine instances of invalid access. The DHW confirmed that once the list of invalid accesses was finalized by the DIS audit specialist, the response shifted to preparing notification letters and no other actions were taken with regard to further investigation, containment or risk assessment.

[70] The DHW relied on the information supplied by Sobeys on September 20, 2017 for its understanding of the nature and scope of the breaches. Had the DHW critically examined the statements provided by Sobeys and conducted its own investigation, it would have found that the reasons provided by the pharmacist for the access were not credible. This should have raised a red flag and prompted further investigation.

[71] The DHW had an internal resource in the DIS audit specialist who knew the operation of the DIS and its interaction with the local POS system. The DIS audit specialist was aware of two key facts:

1. A user does not need to go into DIS to obtain contact information for existing pharmacy clients. That information is available in the local POS system. This means that anyone accessing DIS data is likely seeking sensitive personal health information such as prescription and diagnosis information.
2. In order for a user to access the DIS data relating to an individual who is not a client of a pharmacy the user must take the additional and intentional step of searching for the individual in the provincial Client Registry and synching that information into the local

[22] 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.

> POS system to create a new client profile. The user must then click on the new POS client profile to access the DIS data. The number of steps required means that it is entirely unbelievable that an individual would accidentally create a new user profile in the POS system or "accidentally" access the DIS data of someone who was not a client of the pharmacy.

[72] Therefore, the DHW had the expertise to know this was a motivated individual intentionally and repeatedly accessing personal health information for some unknown purpose. Nothing about the accesses suggested innocent mistakes or merely accessing contact information. The DHW's initial conclusion that there was no malicious intent or that there was no evidence to suggest that the information had been further used or disclosed was not based on any investigation or evidence. No one was interviewed and nothing in the audit report supported this conclusion. Based on our interviews with pharmacy staff, it was clear that information existed between August and December 2017 to support the conclusion that the pharmacist was in fact further using and/or disclosing information inappropriately accessed. Sobeys employees knew that she had phoned at least one person to discuss the information and later, after her employment was terminated, she visited affected individuals in an attempt to get them to provide their consent for the accesses.

[73] On December 18, 2017, Sobeys provided the DHW with a copy of the letter the dismissed pharmacist was using in an attempt to get retroactive consent from affected individuals for her access to their DIS records. Therefore, without question, the DHW had evidence in its possession on that day that the breaches were not contained. The dismissed pharmacist was using information obtained as a result of the breaches (identity, contact information and dates of access) to contact affected individuals. This was a further unauthorized use and a violation of *PHIA*.

[74] Furthermore, Sobeys did not obtain or provide any reasons for the access in relation to the second group of 33 individuals because the pharmacist had been terminated and Sobeys did not interview her in relation to those accesses. Sobeys' analysis consisted of an opinion about valid or invalid access based on information contained in the local POS system.

[75] Had the DHW critically assessed the information it received from Sobeys it should have inquired about more than the validity or invalidity of access events. The DHW should have inquired further about what Sobeys knew of the relationships between the pharmacist and the affected individuals or about whether there were any witnesses and any other relevant information. The DHW could have interviewed the pharmacist or the individuals who were the subject of suspicious access.

[76] The DIS audit specialist and director of the DIS program both confirmed their understanding that their role under the DHW Privacy Breach Protocol was to determine if the questioned access events were valid or invalid. They did not contemplate conducting any interviews with pharmacy staff or taking any other investigative steps. In this circumstance, additional knowledge may have prompted the DHW to take additional containment steps earlier.

[77] The DHW's Privacy Breach Protocol (undated) references *PHIA*, thus must have come into effect sometime after the legislation was proclaimed June 1, 2013.

[78] As they are set out in the DHW's Privacy Breach Protocol, the Key Steps do not accord directly with the generally accepted four key steps in privacy breach management.[23] The protocol lacks clear guidance on how to conduct an investigation or risk assessment for the purpose of informing containment efforts. The protocol states that: "…the affected program and any other relevant agents (e.g. Information, Communication Technology Services) must, in cooperation with the Health Privacy Office, investigate the breach to understand the circumstances that led up to the breach, and to ensure that all efforts to contain the breach have been completed."[24]

[79] As between the program area and the Health Privacy Office, there does not appear to be sufficient clarity about who will conduct the investigation and connect the investigation back to containment.

[80] The PIA for the DIS states that: "All privacy breaches occurring within the pharmacies (i.e., by pharmacy staff) identified during an audit, complaints, or any other process development by the DHW will result in an investigation by the Health Privacy Office, and the DHW will then determine the corrective action. At the time of writing this PIA document, the corrective action process was yet to be developed."[25] No additional corrective action processes were identified by the DHW. The Privacy Breach Protocol does not explicitly address the situation of a breach of the DIS by an agent of another custodian. The DHW, at all times acted, as though it could not interfere with the investigation being conducted by the pharmacy of its employees.

[81] The program area did not have sufficient understanding of what privacy breach investigation questions should be fully answered prior to concluding the investigation, nor did it understand that it was within its mandate to take the investigation forward beyond verifying instances of inappropriate access. The Health Privacy Office did not undertake any additional investigation once the file was within its purview, nor did it advise the program area to do more.

[82] The DHW's Privacy Breach Protocol is inadequate as an administrative safeguard because it is not sufficiently prescriptive or specific. The result in this situation was a lack of effective coordinated breach management response and the lack of certainty around the applicability and authority to investigate a breach by an agent of a custodian that is subject to a user agreement. The provisions contained in the DIS User Agreement and the PIA for the DIS contain further support for the DHW taking a leadership and controlling role in the management of breaches in relation to the DIS. I discuss this aspect of these two documents in more detail in the prevention section below.[26]

---

[23] 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

[24] Department of Health and Wellness Privacy Breach Protocol, p. 4.

[25] Department of Health and Wellness PIA for the DIS p. 43.

[26] See paras 162-176.

[83] As a result of the DHW's failure to actively investigate and challenge Sobeys' characterizations of valid versus invalid access, the DHW failed to identify seven individuals whose personal health information was accessed without authorization. After re-interviewing its staff, Sobeys identified one additional unauthorized access (the pharmacist's doctor) that was not identified by the DHW's audit and the DHW followed-up with notification.

[84] The evidence does not support that six other accesses identified by Sobeys as valid were in fact valid. Four had no customer activity associated with the access, including one who was validated merely because that person was Sobeys' employee. It appears based on the records that these validations were simply in error. A critical review of Sobeys' response to the DHW produced audit list would reveal this type of error.

[85] An additional two individuals were pharmacy employees where there was some pharmacy-related customer activity associated with these employees in the prescribed audit time period. However, based on our interviews with these employees, we determined that one of the accesses coincided with the pharmacy employee's request for reduced hours. Witnesses said that at the time the pharmacist was publicly speculating about the employee's health status. The access date regarding the second employee is the exact same day as the confirmed unauthorized access to that employee's spouse's DIS profile and is not associated with customer activity. Both employees gave evidence that they suspected that the pharmacist was snooping in their DIS accounts without authorization.

[86] OIPC investigators advised the DHW of the identity of the additional affected individuals and recommended that they be provided with immediate notification. The DHW accepted that recommendation and completed the notification on July 2, 2018.

[87] **Finding #1:** The DHW does not have an adequate or effective privacy breach investigation protocol in place to deal with breaches involving multi-user health information databases.

Recommendation #1: DIS Breach Investigation Protocol (Corrective Action Process)
I recommend that the DHW develop and implement an investigation protocol for the DIS. The protocol should:

i. Require that the Health Privacy Office of the DHW lead privacy breach investigations.
ii. Ensure that the Health Privacy Office has the authority to determine corrective action.
iii. Include a clear internal coordination protocol for any DIS privacy breach investigation.

Outstanding containment issues

[88] As noted above, on December 18, 2017, Sobeys notified the DHW of the former pharmacy manager's (pharmacist) attempt to contact at least one affected individual and that Sobeys suspected the pharmacist would attempt to contact other affected individuals in a similar manner. The DHW confirmed during our investigation that it considered the behaviour inappropriate and unprofessional, but did not consider it to be an additional privacy breach at that time.

[89] The access of a person's electronic health records is an activity intended to be done strictly for authorized purposes under *PHIA* and is the subject of specific rights and responsibilities under s. 63 of *PHIA*.

[90] It is very important for health custodians and the public to understand that even if an individual consents to the collection, use or disclosure of her personal health information, a custodian cannot act on that consent unless such activity is "reasonably necessary for a lawful purpose".[27]

[91] In an Ontario Labour Arbitration case, the arbitrator commented on "lawful purpose" as required by Ontario's analogous *Personal Health Information Protection Act* (*PHIPA*) legislation. In that case, the individual accessed the personal health records of her husband and sister with their consent. However, the arbitrator identified the principles that even with consent, to be lawful, the access and use of personal health information can only be on "a need to know" basis and by those health care practitioners who are providing care.[28]

[92] Nova Scotia's law incorporates similar considerations in s. 25 of *PHIA* where it incorporates the language of collection, use, and disclosure that is "limited to the minimum amount necessary to achieve the purpose". It goes on to incorporate for greater certainty that a custodian must limit the use of personal health information to those "agents who need to know the information to carry out the purpose" and that disclosure shall be limited "to those regulated health professionals, who have the right to treat individuals in the custodian's health care facility;" and "only that information that the health professionals require to carry out their duties and responsibilities."

[93] Thus, consent by the affected individual does not establish authorized use. Custodians and their agents are not permitted to access or use any personal health information at their disposal, except in the performance of their duties in providing health care at the custodian's health care facility and except as otherwise provided by *PHIA*. Personal health information is a distinct type of personal information, subject to separate privacy laws and requiring special considerations distinct from other types of personal information.

[94] The pharmacist's actions in contacting affected individuals are a use of the personal health information. Contacting those individuals to obtain consent after-the-fact and/or to document rationale for the accesses is a further breach of the affected individuals' privacy and represents a serious invasion of privacy. At least two individuals who were contacted by the pharmacist expressed their discomfort with and sense of violation from having been approached by pharmacist. Our investigation gathered unsubstantiated information that the pharmacist contacted up to a dozen affected individuals in this manner.

[95] Following my interim recommendation to the DHW on March 29, 2018, the DHW sent a letter to the pharmacist directing her to immediately stop acting on the breached information, stop sharing the information, destroy any copies in her possession, and provide the DHW with a

---

[27] *PHIA*, s. 11(a).

[28] Georgina Bay General Hospital and OPSEU, Local 367 (J(K)(, [2014] OLAA No. 149, 119 CLAS 7.

list of individuals to whom the breached information was disclosed. The DHW completed this containment action on April 24, 2018. In response, the pharmacist's lawyer contacted the DHW and asserted that the pharmacist did not engaged in any further use or disclosure of the personal health information, contrary to the evidence.

[96] The end result of the failure to complete an adequate investigation was that the DHW did not take reasonable steps to contain this aspect of the breaches until April 2018, 11 months after it was first notified of the situation.[29]

[97] A second outstanding area of concern in terms of containment is with regard to the false local profiles created in the local POS system. The existence of those profiles has the potential to cause harm or embarrassment to the 28 affected individuals. The existence of the profiles indicates services rendered or a relationship with that pharmacy. 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. This outstanding containment concern is addressed in the companion investigation report IR18-02 relating to Sobeys' management of these breaches.

[98] A final outstanding area of concern regarding containment is that our investigation determined that the pharmacist was using another provincial health database, the Client Registry, to create user profiles in the local POS system.

[99] It is not known how many times the pharmacist in this case searched the Client Registry, scrolling through the personal information of others while searching for a target. However, it is through this function that the pharmacist identified individuals, created the local POS profiles and then retrieved the DIS profile of individuals who had no connection at all to the pharmacy where the pharmacist was employed.

[100] There appears to be minimal coordination between the management of the Client Registry and the DIS, although the users must use them in a coordinated fashion. In this case, the discovery of the breaches, follow-up and auditing included only the DIS. No inquiry or investigation into the user's activity on the Client Registry was undertaken at all.

[101] As a result, on May 16, 2018, OIPC investigators recommended that the DHW forward the details of this privacy breach to the Nova Scotia Health Authority who provides application support services for the Client Registry so that it could conduct an audit of the use of the Client Registry by the pharmacist. At that time, the DHW agreed with this recommendation.

---

[29] As noted above, the DHW received its first notice of this series of privacy breaches on its Health Privacy 1-800 line on May 29, 2017. DHW confirmed that its practice at the time was not to investigate tips from individuals who wished to remain anonymous.

[102] **Finding #2:** These privacy breaches are not adequately contained while there remains a realistic risk that the pharmacist will continue to use information she gained as a result of these inappropriate accesses.

Recommendation #2: Containment
I recommend that the DHW re-contact all 46 affected individuals to determine if the pharmacist has been in contact with them since April 24, 2018. If so, I recommend that the DHW take further legal action to prohibit the pharmacist from further using or disclosing the personal health information she obtained as a result of these breaches.

[103] In order to address this issue in the longer term, I have set out a recommendation below regarding interrelated electronic databases.

Recommendation #3: Electronic Database Breaches
I recommend that the Privacy Breach Protocol be revised to prescribe that where a user is found to have breached the privacy of any individual(s) via one of the electronic databases, detailed audits of that user's activity in other implicated databases be automatically conducted.

Step 2: Evaluate the risks

[104] 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 breach and the foreseeable harm from the breach.

Personal information involved

[105] The personal information involved is highly sensitive personal health information. The accesses in this case were programmed queries for patients' DIS profiles that returned results of personal health information in standard fields including identifier information, prescription history, medical conditions, allergies, immunization history, services provided and observations. Fields in the results may be blank if no information was populated by a user of the system.

[106] 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.

[107] The fact of an individual taking a particular medication can lead to presumptions or assumptions about an individual. For example, if a woman is prescribed birth control, that information could be divulged in embarrassing ways and lead to assumptions about her lifestyle or sexual status. If an individual is prescribed anti-depressant, anti-anxiety or other medication commonly associated with mental illness, knowledge of this could contribute to social stigma or social-relational harm. If an individual is prescribed opioids it could lead to assumptions about lifestyle or addiction status.

Relationship between the pharmacist and affected individuals

[108] Based on the evidence gathered, it appears that in each case of unauthorized access the pharmacist had some sort of personal relationship with the affected individual. In effect, the pharmacist was using the DIS as a social media website to serve her own purposes.

[109] For example, we know that the pharmacist accessed the DIS profile of teenage minors, one of whom was the pharmacist's own child's romantic partner. A witness confirmed that after accessing that minor's DIS profile, the pharmacist made a phone call to her spouse and commented that their child should not be allowed to see the individual based on what she read in the DIS profile. A witness confirmed that the pharmacist searched for and viewed the DIS profile of an individual she had been in a motor vehicle collision with. The pharmacist's behaviour is a serious encroachment on the personal life and autonomy of other individuals and meddling in the private lives of others using information gained by the intentional unauthorized access of information on the DIS.

[110] The pharmacy at issue here is in a small community. Individuals are familiar with each other and so any failure to contain the breaches has implications for harm discussed below.

Containment efforts

[111] Although Sobeys immediately fired the pharmacist and revoked her access to the POS and DIS systems, our investigation established that the pharmacist continued to use the information obtained after her employment was terminated. The pharmacist made attempts after-the-fact to document consent for the access of some affected individuals' personal health information. Presumably the purpose for this contact was to gather "evidence" that privacy was not breached or that the breaches were not as serious where consent could be established.

[112] A second area of concern in terms of containment is with regard to the false local profiles created in the local POS system. The existence of those profiles has the potential to cause harm or embarrassment to the 28 affected individuals. This outstanding containment concern is addressed in the companion investigation report IR18-02 relating to Sobeys' management of these breaches.

[113] A final outstanding area of concern regarding containment is that our investigation determined that the pharmacist was using another provincial health database, the Client Registry, to create user profiles in the local POS system.

[114] The risk associated with the outstanding containment issues is high.

Cause and extent of the breach

[115] The cause of the breaches is a regulated health professional acting outside the scope of her regulated health practice, and all policies and frameworks in place by both the DHW and the employer pharmacy. The breaches are extensive in terms of the sensitivity of the information

breached, the number of individuals affected (46 individuals) and the time period (October 2015 – August 2017) over which the individual was able to operate undetected.

[116] The range of individuals affected and apparent motivations of the pharmacist all indicate a serious and extensive disregard for the personal privacy of others and an abuse of the trust placed in this authorized user of the DIS. It is not known whether the personal information of minors and/or acquaintances of the pharmacist's child was disclosed to the pharmacist's child or any further.

[117] In my view, these breaches were extensive and high risk. The fact that the pharmacist was able to breach the systems over a two-year period, undetected by either the DHW or Sobeys, suggests that the technical and administrative safeguards in place were not effective or not used effectively.

Foreseeable harm from the breach

[118] The main risks here are hurt, humiliation, damage to reputation or relationships, and social and relational harm. The risk of the disclosure of an individual's prescription history or medical conditions could impact on reputation and self-esteem and could lead to bullying or other forms of social stigma. The sharing of information about medications that indicate a mental health condition, or even birth control, could have serious consequences for the individual in a small community. Once sensitive information of this nature is learned and shared, the damage is almost impossible to repair.

[119] Credit protection services are a common mitigation strategy employed in situations where financial information has been breached. However, there is no equivalent mitigation strategy for personal health information. We cannot subscribe to a protection service to mitigate rumours, whispers, stares, social ostracization and other forms of bullying. It is virtually impossible to undo the harm and sense of violation individuals feel when the intimate details of their personal health information are breached.

[120] I find that the harm from these breaches is significant and foreseeable.

Risk assessment summary

[121] Aggravating factors in these breaches include the long period of time over which the pharmacist accessed highly sensitive personal health information of individuals extending beyond the clientele of the pharmacy, coupled with pharmacist's use of the information and brazen efforts to contact affected individuals to secure consent after-the-fact once the breaches had been discovered. These factors make the circumstances of these breaches high risk. The full extent of what the pharmacist did with the breached information and who she shared it with is still unclear, leaving an undetermined risk of harm to the affected individuals that their personal health information may be circulating within the community.

[122] The supervisory and leadership role played by the pharmacist within the pharmacy is also an aggravating risk factor. Leaders do influence workplace culture and in this circumstance, the

leader's behaviour poses a risk by negatively influencing respect for privacy and clarity with respect to authorized and unauthorized use of the electronic health records for other employees.

[123] More generally, the risks associated with authorized users abusing access to personal health information cannot be understated. Reported cases from across the country suggest that personal health information is highly susceptible to authorized users intentionally using their access for unauthorized purposes.[30] In addition to reported cases, the intentional abuse of access to personal health information by authorized users has also resulted in disciplinary action by regulatory bodies and court cases garnering media attention.

[124] The class action civil lawsuit against Nova Scotia's Southwest District Health Authority that involved a clerk accessing the personal health information of 707 patients resulted in a $1 million civil liability payout to the group of affected individuals.[31] A pharmacist in Bathurst, New Brunswick was found to have sent personal health information to individuals unrelated to the provision of health services via text message.[32] In that case, the pharmacist was suspended from employment, received sanctions from her professional body and was ordered to pay $17,000 in costs.

[125] A former police officer employed by Manitoba Health was convicted of the offence of accessing personal health information in violation of the personal health information law in that province after he accessed the personal health information of his daughter.[33] In that case, the offender was fined $7,500 and the Manitoba Ombudsman publicly released its investigation of Manitoba Health in relation to the incident. The Ombudsman's press release states: "We are releasing this report so that trustees of personal health information and their employees can benefit from the findings and conclusions of our investigation…Organizations that hold personal health information must have policies, procedures and safeguards in place to ensure that this information is only accessed by employees who have a legitimate work-related purpose for doing so. Employees need to know that snooping into the personal health information of others is a very serious matter."[34] The Ombudsman's report in this case examined the measures in place to prevent, detect and respond to the breach.[35]

---

[30] 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 CaLII 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); * this represents a sample of the total reported cases.

[31] http://thechronicleherald.ca/novascotia/1478315-hospital-records-breach-costs-health-authority-1m and https://www.cbc.ca/news/canada/nova-scotia/shelburne-hospital-roseway-clerk-patient-records-settlement-1.4162568

[32] http://www.cbc.ca/news/canada/new-brunswick/bathurst-pharmacist-fined-texting-1.4552139

[33] http://www.cbc.ca/news/canada/nova-scotia/shelburne-hospital-roseway-clerk-patient-records-settlement-1.4162568

[34] https://www.ombudsman.mb.ca/news/news/2017-12-12/manitoba-ombudsman-releases-a-report-under-phia-about-unauthorized-access-to-personal-health-information-at-manitoba-health-seniors-and-active-living.html

[35] https://www.ombudsman.mb.ca/uploads/document/files/case-2014-0500-en.pdf

[126] The occurrence of authorized users working in health care settings intentionally accessing personal health information for unauthorized purposes appears widespread. It is not limited to regional or job classification boundaries. The advent of broad access electronic health records increases the access and availability of personal health information to authorized users, thereby also increasing the risks of authorized users intentionally using their access for unauthorized purposes. Custodians of electronic health records must anticipate and plan for the intentional abuse of access by authorized users. Safeguards designed to detect and prevent such access are reasonably required to satisfy the requirements of *PHIA*.

[127] In my assessment, both the specific and general risks associated with this series of privacy breaches are high.

Step 3: Notification

[128] 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.

[129] Notification conveys respect to the individuals whose privacy has been breached, and allows them to take steps to mitigate any potential harms. In this case, the DHW notified individuals by letter dated December 22, 2017.

[130] My concerns with the notification are three-fold: (a) timing; (b) accuracy and sufficiency of information provided; and (c) failure to notify individuals of their right to complain.

Timing

[131] The DHW first identified six affected individuals on September 20, 2017. On November 8, 2017, the DHW had identified an additional 33 affected individuals. The DHW issued notification letters on December 22, 2017, three months after the first six individuals were identified and six weeks after the second group of 33 individuals was identified.

[132] According to the DHW and Sobeys, the notification efforts were accelerated as it became known that the pharmacist was attempting to contact affected individuals. According to the DHW, it took staff nearly two months to confirm mailing addresses for 39 individuals before notification letters could be sent. The DHW re-checked its databases for updated contact information after six months resulting in renewed notification letters being sent to four individuals on July 18, 2018. The remaining two individuals have not yet received notification and the DHW has taken no additional steps to find the individuals. The DHW plans to re-check its databases for updated contact information in another six months.

[133] *PHIA* requires that notification occur at "the first reasonable opportunity". To be effective, notification must be given in a timely enough fashion to allow those affected to mitigate the breach's risks. The reasonableness of the timing is measured by whether it is objectively diligent and prudent in all the circumstances. Guidelines and laws tend to be

imprecise with regard to time limits on notification to affected individuals because circumstances must be accounted for.

[134] The federal Privacy Commissioner's Key Steps for Organizations in Responding to Privacy Breaches states that notification to affected individuals should occur "as soon as reasonably possible following assessment and evaluation of the breach" and a key consideration is "whether notification is necessary in order to avoid or mitigate harm."[36]

[135] The *General Data Protection Regulations* (*GDPR*), which came into force in Europe on May 25, 2018, is widely regarded as the farthest-reaching privacy and data protection law in the world and is beginning to influence what is regarded as reasonable elsewhere. The notification requirements in the *GDPR* are to notify the supervisory body without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, with an explanation for the delay if it is provided after 72 hours, and "without undue delay" to the affected individual.[37]

[136] Context is an important factor in determining what is reasonable. In a report from the Office of the Information and Privacy Commissioner for British Columbia, former Commissioner Loukidelis observed that: "Where safety is an issue, the importance of prompt notification cannot be over-stated…where notification is determined to be appropriate in accordance with the discussion above, notify affected individuals within hours if not days of the privacy breach." [38]

[137] In the United States, there are at least 12 state laws mandating specific breach notification time periods.[39] The majority of these laws provide that notification must be provided immediately but not later than 45 days after discovering the breach. Seven of the twelve laws use the 45-day standard as a maximum. The remaining five laws range in time between 5 calendar days and 90 days.

[138] Guidelines around notification in Canada suggest multiple formats for notification to affected individuals, always with the purpose of best facilitating the individual taking steps to mitigate harm. It is not necessary that each individual receive the same form letter notification after the investigation is complete. A public body can take a tailored approach to notification at multiple stages of the investigation if that would best facilitate mitigation. For example, a phone call initial notification to provide the individual preliminary ability to manage the risks, followed by formalized notification later in the process, may provide the individual better opportunity to mitigate the potential damage caused by the breach.

[139] By the end of September 2017, the DHW confirmed the privacy of the first six individuals had been breached. The delay of three months until notifying those individuals was

---

[36] https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gl_070801_02/

[37] *GDPR* articles 33 and 34.

[38] "Ministry of Small Business & Revenue & EDS Advanced Solutions Inc," June 20, 2007. OIPC for BC Investigation Report F07-01; [2007] B.C.I.P.C.D. No. 13.

[39] A summary of the twelve laws is available at Baker Hostetler, Data Breach Charts: November, 2017 https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf

not an acceptable delay and does not meet the standard of the first reasonable opportunity. The additional affected individuals were identified by the DHW by November 8, 2017. Notification letters were sent to the entire group on December 22, 2017, six weeks after the identification of the second group of affected individuals.

[140] In this case, notification to the minors who were acquaintances of the pharmacist's child carried a higher degree of risk in a small town environment where gossip or bullying may become a safety issue. This factor weighed heavily in favour of immediate notification.

[141] In summary then, best practices to ensure that breach notifications happen at the "first reasonable opportunity" are:

- Notifications should generally happen within days or weeks, but not months after discovery of a privacy breach. Consider notification by 45 days from the discovery of the breach as the absolute maximum acceptable time period.
- In some cases, the nature of the breach may demand immediate notification – a risk to safety is one of those circumstances.
- Once a health custodian has identified an affected individual, notification should occur immediately. First reasonable opportunity does not allow for health custodians to await the identification of the entire affected group before any affected individual is notified.

Accuracy and sufficiency of information provided

[142] My second concern with the notification provided to individuals is that it is not accurate nor sufficiently specific about what happened. The notice states:

> We learned of the breach because of our audit process. We followed up with a full investigation in cooperation with the user's employer.

[143] The DHW learned of the breaches because suspicions about the user were communicated to the DHW, which then initiated an audit of the user's activity. The statement in the letter gives the impression that the DHW's proactive audit process uncovered the breaches, which is not the case. Furthermore, the DHW ignored the first instance where suspicions about this user were relayed to it via its Health Privacy 1-800 line. In this case, the DHW could have stated that the breach was uncovered by a tip from a concerned party that was followed-up by an audit of user activity.

[144] It is inaccurate to state that the DHW followed-up with a full investigation. It did follow-up to determine if the accesses identified in its audit of the identified user were authorized or not, but it did not fully investigate. A key risk factor in this case is that the pharmacist had a relationship of some kind with every affected individual. The evidence we gathered supports this conclusion. A significant piece of information that would have helped affected individuals decide what they could do to mitigate potential harm from the breaches was the identity of the pharmacist. One witness we spoke with specifically identified this as a shortcoming in the letter. Other recipients specifically requested this information following receipt of the notification letter.

[145] Best practices call for the notification letter to be specific and precise in describing the breach and its outcome to affected individuals. This shows respect for the affected individuals and informs their ability to take steps to mitigate potential harm. The letter describes that the "medication profile" in the DIS was accessed. It was actually the DIS profile that contains a prescription history, in addition to a range of other personal health information profiles, including medical conditions and allergies, that was accessed. The DHW could have provided individuals specific information about what personal health information was accessed. The notification is also vague about the steps being taken to prevent a similar breach from occurring in the future, stating that it "continues to take steps to monitor the use and protect the security of personal health information."

[146] In cases of unauthorized access to personal health information, the custodian should consider whether this includes the identity of the individual who accessed the information. The Saskatchewan information and privacy commissioner has recommended providing the personal information of the perpetrator of inappropriate access to affected individuals in a notification letter, including the name of the perpetrator and the discipline imposed. Saskatchewan's commissioner makes these recommendations on the basis that, under the *Local Authority Freedom of Information and Protection of Privacy Act* (*LAFOIP*) legislation, the health authority has discretion to disclose the personal information of employees,[40] and that given the seriousness of the actions of the individual and its effect to undermine trust in health care services, there is a public interest in disclosing the individual's identity to affected individuals.[41]

[147] In Nova Scotia, *PHIA* supports providing the name of the individual who inappropriately accessed personal information. Section 63 of *PHIA* provides that a custodian shall create and maintain a record of user activity and that such record must be available to the individual on request. In this case, the DHW advised affected individuals of their right to request the record of user activity which would provide the identity of the individual, along with other information. In my view, the better practice is to either proactively provide the record of user activity or to simply provide the name of the individual who engaged in the unauthorized access in the breach notification letter.[42]

[148] The fact of having accessed the personal health information is part of the personal health information record and is information the individual is entitled to receive under *PHIA*. Proactively providing the name of the individual can assist the affected individual to assess the risks and take steps to mitigate the harm with less effort than requiring the additional process of requesting a record of user activity that then necessitates extra analysis to identify an unauthorized access from what is potentially a long and detailed report.

---

[40] Office of the Saskatchewan Information and Privacy Commissioner Investigation Report 100-2015.
[41] Office of the Saskatchewan Information and Privacy Commissioner Investigation Report 136-2017.
[42] Section 33(a) of *PHIA* permits health custodians to use personal health information (such as a record of user activity) for the purpose for which it was created. Therefore, proactively providing a record of user activity to an affected individual is an authorized use under *PHIA*.

Failure to notify individuals of their right to complain

[149] My third concern with the notification is that it fails to clearly advise individuals of their right to complain to my office and inappropriately classifies my office's role as being "consumer oversight". The notification states, "…you have the right to contact the Office of the …OIPC for guidance. The OIPC provides consumer oversight for the Personal Health Information Act (PHIA)."

[150] This statement minimizes the oversight role which is not aimed at providing guidance to individuals or consumer protection. The OIPC role is aimed primarily at providing oversight to ensure custodians are in compliance with the law. Affected individuals have a right to complain to the OIPC and I have the statutory power to investigate those complaints. My office did not receive any complaints in relation to these breaches, possibly because the information to the affected individuals was not fully accurate.

[151] **Finding #3:** The DHW's privacy breach notification was not in compliance with *PHIA* in that it did not occur at the first reasonable opportunity and failed to include adequate information to affected individuals.

Recommendation #4: Privacy Breach Notification

4(a) I recommend that the DHW immediately notify the two individuals who never received the first breach notification letter because the mail was returned unopened. I recommend that the DHW confirm with the OIPC when this step is completed.

4(b) I recommend that the privacy breach notification provisions in the DHW's Privacy Breach Protocol be revised as follows:

i. Clarify that notification at the first reasonable opportunity requires that notification occur within days (not weeks) of identification of affected individuals.
ii. Specify that notification need not await the identification of every affected individual and that notification can therefore occur as individuals are identified.
iii. Require that notification letters include, at a minimum, the following information:
    - A clear and specific statement about what occurred and how it was discovered.
    - A clear and specific statement about the personal health information that was accessed.
    - Information about what the individual can do to mitigate potential harm.
    - A clear and specific statement about steps taken to contain the breach and prevent it from happening in the future.
iv. Require that either the identity of the authorized individual who engaged in unauthorized access be provided in the notification letter or require that the record of user activity be enclosed with the notification letter.
v. Clearly advise affected individuals of their right to file a privacy complaint with the Office of the Information and Privacy Commissioner for Nova Scotia.

Step #4: Prevention

[152] The final step in managing a 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.

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

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

[154] 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

[155] Physical safeguards by the DHW were not a factor in this investigation and were not reviewed.

Administrative controls

[156] The administrative safeguards of the DHW that we reviewed in this investigation included the DHW's Health Privacy 1-800 line, Privacy Policy, Privacy Breach Protocol, and DIS User Agreement. The shortcomings in the Privacy Breach Protocol were discussed above with respect to containment, investigations and notifications.

Health Privacy 1-800 line and breach investigations

[157] The DHW operates a website containing information about the DIS and directing individuals with questions about the DIS or about privacy to contact the phone line. The phone logs for the year 2017 demonstrate multiple instances of individuals calling to register concerns with DIS users' access among other questions and concerns with the DIS, including a call on May 29, 2017 citing concerns about a pharmacist manager's access, which was confirmed to be about this case.

[158] The caller on May 29, 2017 was a pharmacy employee who gave evidence to OIPC investigators that she was ready to provide details regarding the suspected inappropriate access to the DHW staff on the 1-800 line but was encouraged to instead tell her supervisor. When the caller replied that the person in question was her supervisor, the DHW staff did not request the identity of the pharmacist or pharmacy but instead replied that she would consult and get back to the caller. The caller told the DHW staff member that she wished to be anonymous in making the tip because of fear that her job may be at risk. An undated Health Privacy Office phone log note indicates that an attempt was made to return the phone call. The pharmacy employee gave evidence that she did not receive a return phone call and no voice message or other indication of

the call. In the view of the pharmacy employee who phoned in the tip, the DHW took no interest in her concerns or the information she could supply about the abuse of access by this user.

[159] All of the DIS staff interviewed recalled that the tip had come in and had been discussed and that a decision was made that nothing could be done if the tipster was intent on being anonymous. The DIS staff also confirmed that the minimum information required in order to begin investigating an allegation of unauthorized access would be the pharmacy location or the name of the user. They confirmed that the name of the source of the tip or the basis on which the information was brought forward is not necessary to conduct a user audit. It is worth noting that 16 of the unauthorized accesses took place after this tip was received by the DHW.

[160] The DHW now states that it was at all times willing to act on an anonymous tip. However, the evidence with respect to the May 2017 call indicates that the only action taken was to make one call back and to leave no message and further, that key DHW staff (DIS staff) clearly believed at the time that an investigation could not be conducted if the tipster was intent on being anonymous. A more proactive approach would include obtaining the name of the pharmacy or pharmacist in the first call, leaving a message or calling more than once in an attempt to make contact with tipsters.

[161] **Finding #4:** The Health Privacy 1-800 line is an effective administrative safeguard that has generated valuable responses from the public. In this case, the DHW did not use this safeguard effectively.

Recommendation #5: Health Privacy 1-800 Line and Breach Investigations
I recommend that the DHW establish a protocol for investigating anonymous and other tips to its Health Privacy 1-800 line, beginning with communicating to all staff that anonymous tips can and should be followed-up.

The DIS User Agreement

The User Agreement
[162] The agreement between the DHW and other users of the DIS takes the form of the Joint Service and Access Policy (Pharmacies and Dispensing Physician) Confirmation of Acceptance. Access to the DIS is granted to a custodian following the user organization submitting its signed "Confirmation of Acceptance". The Joint Service and Access Policy sets out the responsibilities of the DHW and the responsibilities of the user organization. In this case, the user organization is the pharmacy, who then submits to the DHW the names of individual employees who require the DIS access. On June 13, 2014, Sobeys signed the Confirmation of Acceptance. The pharmacist gained access to the DIS when the local pharmacy where she was employed was connected to the network in June 2015.

[163] The responsibilities of the DHW under the User Agreement provide the DHW with the power to take significant action to manage the use of the DIS with respect to signatory custodians and their agents. The User Agreement deems the DHW as ultimately responsible to

ensure that the personal health information collected, used, disclosed and retained by the DIS is maintained in compliance with *PHIA*.[43]

[164] Under the User Agreement, the DHW maintains the right to monitor and audit the use of the DIS access using its own monitoring and auditing tools and the right to suspend or terminate access is at its own discretion.[44]

[165] The User Agreement explicitly states that the DHW Privacy Breach Protocol will apply and empowers the DHW to investigate breaches, although there is some ambiguity where it states that it may "contact and collaborate with the User Organization representative responsible for privacy and security to conduct an investigation."[45] It does not state who will conduct the investigation but it does leave residual authority with the DHW. The DIS program director is tasked with the responsibility to monitor the implementation, performance and effectiveness of the User Agreement.

[166] The Joint Responsibilities section of the User Agreement recognizes the foundation of the User Agreement is to ensure the collection, use and disclosure of personal health information only in accordance with *PHIA* by explicitly setting out that the purpose of access to the DIS is to provide and support the provision of health care.[46]

[167] The responsibilities of the user organization under the User Agreement include being responsible for the individuals within the user organization and ensuring compliance with the User Agreement.[47] The responsibilities outline a requirement to "monitor access of its staff to the DIS to ensure proper access, use, and disclosure of personal health information"[48] and a recommendation that user organizations should follow the Privacy and Security Guidelines for Best Practices, as set out in Schedule B.

[168] Setting out adherence to the Best Practices in Schedule B as a recommendation that "should" be done is starkly juxtaposed against the requirement to monitor access in s. 5.3.23. The Best Practices contain relevant statements about regularly reviewing access logs to ensure reasonable access to data by authorized users and recommends privacy and security audits of pharmacy software systems annually or more frequently.[49] Some ambiguity is created by making monitoring a requirement in the User Agreement but having the detailed guidance merely a recommendation.

---

[43] Drug Information System Joint Service and Access Policy, s. 5.2.9.
[44] Drug Information System Joint Service and Access Policy, ss. 5.2.10 & 5.2.12.
[45] Drug Information System Joint Service and Access Policy, s. 5.2.13.
[46] Drug Information System Joint Service and Access Policy, s. 5.4.1 and Policy Directive s. 5.1.5.
[47] Drug Information System Joint Service and Access Policy, s. 5.3.6.
[48] Drug Information System Joint Service and Access Policy s. 5.3.23.
[49] Schedule B s. 2.24 & 2.25

Implementation of the User Agreement

[169] The Health Privacy Office provides privacy leadership for the DHW. It describes the relationship between the DHW and custodian user organizations (pharmacies) as a "full trust model". This implementation model was used to explain that the pharmacy must investigate the breaches because the individual user is the pharmacy's employee. The DHW did not view for itself a direct role or ability to investigate or take action in response to the actions of an employee of a user organization.

[170] The DHW's questions of Sobeys were limited to the validation or non-validation of specific access events from the user access logs. The DHW did not undertake any additional fact-finding related to the scope, risks, containment or root cause analysis and Sobeys did not volunteer any of the information it had gleaned early on in its investigation.

[171] Further, the DHW appears to have taken a deferential approach to the pharmacy's investigation and determination of validity of access. In an email exchange between the DIS audit specialist and the pharmacy's corporate officer, the audit specialist questioned the information and validity determination in relation to the pharmacist's access of another store employee's information. The audit specialist confirmed that if there was no valid dispensing or other activity within the prescribed period, then the DIS would deem the access invalid. In reply, Sobeys confirmed that there was no dispense activity within the specified period, but that, as the client is well known to pharmacy staff as a store employee, the access was interpreted as possibly valid, although agreed it was difficult to say with certainty. The DHW accepted this statement by Sobeys and omitted this individual from the list of confirmed privacy breaches. No other investigative steps were taken.

[172] The DHW's reticence to investigate beyond identification of inappropriate access and deference to the pharmacy's determination of validity of access appears to be related to the concept of the "high trust model" of agreement. Although the director of Health Privacy Office stated that if the need arose she would question the information coming from a user organization during a privacy breach investigation, she has never done so.[50] The DHW has never conducted an audit of user organizations' compliance with their responsibilities under the User Agreement.

[173] Reference to the "high trust" model with regard to the "Users of Personal Information" can be found in the privacy impact assessment prepared by the DHW prior to the implementation of the DIS. The PIA describes the "High Trust Model" as follows:

> Access to the DIS database from pharmacy POS systems will use a "High Trust" model, whereby individuals who are authorized to access the DIS without having to log in specifically to the DIS. By virtue of this High Trust model, the level and type of access to the DIS by users is determined by the pharmacy POS system, not the DIS. Pharmacists determine what functions are delegated to whom.[51]

---

[50] Meeting with the DHW director of the Health Privacy Office, March 7, 2018.

[51] PIA Stream 1 - (Community) Pharmacy p. 16, March 11, 2013, PNNS0102-022A, p. 38.

[174] Within the PIA, the High Trust Model appears only to relate to the manner of granting access credentials to individual users at the local level. No risks are attributed to the High Trust Model within the PIA. However, in implementation the concept of "High Trust" appears to have filtered into other areas of managing the agreement and appears to have given the DHW officials the impression of being unable to fully investigate or take action in response to this series of breaches.

[175] Despite the explicit assigning of responsibilities and enabling of action for the DHW under the User Agreement, the implementation of the agreement falls short of fulfilling those responsibilities and fails to take advantage of the scope of the DHW role envisioned by the User Agreement.

[176] **Finding #5:** The roles and responsibilities under the User Agreement are sufficiently outlined and it serves as an adequate administrative safeguard. The implementation of the User Agreement does not accord with the roles and responsibilities set out and is unnecessarily hindered by the 'high trust model' of implementation.

Recommendation # 6: DIS User Agreement
I recommend that the DHW take the following actions with respect to the DIS User Agreement:

i. **Enforce existing terms**: The DHW should re-familiarize itself with its User Agreement and clarify internally the full extent of its authority and its responsibilities to manage and investigate a privacy breach by agents of a third-party user organizations under the Agreement.
ii. **User organization audits**: Require the DIS user organizations to regularly review access logs and conduct security audits of pharmacy software systems annually or more frequently.
iii. **Monitoring of user organizations**: Make the type and frequency of the DHW monitoring of user organization audits and audit capacity explicit and make the authority of the DHW to investigate privacy breaches involving the DIS explicit.
iv. **Notification to DIS user organizations**: Remind all DIS user organizations by August 31, 2018 that they must comply with the DIS User Agreement requirement that they regularly review access logs and that, at a minimum, they must conduct security audits of pharmacy software systems annually.

The DIS user training

[177] The PIA for the DIS states that one of the administrative safeguards in place is that "pharmacy users will be requested to add an electronic patient note explaining the reason for access…" when the encounter does not result in a subsequent medication dispense.[52] The PIA states that "through communications and training, pharmacy users will be informed that access to DIS profiles, when other services are not performed, will be highlighted for audit." This administrative safeguard connected to the technical safeguard of audit practice has merit in theory.

[52] PIA Stream 1 - (Community) Pharmacy p. 16, March 11, 2013, PNNS0102-022A, p. 42.

[178] The DHW identified in the PIA that viewing a DIS profile should be accompanied either by a dispensing activity or by a notation indicating the reason for the access. However, the users at this pharmacy were not in the practice of doing this. The DHW never identified or followed up on logged activity not associated with dispense activity that did not have an accompanying notation at this pharmacy. Had the DWH followed up on this intended mitigation strategy, the pharmacist's activities may have been discovered sooner. The DHW does not have a system-wide flag for this type of activity. The importance of this audit criteria is discussed below.[53]

[179] **Finding #6:** The administrative safeguard of requiring documentation when a DIS access is not accompanied by logged dispense activity has merit if implemented and associated with proactive monitoring.

Recommendation #7: DIS User Training
I recommend that the DHW conduct training for all users of the DIS on the use of DIS notations.

The DHW's Privacy Policy

[180] The DHW's current Privacy Policy (policy) came into effect on June 1, 2013. It includes references to *PHIA* and a definition of a privacy breach. Generally, it assigns responsibility for compliance with the policy and applicable privacy legislation to the director of the Health Privacy Office under the broad accountability of the DHW's deputy minister.[54] The policy defines "agent" as, "a person who acts for or on behalf of the Department, and for the purposes of the Department."[55]

[181] The DHW does not dispute that it is the custodian of the personal health information contained in its DIS database. The personal health information contained therein is collected and uploaded to the database by multiple users across the province, many of whom are not employed by the DHW. There is question whether those users should be considered agents of the DHW when they are acting in relation to the province's electronic health record database. The DHW interprets its policy as applying to and creating direct responsibility for employees of the DHW only. The policy is ambiguous on this point. Are pharmacists employed by a commercial pharmacy acting for or on behalf of the DHW and for the purposes of the DHW when they upload or access personal health information contained in the DIS?

[182] The definition of agent under *PHIA* is broader than the DHW's policy where it states that an agent "in relation to a custodian, means a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian…" This definition

[53] See paras 195-197.
[54] Notwithstanding some slight variation in the title, it was acknowledged by the DHW that the director of the Health Privacy Office is referred to in the policy.
[55] DHW Privacy Policy, s. 2.1.1.

of agent contains two critical factors: first, that the agent is authorized by the custodian, and second, that paid employment status is not determinative of agency.

[183] In the circumstances of this series of breaches, the pharmacist was authorized by the DHW to access the DIS database for the purpose of recording dispensed pharmaceuticals and consulting patient status and history in the course of providing pharmacy services. One of the DHW's purposes with its DIS database is to facilitate the Prescription Monitoring Program, which could not operate effectively without every prescription being recorded with the DIS. Its purpose is also to promote patient safety by ensuring that those dispensing drugs or providing over-the-counter pharmacy advice, have access to relevant information about the patient, such as allergies and potential drug interactions.

[184] However, the pharmacist's primary purpose is to provide health care services to the patient. The lines of purpose are blurred. One could say that pharmacists do not require the DIS in order to carry out their independent purpose of filling prescriptions for patients. Indeed, pharmacists fulfilled this purpose without the DIS prior to its launch in 2015. In my view, when supplying information to the DIS, the pharmacist is acting for the purposes of the DHW. However, in accessing the information contained in the DIS supplied by others, the information is used to improve the quality of the health care services provided to the patient and thus, the pharmacist is not acting for the DHW's purpose, but rather for purpose of providing health care to the patient.

[185] To the extent that the Privacy Policy is understood to exclude from agent status based on whether the individual is employed by the DHW, the policy is not in compliance with *PHIA* which makes no such distinction. *PHIA* would permit the DHW to establish an agency relationship with individual users of the DIS. Whether an agency relationship is a required administrative safeguard is another matter and is addressed under the analysis of the User Agreement.

[186] The DHW's Privacy Policy directs those subject to the policy to "…ensure any Agreements entered with third parties are compliant with any governing legislation or regulations and the directives of this Privacy Policy." The third party user agreement at issue here sets out a custodian to custodian relationship. As the custodian of the information in the DIS, the DHW is authorized to "disclose personal health information about an individual to a custodian involved in the individual's health care if the disclosure is reasonably necessary for the provision of health care to the individual."[56]

[187] **Finding #7:** As an administrative safeguard, the DHW's Privacy Policy is ambiguous about its applicability to others outside of the DHW. However, taken together with the DIS User Agreement, it appropriately assigns responsibilities for the privacy program, including ensuring that any agreements entered into with third parties be compliant with legislation, regulations and the directives of the Privacy Policy.

---

[56] *PHIA*, s. 36.

Recommendation #8: The DHW Privacy Policy
I recommend that the DHW Privacy Policy be updated to reflect current position titles and to remove ambiguity about agency status of individuals not employed by the DHW.

Technical controls

[188] The technical safeguards that we reviewed in this investigation were user activity audits. Both the DHW and Sobeys have user audit programs in place, but neither of them successfully identified the pharmacist's activities over the two years that she abused the authorized access. Because the nature of the breaches did not raise any other technical security issues, other technical aspects such as cybersecurity, infrastructure vulnerabilities or penetration potential were not reviewed.

[189] The ability of a proactive audit to detect suspicious activity depends on its configurations and parameters.

[190] Electronic activity logs offer 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 electronic log needs to be effectively audited to identify problem activity. Electronic tools used in the audit process can assist with the labour of audit but they must be calibrated and be able to provide information open to multiple interpretations. Although a powerful technological requirement for any custodian, activity logs alone cannot supply all of the safeguards. The details of user activity data, configurations and audit analysis procedures are also important considerations.

[191] It is clear though, that reasonable security requires electronic activity logs accompanied by an effective audit procedure. It should be anticipated by custodians that some authorized users will engage in inappropriate access, use and disclosure of information at their disposal, and custodians must be vigilant to identify instances of it as quickly as possible.

[192] The DHW's PIA for the DIS contemplates the use of the FairWarning audit system as an audit tool to assist with performing regular monitoring of user activity.[57] The PIA sets out a list of fields that will be extracted daily from the DIS audit log for use with the FairWarning audit tool. The PIA also specifies that auditing will be conducted in accordance with the Provincial Audit Policy, which was being drafted at the time of the PIA.

[193] The DHW created a draft general audit policy January 15, 2013. It also created an undated draft audit procedure for the DIS. The DIS staff acknowledge that the procedure has not been finalized and is scheduled to be reviewed this year.

[194] The DIS audit specialist is responsible for the audits conducted of the DIS in accordance with the criteria set out in the procedures and developed over time. Ad hoc audits can be conducted for any user or any patient at any time and are often conducted based on a tip or

[57] PIA Stream 1 - (Community) Pharmacy p. 16, March 11, 2013, PNNS0102-022A, p. 46.

information received. A series of weekly proactive audits are also currently conducted based on random samples from the pool of users province-wide. The DIS audit specialist requests the reports from the FairWarning platform operated by the Nova Scotia Health Authority (NSHA). According to the DIS staff, the proactive audits have successfully identified suspicious activities in the past, but some aspects of the audit process could be improved for better outcomes.

[195] Areas of improvement identified by the DHW are:

1. Direct access to the FairWarning platform and DIS logs would assist DHW to fully leverage the data and metadata kept in the logs. Currently, only pre-programmed fields are carried over from the DIS logs into the FairWarning platform. For example, end of action time stamps would provide more information about how long a record was open and what was done with it. Currently, FairWarning only draws out of the log the recorded time that the profile was accessed (start time stamp).
2. Direct access to the FairWarning platform and DIS logs would assist the DHW to fully leverage the data by being able to run reports directly as needed. Currently reports must be requested from NSHA occasionally resulting in delay and only pre-programmed reports can be provided easily.
3. The ability to exclude individuals recently audited from the random samples would improve the effectiveness of the random samples. Currently, the same individual may be included in the random sample shortly after previously being included. By excluding those recently audited from the random sample, the coverage of the random samples over time will be expanded.
4. Increasing the sample size would increase the coverage of the proactive audits. Currently, sample groups are 10 out of thousands of users across the province.
5. Strengthening the parameters of deemed appropriate access to capture more suspicious activity. Currently, access by a user that is accompanied by dispense activity within a prescribed period of time before and after the access is considered valid. Two possible improvements were identified by the DHW: a shorter time frame before and after prescription activity and a requirement that for a valid access finding the user in question must be the individual engaged in any identified prescription activity.

[196] As noted earlier, the access of individual users to the DIS is based on the access granted in the local POS system. The 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." Such monitoring would occur through the use of auditing user access to the POS database. The DHW's evidence was that it has not audited user organizations to ensure that they are themselves regularly monitoring access of their staff to the DIS or to their own POS system.

[197] **Finding #8:** The DHW has failed to adequately audit the DIS user organizations to ensure that the user organizations are regularly monitoring access of their staff to the DIS. The DHW's audit procedure for the DIS does not provide reasonable security for personal health information in that database.

Recommendation #9: DIS Audit Policy and Procedure

I recommend that the DHW develop more robust and systematic auditing policies and practices by taking the following steps:

i. The DHW either purchase its own version of the FairWarning platform for use on the DIS logs or arrange for direct access to the FairWarning platform held by the Nova Scotia Health Authority so that it can produce better and more effective audits.

ii. Update the audit criteria to include a requirement for proactive audits that flag:
   - same name lookups,
   - user organization employee lookups, and
   - lookups without user notes and not associated with dispensing activity within one week before or two weeks after the look up.

iii. Within six months of this report, conduct audits to ensure that:
   - All user organizations have the audit capacity to monitor access of staff to the DIS as required by the User Agreement. Where user organizations do not have such capacity, I recommend that the DHW ensure that an appropriate risk mitigation strategy is immediately implemented and that a FairWarning audit of all users within non-compliant user organizations is immediately conducted.
   - All user organizations are maintaining a record of every security breach of the custodian's electronic information system as required by *PHIA* Regulation 10(3).

4.3 Does the Department of Health and Wellness have reasonable security and information practices in place for the DIS in compliance with ss. 61, 62 and 65 of *PHIA*?

[198] Sections 61, 62 and 65 set out the security standards expected of health custodians. Section 65 raises the bar for custodians who maintain an electronic information system by requiring the custodians to implement additional safeguards as set out in the Regulations.[58] The DIS is one component of a much larger electronic information system serving the health care system in Nova Scotia.

[199] The PIA for the DIS describes the safeguards envisioned to protect the personal health information in the DIS. For example, the DIS is hosted on the NS Health Network on servers managed by the provincial government's information technology team. Entry points are firewall protected and access is limited by the data segregation of the various components of the overall electronic information system. The DIS is housed on dedicated servers separate from other health databases. The physical servers are protected by a secure access building with 24-hour security, video surveillance and staff are required to wear identification.

[200] Additional technical safeguards include the logging of transaction and access in the DIS audit log and all log files are backed up according to the province's backup procedures. As the DIS is one component of a larger electronic health information system, the assessment of the additional safeguards for the system cannot be viewed in isolation. The components are designed to work together.

---

[58] *Personal Health Information Act* Regulation, N.S. Reg. 217/2012 as amended, s. 10 (1-4).

[201] However, the management of the components of the system is separate and distinct. In this case, two integrated components are managed by different organizations, although still under the umbrella of the Minister of Health and Wellness. The DIS is managed by the DHW as a program area. The provincial Client Registry, also implicated in this series of privacy breaches, is managed by the Nova Scotia Health Authority who provides application support services. The Regulations prescribe that additional safeguards must be implemented to protect:

- Network infrastructure, including physical and wireless systems;
- Hardware and its supporting operating systems; and,
- Software, including the way a user's identity is authenticated.

[202] *PHIA* requires "additional safeguards" that are specific to the risks of an electronic system. The safeguards prescribed by the Regulations are inclusive, not exhaustive. Reasonable security measures require a custodian to anticipate risks and design mitigations that make sense. In this case, the custodian is the DHW operating multiple interrelated electronic health information databases that effectively form one electronic system where some users have access to multiple system components.

[203] The combination of these two databases with province-wide access provides a powerful ability to look up any person in the databases by first name, last name, or health card number. The Client Registry search function is such that a name look-up may produce many results which the user then scrolls down to select the individual she is looking for. Although the Client Registry provides a narrower scope of information, the search function is a powerful tool that can be used to identify a targeted individual with little to no information and no requirement to connect a search to providing health care services. Once a targeted individual is identified, further information from other databases, such as the DIS, can be retrieved.

[204] Our investigation revealed four significant shortcomings in the current management of Nova Scotian personal health information contained in large multi-user databases:

1. The compartmentalization of the management of each component limits an integrated management. In particular, the housing of the provincial Client Registry with a different organization (NSHA) hinders the DHW's ability to exercise its custodianship over that database and ignores the interrelated nature of the Client Registry with the DIS or other electronic health systems.
2. The broad ability to search the Client Registry with little to no information and no requirement to connect a search with the provision of health services makes the Client Registry an access portal or gateway for fishing expeditions that has implications for other health databases.
3. Within individual multi-user databases, such as the DIS, there is a lack of clarity around who has control of the data and who is ultimately responsible for the security of the data and the management of privacy breach investigations.
4. The ability of individuals tasked with auditing access to individual multi-user databases such as the DIS is hindered by their lack of direct access to the necessary audit tools and data.

[205] **Finding #9:** The DHW does not have sufficient additional safeguards in place to protect the database content of its broadly defined electronic health information systems, of which the DIS is one component, as required by s. 65 if *PHIA* and by Regulation 10(1)(c).

[206] In September 2016, I wrote to the Minister of Health and Wellness to highlight my concerns regarding control of large interoperable databases:

> There is an urgent need to create clarity around who has control of large interoperable databases. Multiple custodians have access to the data and can add to and amend the data through the life of the patient. From a patient's perspective, he or she may believe that his or her own custodian has complete control over the record of that "the government" has control over the record. Or, he or she may be entirely uncertain who is responsible for the record. The same is true for many custodians who access shared data without having a clear idea who is ultimately responsible for the data. Providing clarity on this issue will assist patients and custodians and will ensure that patients have a meaningful right of access. As electronic health record databases expand, this issue will be more and more of a problem. Addressing it now will create certainly for the further e-health projects.[59]

[207] At that time, I recommended that *PHIA* be amended to assign responsibilities for interoperable health databases in use in Nova Scotia to "prescribed entities". Prescribed entities already exist in *PHIA*, are subject to OIPC oversight and can be assigned specific responsibilities. I recommended that those responsibilities include auditing and monitoring use of interoperable data bases. On May 30, 2018, the DHW issued the *PHIA* Three Year Review Findings. The DHW determined that the issue of multiple custodians and electronic health records requires more study and proposed that a Digital Health Privacy Working Group be struck to study this issue. Issues relating to the security of data in multi-user, interoperable databases will only grow with the development of this technology. A longer-term solution is required to manage the increasing risks associated with this type of data management strategy. Any solution must involve accountability and oversight.

Recommendation #10: Multi-User Electronic Health Records

I recommend that the DHW amend *PHIA* by adding provisions that assign responsibilities for interoperable health databases in use in Nova Scotia to prescribed entities as follows:

i. Assign specified duties to these prescribed entities including:
   - manage and integrate personal health information received from custodians,
   - ensure proper functions of the electronic health record,
   - ensure accuracy and quality of personal health information,
   - keep an audit log (record of user activity) with prescribed information requirements,
   - keep an electronic record of all instances where a consent directive (s. 17 *PHIA*) is made, withdrawn or modified and include prescribed information requirements,

[59] Letter from Catherine Tully to the Honourable Leo Glavine, September 28, 2016.

- audit and monitor records it is required to keep (consent directives, audit logs), and
- make available record of user activity, consent directives and audit logs at the commissioner's request.

ii. In developing and maintaining the electronic health record, require the prescribed entities to:
- take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for developing and maintaining the electronic health record,
- prohibit employees from viewing, handling or otherwise dealing with personal health information unless the employee agrees to comply with the restrictions that apply to the prescribed organization,
- make available to the public and to each health information custodian that provides personal information to it a plain language description of the electronic health record and any directives, guidelines and policies of the prescribed organization that apply to the personal health information, and
- conduct threat and risk assessments including vulnerability and penetration testing with respect to the security and integrity of the personal health information.

iii. Set clear standards for privacy breach identification and notification to affected individuals, health custodians and the commissioner.

iv. Amend s. 5(1)(b) to make clear that prescribed entities are subject to *PHIA* and to the oversight of the OIPC.

5.0 Summary of Findings and Recommendations:

[208] I find that:

#1: The DHW does not have an adequate or effective privacy breach investigation protocol in place to deal with breaches involving multi-user health information databases.

#2: These privacy breaches are not adequately contained while there remains a realistic risk that the pharmacist will continue to use information she gained as a result of these inappropriate accesses.

#3: The DHW's privacy breach notification was not in compliance with *PHIA* in that it did not occur at the first reasonable opportunity and failed to include adequate information to affected individuals.

#4: The Health Privacy 1-800 line is an effective administrative safeguard that has generated valuable responses from the public. In this case, the DHW did not use this safeguard effectively.

#5: The roles and responsibilities under the User Agreement are sufficiently outlined and it serves as an adequate administrative safeguard. The implementation of the User Agreement does not accord with the roles and responsibilities set out and is unnecessarily hindered by the 'high trust model' of implementation.

#6: The administrative safeguard of requiring documentation when a DIS access is not accompanied by logged dispense activity has merit if implemented and associated with proactive monitoring.

#7: As an administrative safeguard, the DHW's Privacy Policy is ambiguous about its applicability to others outside of the DHW. However, taken together with the DIS User Agreement, it appropriately assigns responsibilities for the privacy program, including ensuring that any agreements entered into with third parties be compliant with legislation, regulations and the directives of the Privacy Policy.

#8: The DHW has failed to adequately audit the DIS user organizations to ensure that the user organizations are regularly monitoring access of their staff to the DIS. The DHW's audit procedure for the DIS does not provide reasonable security for personal health information in that database.

#9: The DHW does not have sufficient additional safeguards in place to protect the system software and database content of its broadly defined electronic health information systems, of which the DIS is one component, as required by s. 65 if *PHIA* and by Regulation 10(1)(c).

[209] I recommend that:

#1: DIS Breach Investigation Protocol (Corrective Action Process)
The DHW develop and implement an investigation protocol for the DIS. The protocol should:

i. Require that the Health Privacy Office of the DHW lead privacy breach investigations.
ii. Ensure that the Health Privacy Office has the authority to determine corrective action.
iii. Include a clear internal coordination protocol for any DIS privacy breach investigation.

#2: Containment
The DHW re-contact all 46 affected individuals to determine if the pharmacist has been in contact with them since April 24, 2018. If so, I recommend that the DHW take further legal action to prohibit the pharmacist from further using or disclosing the personal health information she obtained as a result of these breaches.

#3: Electronic Database Breaches
The Privacy Breach Protocol be revised to prescribe that where a user is found to have breached the privacy of any individual(s) via one of the electronic databases, detailed audits of that user's activity in other implicated databases be automatically conducted.

#4: Privacy Breach Notification
4(a) The DHW immediately notify the two individuals who never received the first breach notification letter because the mail was returned unopened. I recommend that the DHW confirm with the OIPC when this step is completed.
4(b) The privacy breach notification provisions in the DHW's Privacy Breach Protocol be revised as follows:

i. Clarify that notification at the <u>first reasonable opportunity</u> requires that notification occur within days (not weeks) of identification of affected individuals.

ii. Specify that notification need not await the identification of every affected individual and that notification can therefore occur as individuals are identified.
iii. Require that notification letters include, at a minimum, the following information:
    - A clear and specific statement about what occurred and how it was discovered.
    - A clear and specific statement about the personal health information that was accessed.
    - Information about what the individual can do to mitigate potential harm.
    - A clear and specific statement about steps taken to contain the breach and prevent it from happening in the future.
iv. Require that either the identity of the authorized individual who engaged in unauthorized access be provided in the notification letter or require that the record of user activity be enclosed with the notification letter.
v. Clearly advise affected individuals of their right to file a privacy complaint with the Office of the Information and Privacy Commissioner for Nova Scotia.

#5: Health Privacy 1-800 Line and Breach Investigations
The DHW establish a protocol for investigating anonymous and other tips to its Health Privacy 1-800 line, beginning with communicating to all staff that anonymous tips can and should be followed-up.

#6: DIS User Agreement
The DHW take the following actions with respect to the DIS User Agreement:
i. **Enforce existing terms**: The DHW should re-familiarize itself with its User Agreement and clarify internally the full extent of its authority and its responsibilities to manage and investigate a privacy breach by agents of a third-party user organizations under the Agreement.
ii. **User organization audits**: Require the DIS user organizations to regularly review access logs and conduct security audits of pharmacy software systems annually or more frequently.
iii. **Monitoring of user organizations**: Make the type and frequency of the DHW monitoring of user organization audits and audit capacity explicit and make the authority of the DHW to investigate privacy breaches involving the DIS explicit.
iv. **Notification to DIS user organizations**: Remind all DIS user organizations by August 31, 2018 that they must comply with the DIS User Agreement requirement that they regularly review access logs and that, at a minimum, they must conduct security audits of pharmacy software systems annually.

#7: DIS User Training
The DHW conduct training for all users of the DIS on the use of DIS notations.

#8: The DHW Privacy Policy
The DHW Privacy Policy be updated to reflect current position titles and to remove ambiguity about agency status of individuals not employed by the DHW.

#9: DIS Audit Policy and Procedure

The DHW develop more robust and systematic auditing policies and practices by taking the following steps:

i. The DHW either purchase its own version of the FairWarning platform for use on the DIS logs or arrange for direct access to the FairWarning platform held by the Nova Scotia Health Authority so that it can produce better and more effective audits.
ii. Update the audit criteria to include a requirement for proactive audits that flag:
    - same name lookups,
    - user organization employee lookups, and
    - lookups without user notes and not associated with dispensing activity within one week before or two weeks after the look up.
iii. Within six months of this report, conduct audits to ensure that:
    - All user organizations have the audit capacity to monitor access of staff to the DIS as required by the User Agreement. Where user organizations do not have such capacity, I recommend that the DHW ensure that an appropriate risk mitigation strategy is immediately implemented and that a FairWarning audit of all users within non-compliant user organizations is immediately conducted.
    - All user organizations are maintaining a record of every security breach of the custodian's electronic information system as required by *PHIA* Regulation 10(3).

#10: Multi-User Electronic Health Records

The DHW amend *PHIA* by adding provisions that assign responsibilities for interoperable health databases in use in Nova Scotia to prescribed entities as follows:

i. Assign specified duties to these prescribed entities including:
    - manage and integrate personal health information received from custodians,
    - ensure proper functions of the electronic health record,
    - ensure accuracy and quality of personal health information,
    - keep an audit log (record of user activity) with prescribed information requirements,
    - keep an electronic record of all instances where a consent directive (s. 17 *PHIA*) is made, withdrawn or modified and include prescribed information requirements,
    - audit and monitor records it is required to keep (consent directives, audit logs), and
    - make available record of user activity, consent directives and audit logs at the commissioner's request.
ii. In developing and maintaining the electronic health record, require the prescribed entities to:
    - take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for developing and maintaining the electronic health record,
    - prohibit employees from viewing, handling or otherwise dealing with personal health information unless the employee agrees to comply with the restrictions that apply to the prescribed organization,
    - make available to the public and to each health information custodian that provides personal information to it a plain language description of the electronic

health record and any directives, guidelines and policies of the prescribed organization that apply to the personal health information, and

- conduct threat and risk assessments including vulnerability and penetration testing with respect to the security and integrity of the personal health information.

iii. Set clear standards for privacy breach identification and notification to affected individuals, health custodians and the commissioner.

iv. Amend s. 5(1)(b) to make clear that prescribed entities are subject to *PHIA* and to the oversight of the OIPC.

6.0 Conclusion

[210] At the time of these breaches, the DHW did not have adequate processes in place to properly safeguard data in the DIS system nor to fully investigate and contain privacy breaches committed by an authorized user of the DIS system. This investigation highlights the immediate and urgent need for the DHW to develop long-term strategies that take into account the DHW's leadership role in the management and use of multi-user, multi-custodian systems. The DHW must have in place both administrative safeguards and technical safeguards in order to meet its obligations as a custodian under *PHIA* and more importantly, to meet the reasonable privacy expectations of Nova Scotians.

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

7.0 Acknowledgements

[212] 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.

[213] 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