Office of the Information and Privacy Commissioner for Nova Scotia

INVESTIGATION REPORT IR23-01

Nova Scotia Health
Intentional Employee Privacy Breaches

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia

TABLE OF CONTENTS

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Tricia Ralph

INVESTIGATION REPORT IR23-01

February 8, 2023

Nova Scotia Health

Commissioner's Message

The issue of intentional and unauthorized looking up and viewing of personal health information by healthcare employees (colloquially referred to as "snooping") is not new. This office has investigated previous incidents not only at Nova Scotia Health[1] (NSH) but at other custodians of health information. This investigation demonstrates how easy it is for employees to intentionally violate individuals' privacy when electronic health records are broadly available across many electronic information systems. It also demonstrates many of the challenges custodians face in holding employees accountable for this behaviour. It was no small job for NSH to respond to this series of privacy breaches, with a cascading discovery of historical privacy breaches, as was the case here.

This investigation finds that while NSH took many reasonable steps in responding to incidents of employees abusing their access to electronic health records, it also reveals areas where further investigation is warranted and identifies weaknesses in NSH's information practices to safeguard Nova Scotians' personal health information. I make recommendations for additional follow-up steps and for stronger safeguards to limit employees' access to look up and view only the electronic health records that they need to fulfill their jobs.

NSH now has a big task in front of it to set in motion what is required to prevent privacy breaches like these from happening in the future. If action is not taken, there will continue to be incidences of intentional privacy breaches by employees of NSH. Most Nova Scotians have no choice but to trust NSH to safeguard their most sensitive and intimate health information. Intentionally snooping on that information deserves condemnation and demands action to prevent its recurrence.

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia

[1] Nova Scotia Health is formally known as the Nova Scotia Health Authority established under Nova Scotia's *Health Authorities Act*.

Executive Summary

[1] In the weeks following Nova Scotia's tragic mass casualty event on April 18-19, 2020 (April 2020 tragedy), Nova Scotia Health (NSH) proactively monitored employees who were accessing the electronic health records of individuals associated with the events to ensure they had a valid reason to be viewing those records. Through this monitoring, NSH identified eight employees who accessed the electronic health records of individuals related to the April 2020 tragedy without a valid purpose. NSH then voluntarily reported these privacy breaches to the Office of the Information and Privacy Commissioner (OIPC).

[2] NSH conducted follow-up investigations which eventually identified more instances of unauthorized access of additional electronic health records by six of those eight employees and confirmed that two of them had long histories of what can only be described as 'serial snooping', where the employees repeatedly abused their access to NSH electronic health records to look up hundreds of individuals' sensitive personal health information without a legitimate need to do so. In these instances of unauthorized access, individual patients were specifically targeted by name because of their connection to the employee who was looking them up. The types of relationships that inspired employees to look up health information in these cases include: family, friends, children's friends, acquaintances from community organizations and sports, co-workers, neighbours, the other party in an automobile collision, former patients and persons receiving public attention or notoriety.

[3] The severity of the breaches was in direct correlation with the degree of access to electronic information systems granted to each employee. That is, employees who were granted greater access to electronic information systems looked up more sensitive and detailed personal health information far outside the requirements of their roles within NSH. In some cases, they accessed detailed health records about individuals' traumatic experiences and serious illnesses.

[4] The overall findings of this investigation are that despite the implementation of safeguards at NSH, unauthorized access to personal health information by NSH employees continues to be a recurring problem. While this investigation finds that NSH took many reasonable steps in responding to these privacy breaches, it also reveals areas where further follow-up actions are warranted and identifies weaknesses in NSH's information practices. I make recommendations to complete additional investigation follow-up and to implement stronger safeguards to protect the personal health information in NSH's custody or control.

1.0 Introduction, Jurisdiction and Investigative Process

1.1 Introduction

[5] On April 18-19, 2020, a man killed 22 people in and around Portapique, Nova Scotia. I refer to these events throughout this report as the April 2020 tragedy. These tragic events attracted a lot of attention with widespread, worldwide media coverage. The details of this appalling mass casualty event became the subject of a public inquiry.[2]

[6] NSH[3] proactively determined that it should monitor employee access to the electronic health records of individuals involved in or related to the April 2020 tragedy. From this initial monitoring, NSH identified eight employees who accessed electronic health records without a valid reason and voluntarily reported these as privacy breaches to the Office of the Information and Privacy Commissioner (OIPC), on June 15, 2020.

[7] NSH then conducted further investigations of access to electronic health records by these eight employees when it was determined that they had no valid reason to access high-profile electronic health records. The subsequent investigations uncovered significant additional unauthorized accesses which proved to be an important aspect of containing these privacy breaches.

[8] Based on NSH's voluntary report to this office, I initiated this investigation.

[9] The situation of a public tragic event inspiring authorized users of electronic information systems to abuse their access to look up individuals' medical information is not unique. The Humboldt Broncos hockey team bus crash of 2018 resulted in five reports issued by the Saskatchewan Information and Privacy Commissioner.[4] A doctor who was the subject of one of those investigations tried to prevent the publication of her identity in the Saskatchewan Commissioner's report. In denying her injunction request, the judge commented about people abusing their access to medical records. He said:

> Of course, people wanted to know what had happened, and why. They wanted to know how the survivors were doing. In a time marked by confusion, and in a time simultaneously calling for privacy and compassion, the quest for information that is the hallmark of our present era continued unabated.[5]

[10] Although that situation was different than the one looked at here, there are many similarities and Justice Danyliuk's words could equally be written about this case. While it may

---

[2] The Mass Casualty Commission website, online <https://masscasualtycommission.ca>.
[3] In 2020-2021, NSH rebranded from Nova Scotia Health Authority to Nova Scotia Health. Its legal name remains Nova Scotia Health Authority.
[4] *SK IR177-2018, Ockbazghi (Re)*, 2019 CanLII 7175 (SK IPC); *SK IR240-2018, Saskatchewan Health Authority involving Dr. M (Re)*, 2019 CanLII 7171 (SK IPC); *SK IR161-2018, eHealth Saskatchewan (Re)*, 2019 CanLII 7176 (SK IPC); *SK IR162-2018, Falah Majid Medical P.C. Inc. (Re)*, 2019 CanLII 7173 (SK IPC); *SK IR180-2018, 181-2018, 226-2018, Saskatchewan Health Authority involving Dr. R (Re)*, 2019 CanLII 7172 (SK IPC).
[5] *Stebner v. Canadian Broadcasting Corporation*, 2019 SKQB 91 (CanLII), at para. 12.

be natural to want to know what happened to the individuals associated with the April 2020 tragedy, employees were not entitled to look at their electronic health records without a valid reason to do so, such as being directly involved in their care. Employees must set that curiosity aside and respect the fundamental rule that they are not entitled to look at electronic health records without a valid reason.

1.2 Jurisdiction

[11] NSH is a designated custodian within the meaning of s. 3(f)(iv) of the *Personal Health Information Act* (*PHIA*)[6] and its employees meet the definition of "agent" within the meaning of s. 3(aaa) of *PHIA*. In this report, NSH is referred to as custodian. The individual employees at the heart of the privacy breach responses reviewed here are referenced by assigned letter A, B, C, D, E, F, G and H.

[12] NSH audit reports of employee access show that eight employees accessed varying degrees of personal health information, ranging from registration information (such as name, date of birth, health card number and appointment schedule) to, in some cases, detailed and highly sensitive medical records generated in clinics or parts of NSH far outside what they needed to view in order to do their work (both geographically and in terms of subject matter). The information accessed by the eight employees is personal health information within the meaning of s. 3(r) of *PHIA*. The information stored within NSH's electronic information systems was within its custody and control. Therefore, *PHIA* applies.

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

[14] The information provided to this office on June 15, 2020, outlines a series of privacy breaches of a broad scale and large volume in terms of the number of individuals affected, the number of employees identified, the diversity of employee positions and worksites involved, and the range of historical, repeated and systematic privacy breaches that were uncovered by NSH. These facts provided sufficient grounds to initiate this investigation under s. 92(2)(b) of *PHIA*.

1.3 Investigative process

[15] The OIPC obtained and reviewed NSH's policies, procedures and records related to NSH's electronic information systems, how NSH maintains those systems, how access to them is granted to employees, as well as the steps NSH took to investigate and respond to this series of privacy breaches.

[16] Oral and written representations were obtained from NSH's Privacy, Human Resources and Information Technology (IT) Offices. Oral statements were also obtained from individuals

---

[6] *Personal Health Information Act (PHIA)*, SNS 2010, c 41.

who complained to this office following notification of the privacy breaches. Each of the eight identified employees was invited to provide oral representations. Only one did.[7]

[17] Both the NSH and OIPC investigations unfolded in the context of the state of emergency declared in Nova Scotia in response to the COVID-19 pandemic. NSH was navigating care provision and actioning evolving Public Health Directives during a global pandemic at the same time it was investigating these privacy breaches and responding to the OIPC's investigation. This made this large-scale investigation particularly challenging. Despite this, NSH was responsive and engaged with the OIPC investigation.

2.0 Background

2.1 About NSH as it relates to this investigation report

[18] NSH is a provincial health authority under the *Health Authorities Act*[8] created in 2015. According to its *2020-21 Annual Report*,[9] NSH employs approximately 24,722 unionized and non-unionized employees organized in four zones: Central, Northern, Eastern and Western. It operates 10 hospitals and 135 other community clinical or support and administrative units.

[19] To deliver its mandate, NSH currently operates a complex web of up to 500 electronic clinical software applications and over 20 diagnostic imaging applications, along with the associated digital storage, retrieval and viewing systems that together make up NSH's electronic information systems.[10]

[20] Over the years, NSH has implemented the following initiatives in support of protecting privacy:

- In 2013, NSH implemented an add-on to its electronic information systems called Fairwarning[11] to collect information about user activity from source systems, platforms and equipment. Fairwarning allows NSH to search within the data of user activity and run reports which are used to audit and monitor activity. The reports are referred to as audit reports.
- In 2016, NSH implemented a provincial Privacy Office with a privacy manager leading a team of four privacy officers, one for each zone of NSH operations.

---

[7] It is worth noting that in Nova Scotia, the legislation does not give the Information and Privacy Commissioner authority to compel oral or written evidence. As I explained in *Review Report 20-07, Public Prosecution Service (Re)*, 2020 NSOIPC 7 (CanLII), at para. 21, this lack of authority is problematic and should be rectified as almost every other jurisdiction in Canada gives its Information and Privacy Commissioner some authority to compel witness testimony.

[8] *Health Authorities Act*, SNS 2014, c 32.

[9] NSH, *By the Numbers 2020-21* (undated), online: NSH <https://www.nshealth.ca/AnnualReport2020-21/numbers.html>.

[10] NSH Information Technology Office oral representations January 18, 2021.

[11] Fairwarning is a commercial application that interfaces with electronic information systems and devices, pulling up user activity so it can be compiled and searched.

- In 2017, NSH approved a privacy policy setting out various procedures relating to the privacy and confidentiality of personal health information, referred to as the *NSH Privacy Policy*.[12]
- In 2019, NSH approved an updated protocol to help manage privacy breaches referred to as the *NSH Privacy Breach Protocol*.[13]
- In 2019, NSH approved a policy related to auditing user activity referred to as the *NSH Auditing Policy*.[14]
- In 2019, NSH initiated a program to regularly audit user activity referred to as the *NSH Audit Plan*.[15]
- NSH maintains an ongoing privacy education program including:
    - Topic specific posters and memos to employees;
    - An intranet website providing access to privacy education and resources;
    - An annual online learning module for employees;
    - An annual employee confidentiality pledge that explicitly sets out the limits of employees' authority to collect, access, use or disclose personal health information;
    - A privacy and confidentiality presentation for new employees;
    - Privacy education sessions for supervisors and managers.

2.2 A history of intentional privacy breaches by NSH and former district health authority employees

[21] Over the years, NSH and the former district health authorities it replaced have responded to a number of intentional privacy breaches by employees abusing their access to electronic information systems without a valid reason.

[22] In 2017, the Supreme Court of Nova Scotia approved a settlement after 707 patients were notified that their personal health information had been inappropriately viewed by an employee without a work-related purpose for over a year. The proposed settlement was one million dollars.[16]

---

[12] NSH, *Privacy and Confidentiality of Personal Health Information Policy (NSH Privacy Policy)* (Approval date: February July 10, 2017. Effective date: February 13, 2020), online: <http://policy.nshealth.ca/Site_Published/NSHA/document_render.aspx?documentRender.IdType=6&documentRender.GenericField=&documentRender.Id=75676>.

[13] NSH, *Nova Scotia Health Authority Privacy Breach Management Protocol* (*NSH Privacy Breach Protocol*), (updated May 2019). This policy is not available online. It was provided to the OIPC in NSH written representations dated September 3, 2020.

[14] NSH, *Auditing of Access to Personal Health Information in Electronic Information Systems Policy* (*NSH Auditing Policy*) (Approval date: February 4, 2019. Effective date: July 3, 2019), online: NSH <https://policy.nshealth.ca/Site_Published/nsha/document_render.aspx?documentRender.IdType=6&documentRender.GenericField=&documentRender.Id=74370>.

[15] NSH, *Annual Audit Program 2019* (*NSH Audit Plan*) (2019). This plan is not available online. It was provided to the OIPC in NSH written representations dated September 3, 2020.

[16] Elizabeth Chiu, *Hospital Clerk's Snooping Could Cost Nova Scotia Taxpayers $1M* (June 2017), online: CBC <https://www.cbc.ca/news/canada/nova-scotia/shelburne-hospital-roseway-clerk-patient-records-settlement-1.4162568>. While there is publicly available information that a settlement was reached, the amount ultimately reached is not readily available online. See Wagners, *South West Health Privacy Breach* (January 2019), online: Wagners: <https://wagners.co/practice-areas/class-actions/south-west-health-privacy-breach/>.

[23] In 2017, the OIPC completed an investigation after being informed by NSH of a series of privacy breaches affecting 335 electronic health records by six employees at multiple worksites. We reported that "Our investigation revealed a dangerous and insidious culture of entitlement to view health records, with accounts of unauthorized access that, in some cases, took place over a long period of time."[17] NSH accepted the OIPC's recommendations and took steps to improve its education to employees and strengthen its privacy breach management protocol.

[24] During this current OIPC investigation, NSH stated that between August 2017 and February 2020, it also responded to intentional privacy breaches by another eight employees affecting 22 individuals. These breaches occurred at the same worksites that are under review in this investigation.[18] None of these breaches were reported to the OIPC or to the public, but the affected individuals were notified as required by *PHIA*.[19]

[25] In 2018, NSH reached a $400,000 settlement agreement after 105 peoples' electronic health records were improperly accessed between 2005 and 2011. The former NSH employee gave a statement to media in 2012 where she said that she wasn't proud of what she did and explained her actions this way: "Plain and simple, the information was there. So easy."[20]

[26] In 2019, NSH voluntarily reported to the OIPC that it was notifying 57 individuals who were targeted by one of its senior transcriptionists who searched for and viewed sensitive personal health information and used that information to the detriment of the targets.

[27] In November 2020, another class action lawsuit involving employee snooping at NSH was filed. The proposed class members are individuals whose privacy was breached due to inappropriate employee access to their personal health information from 2018 to 2020.[21]

[28] This current investigation was conducted in the context of the history of unauthorized access to electronic health records by some employees at NSH. It is clear from this historical accounting and the continued discovery of this type of intentional privacy breach that the problem is not isolated or infrequent, rather it is reoccurring and widespread.

---

[17] Office of the Information and Privacy Commissioner for Nova Scotia, *2017-2018 Annual Report* (November 2018) online: <https://oipc.novascotia.ca/sites/default/files/publications/annual-reports/OIPC%202017-2018%20Annual%20Report_0.pdf> at pp. 21-22.
[18] NSH *Breach Listing*, undated document, NSH written representations January 11, 2021.
[19] Sections 69 and 70 of *PHIA* require notification to the OIPC only in situations where it is unlikely that a breach of the personal health information has occurred, or there is no potential for harm or embarrassment to the individual as a result and the custodian has decided to not notify the individuals.
[20] CBC, *Former Capital Health Worker Sorry for Privacy Breach* (February 2017), online: CBC <https://www.cbc.ca/news/canada/nova-scotia/former-capital-health-worker-sorry-for-privacy-breach-1.1222089>.
[21] *Carla Munroe v. the Nova Scotia Health Authority* (23 Nov 2020), Halifax 502113 (NSSC) (Statement of Claim) <https://www.courts.ns.ca/Supreme_Court/documents/HFX_502113_Statement_of_Claim.pdf>.

3.0 Issues

[29] There are two issues in this investigation:

1. Did NSH take reasonable steps in response to the reported privacy breaches as required by ss. 61 and 62 of *PHIA*?
2. Did NSH have reasonable security and information practices in place for its electronic information systems as required by ss. 61, 62 and 65 of *PHIA*?

4.0 Analysis and Findings

4.1 Issue #1: Did NSH take reasonable steps in response to the reported privacy breaches as required by ss. 61 and 62 of *PHIA*?

[30] The reasonableness of a response following a privacy breach must be assessed within the specific circumstances of the privacy breach. The OIPC encourages entities responding to a privacy breach to follow four steps, as set out in the OIPC's guidance document entitled *Key Steps to Responding to Privacy Breaches* (*NS OIPC Key Steps Document*).[22] The four key steps are:

1. Contain and investigate the breach
2. Evaluate the risks
3. Notification
4. Prevention

Step 1: Contain and investigate the breach

[31] Step 1 of the response to a privacy breach is to contain and investigate it. This step requires a custodian to take immediate and common sense steps to limit the breach. The specific steps required will depend on the specific privacy breach at issue, but include:

a) *Contain*: Immediately stop the unauthorized practice and shut down a breached electronic information system or access to an electronic information system.
b) *Initial investigation*: Immediately conduct an initial investigation with a designated lead individual who has authority to complete the initial investigation. Conduct a more detailed investigation subsequently if required.

---

[22] NS OIPC, *Key Steps to Responding to Privacy Breaches* (December 2019), online: NS OIPC <https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20to%20Responding%20to%20Privacy%20Breaches%20-%20OIPC%20-2019%2012%2002.pdf>. This document 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*; the Office of the Information and Privacy Commissioner for British Columbia *Privacy Breaches: Tools and Resources;* the Office of the Information and Privacy Commissioner of Alberta, *Key Steps in Responding to Privacy Breaches* and the Office of the Information and Privacy Commissioner of Ontario, *Responding to a Privacy Breach: Privacy Breach Protocol*.

c) *Internal notifications*: Give appropriate internal notifications to the privacy officer and others who need to be made aware.
d) *Breach response team*: Determine whether a breach response team is required.
e) *Police*: Determine whether police should be involved.
f) *Preserve evidence*: Preserve any evidence of what occurred.[23]

[32] The *NSH Privacy Breach Protocol*, *NSH Auditing Policy* and the *NSH Audit Plan* are key information practices implemented by NSH to help guide its responses to privacy breaches.

[33] The *NSH Auditing Policy* and *NSH Audit Plan* call for initial monitoring of employee access to "high-profile" patient records. NSH began monitoring access to the electronic health records of the individuals associated with the April 2020 tragedy using audit reports drawn from its Fairwarning system. The initial monitoring period covered user activity from April 19, 2020, with the first audit report generated on April 27, 2020. This was effective in discovering unauthorized access to the electronic health records of individuals associated with the April 2020 tragedy by eight NSH employees. Without this monitoring, the unauthorized employee activity might have gone unnoticed.

[34] NSH then conducted further investigations of access to electronic health records by these eight employees when it was determined that their high-profile access had no valid reason. The subsequent investigations uncovered significant additional unauthorized accesses of information of a wide range of people unassociated with the April 2020 tragedy.

[35] Despite the above, there are some areas where NSH's investigation and containment efforts were not fulsome or complete.

Review of investigation and containment efforts

Employee A: Booking and registration clerk

[36] Employee A was flagged by the NSH Privacy Office after accessing the electronic health records of an individual associated with the April 2020 tragedy on April 20, 2020. NSH then did an expanded audit of all Employee A's access over a one-year period and eventually confirmed unauthorized access of an additional two individuals, confirmed to be Employee A's neighbours.

[37] NSH held three meetings with Employee A, during which Employee A was asked to explain the access shown on the audit reports that did not match Employee A's job duties. During the first meeting, Employee A admitted to looking up information about an individual associated with the April 2020 tragedy and provided an explanation that they were shocked and scared, and that their family member had been nearby during the events and could have been a victim. During the first meeting, Employee A denied knowing any of the other individuals whose information they accessed. NSH could not identify a job-related reason for the employee to access the records.

[23] *NS OIPC Key Steps Document* at p. 3.

[38] During the second meeting, Employee A again denied knowing the other individuals, but claimed to have received a phone call transferred by the switchboard from a mother looking for information about her son.

[39] Finally, during the third meeting, NSH confronted Employee A with the home addresses for the two additional individuals for whom Employee A accessed electronic health records. Those individuals lived on the same street as Employee A. Employee A then admitted to being a neighbour of those two individuals. Employee A provided an explanation that the telephone call was real, it was the neighbour, a mother trying to get information about why her adult child was in the hospital and whether certain medications were being prescribed. No explanation was given for the other unauthorized access. Employee A denied sharing any information with anyone. Additionally, NSH reviewed Employee A's NSH email account to determine if any personal health information had been shared using that platform and found none.

[40] Employee A was placed on administrative leave on April 21, 2020, until employment was terminated on May 20, 2020. Employee A's access to electronic information systems was not suspended during the period of administrative leave.

Employee B: Ward clerk

[41] Employee B was flagged by the NSH Privacy Office after accessing the electronic health records of an individual associated with the April 2020 tragedy on April 20, 2020. NSH then did an expanded audit of all Employee B's access over a one-year period. The expanded audit found that Employee B accessed the information of 75 individuals whom the supervisor recognized as nursing and physician staff at the facility where Employee B worked.

[42] NSH held two meetings with Employee B to investigate. During their meetings, the employee admitted to accessing these electronic health records and admitted to knowing it was wrong and in violation of NSH privacy policies. NSH documented that the employee's explanation was that a recent conversation with a paramedic had prompted the lookup as the employee was trying to determine if a specific individual associated with the April 2020 tragedy was a patient Employee B had previously discussed with the paramedic. In terms of the other lookups, the supervisor eventually determined that there were explanations and consent of the employees Employee B looked up and was satisfied that the additional accesses to the information of 75 individuals were not privacy breaches, though they were also not authorized because they were not strictly speaking part of the employee's job.

[43] Employee B was placed on paid administrative leave pending the investigation and was issued discipline in the form of a one-day suspension. Employee B's access to NSH electronic information systems was not suspended during the period of administrative leave.

Employee C: Nurse navigator

[44] Employee C was flagged by the NSH Privacy Office after accessing the electronic health records of an individual associated with the April 2020 tragedy on April 22, 2020. NSH then did an expanded audit of Employee C's access over a one-year period and identified access to the

electronic health records of 16 individuals for which it could not confirm a valid work-related purpose.

[45] NSH held two meetings with Employee C, during which Employee C admitted to accessing the health information of a former patient who was associated with the April 2020 tragedy. Employee C admitted to accessing the electronic health records after hearing of the former patient's death to see the individual's health status at the time of death. Employee C immediately acknowledged that it was wrong and in violation of NSH's privacy policies. Employee C was placed on administrative leave on May 12, 2020, and access to electronic information systems containing personal health information was suspended on May 14, 2020.

[46] In terms of the expanded one-year audit, Employee C denied looking up the individuals for any unauthorized purpose. Eventually, NSH concluded that the access to the information of the identified 16 individuals related to the employee looking up the records of individuals who called to inquire about the program delivered by the clinic. This type of phone inquiry was not previously documented if the inquiry did not result in the individual formally engaging with the program. NSH eventually decided that, because of the nature of the specialty program, it was reasonable for Employee C's role to have accessed the records of individuals who inquired about the program even if they didn't subsequently pursue the program. However, without a process to document this type of inquiry, NSH could not confirm on its own that the accesses in question were done for this reason. NSH did not contact those individuals whose records were accessed by Employee C to confirm whether they had inquired about the program by phone. NSH did implement a new tracking system at that clinic to document this type of inquiry in the future.

[47] Employee C was issued discipline in the form of a one-day suspension, following which Employee C was required to re-complete NSH's online privacy training module and re-sign its Confidentiality Pledge. Employee C's access to electronic health records was reinstated after the conclusion of the investigation.

Employee D: Nurse practitioner

[48] Employee D was flagged by the NSH Privacy Office on May 5, 2020, after accessing the electronic health records of an individual associated with the April 2020 tragedy on May 1, 2020.

[49] On May 14, 2020, the employee's manager had a meeting with Employee D. The employee admitted to checking the patients discharged from their program area because they thought that one of the casualties of the April 2020 tragedy was one of the program's patients. NSH did no additional follow-up with this employee until the OIPC asked follow-up questions as part of this investigation. No additional auditing was done of this employee's historical access. Employee D's access to NSH's electronic information systems was never suspended.

[50] Catching an employee accessing the records of someone that is getting media attention is a reasonable basis on which to conduct additional audits of the employee's access. Looking up a high-profile individual is a reasonably good indicator of the potential for other unauthorized access and audit reports are the primary way of discovering unauthorized access by users of an

electronic information system. Additional audits in these circumstances offer significant protection for personal health information.

[51] Conducting additional audits in the circumstances that flagged Employee D's access is provided for under the *NSH Privacy Breach Protocol* and in the *NSH Auditing Policy*. These two NSH policies set out reasonable information practices for these circumstances and NSH did not comply with them in the case of Employee D.

Employee E: Admitting clerk

[52] Employee E was flagged by the NSH Privacy Office after accessing the electronic health records of two individuals associated with the April 2020 tragedy on April 19, 2020, and on May 9, 2020. NSH did an expanded audit of all of Employee E's access for the previous six-month period. The employee initially denied it, but once confronted with the audit reports, admitted that some of the accesses on the additional audit reports were looking up their family members without a valid job-related purpose.

[53] As part of its investigation, NSH held a meeting with Employee E on May 27, 2020.

[54] The records of the meeting held on May 27, 2020, and the letter of termination, document the explanations for the access that Employee E provided, which were:

- In relation to family members: Checking to see who was listed as the emergency contact; checking the demographic information on record; looking up lab results; looking to see when surgery was scheduled; wanting to know when the surgery was scheduled because anxious about getting the day off to support that family member.
- In relation to the April 2020 tragedy: Admitted to accessing the electronic health records of an individual associated with the April 2020 tragedy but could not say why; admitted to accessing the electronic health records of another individual associated with the April 2020 tragedy but thought it was because someone called looking for information. When asked about giving information over the phone, Employee E responded that they "couldn't find anything to give them anyway."

[55] Employee E's access to NSH's electronic information systems was not suspended during the investigation. Employee E was terminated on June 2, 2020, but access to the systems continued until June 5, 2020 (after the date employment was terminated).

Employee F: Secretary at an outpatient clinic

[56] Employee F was flagged by the NSH Privacy Office after attempting to search the name of an individual associated with the April 2020 tragedy on April 24, 2020. The attempt was not successful because there were no corresponding records, but the NSH Privacy Office flagged the attempt as requiring further investigation because it suspected there was no valid purpose for the lookup.

[57] A first meeting was held with Employee F on June 4, 2020, during which Employee F initially denied attempting to access any records without a valid reason. However, by the end of the meeting, Employee F admitted to additional accesses and claimed to have looked up staff phone numbers to prepare a 'call out' list for emergencies, along with a range of other explanations for what might look like random patient lookups on the user access reports.

[58] The supervisor then initiated a broader audit of the employee's access over the previous two years. NSH also continued to investigate by interviewing other employees, comparing the access activity with known patients of the clinic and analyzing the list of people Employee F accessed in light of the employee's claim about creating a 'call out' list.

[59] A second meeting was held on June 19, 2020, to discuss the results of the additional audit reports and investigation. NSH eventually concluded that Employee F was responsible for 612 privacy breaches affecting 146 individuals including co-workers and their families, staff in other departments of NSH, physicians, and prominent members of the local community, including a former premier and his family. Employee F only had access to registration and scheduling information for the position, therefore the extent of the access was limited. However, the scheduling information displays a person's past and future appointments, including location and purpose of the appointment, which Employee F accessed.

[60] Employee F was placed on administrative leave pending the investigation on June 10, 2020 and was terminated on June 19, 2020. Employee F's access to NSH's electronic information systems was maintained until July 6, 2020, at which time it was terminated.

[61] NSH concluded that many of the patients whose information Employee F accessed had never been seen in the clinic where Employee F worked. NSH also concluded that Employee F demonstrated a pattern of accessing patient information when Employee F was aware that the patient might need health care.

[62] Additionally, in conducting its follow-up investigation, NSH discovered through its communication with affected individuals (Employee F's co-workers), that previous complaint(s) had been made by co-workers about Employee F looking up people's information. NSH had no record of a previous complaint and therefore could not confirm the scope of the complaint or any follow-up actions. The staff in the relevant positions had all turned over since that time. NSH responded to this as an unaddressed concern and held a meeting "to ensure that the current manager was aware of her duties in ensuring that future concerns are handled appropriately."[24]

Employee G: Secretary at a regional hospital

[63] Employee G was flagged by the NSH Privacy Office after accessing the electronic health records of an individual associated with the April 2020 tragedy on April 21, 2020.

[64] NSH held a meeting with Employee G on June 4, 2020, during which Employee G stated that in the days following the April 2020 tragedy, several of the staff were curious about one of

[24] NSH written representations January 11, 2021.

the individuals associated with that event, but Employee G was the one "that bit the bullet" and looked that person up. NSH did no additional follow-up to determine if any other staff were present when Employee G looked up those electronic health records.

[65] NSH did expanded audits of six months and then two years of Employee G's access to electronic health records. From those audits, the access of the information of 42 patients was initially identified as having no known purpose for Employee G's position. The nurse practitioner at the site where Employee G worked confirmed that it is common to ask this employee to look up personal health information on their behalf for the purpose of providing care. A physician at the site responsible for the patients, who did not normally work with Employee G, thought it was possible but did not recall having asked the employee to look up anything related to their patients.

[66] NSH ruled out as privacy breaches any patients who were connected to the nurse practitioner and all the doctors at the clinic on the off chance they were connected to a legitimate work-related purpose. After this, there remained 12 individuals who had no connection to the clinic where Employee G worked and for whom there was no identified legitimate reason for Employee G to access their records. NSH could not decide if Employee G's access was authorized or not, and initially took no action to notify affected individuals. However, it eventually notified the 12 individuals after the OIPC inquired about notification to them during this investigation.

[67] The NSH held one meeting with Employee G on May 27, 2020. NSH records show that the human resources manager decided there was "a different vibe" when the breaches were discussed with this employee versus two others the human resources manager had spoken with. Employee G was given a verbal warning which was confirmed in writing on July 30, 2020. Employee G's access to NSH's electronic information systems was never suspended.

Employee H: Booking clerk

[68] Employee H was first flagged by the NSH Privacy Office after accessing the electronic health records of several individuals associated with the April 2020 tragedy on April 21, 2020.

[69] NSH did an expanded audit of Employee H's access over a two-year period. Meetings were held with Employee H, the manager, a human resources representative and a union representative on May 21, June 17, July 17 and August 4, 2020.

[70] Employee H did eventually admit to accessing electronic health records without a valid purpose. The explanations Employee H provided were boredom, curiosity and that they "felt too comfortable in the role." NSH concluded that Employee H was responsible for 525 privacy breaches affecting 101 individuals, slightly more than half of which involved accessing highly sensitive and detailed health information, including records from a wide range of clinics and care sites in multiple zones of the health authority.

[71] The NSH investigation found that Employee H had a pattern of accessing information about neighbours, friends, co-workers, children's friends or associates and their parents, individuals associated with other tragic events and others unknown.

[72] Employee H was placed on paid administrative leave on May 21, 2020, and access to NSH's electronic information systems was suspended on May 22, 2020. Employee H's employment was terminated on August 4, 2020.

A ninth employee flagged but not identified

[73] NSH did not contain or complete the investigation of an additional ninth confirmed unauthorized lookup of the electronic health records of an individual associated with the April 2020 tragedy. This additional ninth employee's access was not reported to the OIPC along with the eight others, rather it was discovered among the records the OIPC reviewed as part of the investigation.

[74] This ninth unauthorized user access was logged by a user account assigned to a doctor. NSH's monitoring flagged the lookup for follow-up to confirm the validity of the purpose. NSH questioned the doctor about the lookup and the doctor claimed that someone else must have used their login information without their knowledge.[25]

[75] The NSH Privacy Office followed up with the doctor's supervisor and reviewed additional audit reports around the time of the flagged access. NSH noted several unsuccessful login attempts under the doctor's account around the time of the unauthorized access and concluded that the failed login attempts showed someone attempting to login with different passwords, eventually being successful. NSH did not make any further attempts to determine which employees were working during the time of the flagged access in proximity to the terminal that was used and who may have had access to the doctor's login credentials.

[76] The NSH privacy representative admitted that the individual responsible for this unauthorized lookup has not been identified.[26] Because the person responsible for this instance of unauthorized access has not been identified, the breach is not contained. Additional investigation could elicit more about the author of this privacy breach. Conducting further audits of the doctor's access is warranted.

[77] In the other breaches under review here, multiple employees initially lied about their access and another never claimed responsibility for the identified access that had no valid purpose. Conducting additional audits for a one-year period prior to a confirmed privacy breach is a safeguard specifically designed to identify other potential unauthorized accesses and has been effective in confronting employees who initially lied. Conducting further audits of employee access is a reasonable information practice in these circumstances.

[25] NSH Privacy Office oral representations March 12, 2021.
[26] NSH Privacy Office oral representations March 12, 2021.

[78] Further, in this circumstance, it would also be warranted to investigate the doctor's claim that someone commandeered their account. If this is the case, an individual willing to go to such lengths to hide their misconduct poses a serious ongoing risk to personal health information at NSH. Additional questions should be asked about who the doctor shared their login credentials with or how someone could obtain those credentials. What device or terminal was used during the access and which staff who may have had access to the doctor's login credentials were working in the vicinity of the terminal on the day of the access? Answering these questions could narrow the possibilities down to a smaller group of people for further investigation.

[79] **Finding #1:** I find that NSH's initial response of conducting additional audits of employees whose access was flagged on audit reports was reasonable and required by the circumstances. However, I further find that NSH failing to conduct additional audits of Employee D and the doctor associated with the ninth unidentified employee was not reasonable in the circumstances.

[80] **Recommendation #1:** I recommend that within 60 days of the date of this report, NSH conduct additional audits of electronic information systems access by Employee D and the doctor associated with the ninth unidentified employee for the one-year period prior to the identified privacy breach and conduct any investigations required as a result of those audits.

Suspending employees' electronic information systems access

[81] Both the *NS OIPC Key Steps Document* and the *NSH Privacy Breach Protocol* note the importance of immediately suspending employee access to electronic and physical information systems pending investigation. In some cases, NSH failed to do this. As set out below, real harm resulted from this failure.

[82] Step 1 of the *NSH Privacy Breach Protocol* states that employees who discover a potential breach must take immediate steps to contain the breach and secure the affected records and systems. It points the reader to Appendix B for suggested containment strategies. Appendix B then states, "Access to electronic, physical and verbal PHI is immediately restricted, suspended or revoked until completion of the investigation."

[83] For further clarity, Appendix A of the *NSH Privacy Breach Protocol* sets out the "Roles and Responsibilities" in detail where it states that the zone privacy officer's responsibilities include, "In cases of inappropriate access, ensures that all system access is revoked while the investigation is ongoing; obtains or run employee activity audits for affected systems." The NSH provincial privacy manager and NSH general counsel responsibilities include, "Decides upon containment strategies when there is a disagreement. Approves requests to NOT suspend system access or employment for investigations involving inappropriate access."

Suspending remote access to electronic information systems pending investigation

[84] One of the suggested investigation techniques explained in Appendix C of the *NSH Privacy Breach Protocol* is to investigate any remote access abilities of the employee. Despite this, NSH missed identifying that seven of the eight employees had virtual private network

(VPN) access enabled. VPN technology supports remote access to web-based applications.[27] As a result, the employees who were enabled with a VPN and whose electronic information systems access was not suspended appear to have maintained remote access to those systems and to web-enabled systems throughout the investigation and while on administrative leave (if they were placed on administrative leave), and in one case, access was maintained for three days after the employee was terminated.

[85] When asked about remote access by the employees, the representative of NSH's Human Resources Office thought that placing an employee on administrative leave was essentially the same thing as suspending access to the electronic information systems and had not considered the possibility of remote access by these employees.[28] The representative of the NSH Privacy Office stated that before the OIPC requested a list of access granted to each employee, it was not their practice to take this step and they did not realize the full extent of the access granted to these employees.[29]

[86] NSH did not appear to consider the requirement for immediate suspension of electronic information systems access in any of the cases reviewed here. NSH provided no documentation that immediate suspension of systems access upon first flagging the employees' accesses to information of individuals related to the April 2020 tragedy was part of its immediate initial containment efforts, despite the *NSH Privacy Breach Protocol* stating that "containment strategies should be identified and implemented on the day the breach is discovered."[30]

Inconsistencies and delays in suspending in-person access to electronic information systems

[87] Appendix B of the *NSH Privacy Breach Protocol* provides suggested containment strategies which include immediately restricting, suspending or revoking access to personal health information pending the outcome of the investigation. In this case, there were significant delays and inconsistencies in the suspension of in-person electronic information systems access. The OIPC calculated the number of days it took NSH to suspend the access of each of the employees after having been flagged: [31]

Employee A: 23 days
Employee B: never suspended
Employee C: 17 days
Employee D: never suspended
Employee E: 39 days (three days after Employee E was terminated)
Employee F: 70 days (Employee F was placed on administrative leave after 44 days)
Employee G: never suspended
Employee H: 25 days

[27] NSH records of each employee's access to electronic information systems show that Employees A, B, C, D, E, F and G were enabled with a Global Protect Virtual Private Network.
[28] NSH Human Resources Office oral representations January 21, 2021.
[29] NSH Privacy Office oral representations January 22, 2021.
[30] *NSH Privacy Breach Protocol* at p. 3.
[31] The dates employees' access to electronic information systems was suspended was provided by NSH written representations December 7, 2020. The OIPC calculated the days from April 27, 2020, which is the date of the first confirmed audit report that contained the employees' unauthorized access related to the April 2020 tragedy.

[88] The OIPC confirmed that both Employees E and H went on to conduct additional privacy breaches after being flagged on an audit report and before their electronic information systems access was suspended. Employee E was flagged on an initial audit report generated on April 27, 2020, covering activity during the period of April 19 – 25, 2020, after accessing the electronic health records of an individual associated with the April 2020 tragedy on April 19, 2020. Additional audit reports show that 20 days later, Employee E accessed the records of another individual associated with the April 2020 tragedy four times on May 9, 2020, which was before network access was suspended.

[89] Employee H was first flagged on four different audit reports all generated on April 27, 2020, covering activity during the period of April 19 – 25, 2020. These audits showed:

- **April 20, 2020**: Employee H accessed one individual's electronic health records nine times and made two different attempts to look up another's electronic health records. Those attempts were unsuccessful because of incorrect name spelling and lack of records.
- **April 24, 2020**: Employee H accessed two others' electronic health records three times each.

[90] NSH Privacy Office's chronology of the response to Employee H's breaches, together with additional audit reports of activity after April 25, 2020, show the following:

- **April 27, 2020**: Employee H accessed the electronic health records of an individual associated with the April 2020 tragedy three times. Employee H used the phone number from that individual's electronic health records and performed a "phone number lookup" to identify other records associated with the phone number. This supplied Employee H with the identity of this individual's family members. Employee H then looked up the family members' electronic health records two times each.
- **May 8, 2020**: Follow-up from the initial audit report generated on April 27, 2020 was assigned to the privacy officer for the zone Employee H worked in.
- **May 11, 2020**: The zone privacy officer contacted the employee's manager and the Human Resources representative to "inform them of investigation into potential snooping breach and preliminary results" and a decision was made to audit the employee's activity for the prior six months.
- **May 12, 2020**: Employee H accessed the electronic health records of another high-profile person (unrelated to the April 2020 tragedy). Employee H took the phone number from that person's electronic health records and performed a "phone number lookup" to identify other records associated with the phone number. Employee H then accessed the electronic health records of two of that person's family members: one of them fourteen times and another seven times.
- **May 15, 2020**: The zone privacy officer met with Employee H's managers and Human Resources to discuss the audit reports of Employee H's activity in the prior six months. This initial review flagged an additional twelve suspicious access events.
- **May 20, 2020**: The Privacy Office recommended to Employee H's manager that access to electronic information systems be suspended.
- **May 22, 2020**: Employee H's electronic information systems access was suspended.

[91] When questioned about the month-long delay in suspending Employee H's access to the electronic information systems, NSH responded that all of those involved from the Human Resources Office, Privacy Office, and the employee's manager were new to their positions at the time and that questions about how best to initiate the suspension of access to electronic information systems in a privacy investigation remain.[32] The privacy representative stated that there remains some confusion about what everyone's role is and how to invoke the immediate suspension because it involves making a request to the IT Office which is not directly administered by NSH, but rather by the Province's Nova Scotia Digital Service.[33] The NSH privacy representative stated that one of the challenges is coordination between the manager, Human Resources Office and Privacy Office and that there are some differences across zones still lingering. The privacy representative said that "it is fair to say we were not well coordinated."[34]

[92] The *NSH Privacy Breach Protocol* clearly sets out who is responsible for initiating the immediate suspension of electronic information systems access pending an investigation of unauthorized access. It also identifies who is responsible for decision-making in the event there may be disagreement on appropriate containment, and for approving the non-suspension of the employee's access to electronic information systems containing personal health information if there is a clinical reason for maintaining system access.

[93] The *NSH Privacy Breach Protocol* is an important information practice that contains provisions to guide the containment of a privacy breach when it occurs. The suspension of an employee's access to the electronic information systems pending an investigation for unauthorized access is a critical containment strategy and is reasonable in the circumstances. Because it is in the nature of some employees to abuse their access, the custodian cannot expect that it will only happen once. Where NSH deviated from its protocol by failing to immediately suspend employee access to personal health information pending its investigations, its actions were not reasonable.

[94] **Finding #2:** I find that NSH failed to contain the privacy breaches by not suspending some employees' electronic information systems access once their unauthorized accesses were being investigated. This resulted in two employees continuing to view electronic health records without authority, which affected an additional seven individuals.

[95] **Recommendation #2:** I recommend that within three months of the date of this report, NSH implement training for all positions that have roles to play in responding to privacy breaches about their respective roles and responsibilities in the *NSH Privacy Breach Protocol*, specifically regarding the responsibility to immediately suspend access to electronic information systems pending investigation. This training should then be ongoing annually.

---

[32] NSH Privacy Office oral representations March 12, 2021.
[33] Nova Scotia Digital Service is a division under the Government of Nova Scotia's Department of Service Nova Scotia and Internal Services.
[34] NSH Privacy Office oral representations January 25, 2021.

Failure to audit all electronic information systems employees had access to

[96] Step 2 of the *NSH Privacy Breach Protocol* speaks to investigation and specifically mentions the need to conduct audits of electronic information systems, as required.

[97] The two electronic information systems audited by NSH were (1) the Meditech system, which is used as the main electronic health record in the Northern, Eastern and Western zones; and (2) the One Content system (formerly the Horizon Patient Folder system), which is used as the main electronic health record in the Central zone. However, these were not the only electronic information systems the employees had access to.

[98] Those responsible for containment of the privacy breaches did not obtain a list that showed what electronic information systems each employee had access to, as is called for in the *NSH Privacy Breach Protocol*. By not obtaining a list of all access available to the employees, NSH failed to identify other electronic information systems the employees had access to. As a result, the employees' access within other electronic information systems has never been audited.

[99] Some of the employees had access to the provincial Nova Scotia Drug Information System (DIS)[35] which is operated by the Department of Health and Wellness.[36] Only the Department of Health and Wellness can conduct audits of user activity within the DIS. When asked about notifying the Department of Health and Wellness to prompt auditing of the employees' access to DIS, the NSH Privacy Office stated that it did tell the privacy lead at the Department of Health and Wellness about the privacy breaches but could not recall if the names of the employees had been provided and no follow-up was done to confirm any audit results.[37]

[100] The DIS contains large amounts of sensitive personal health information about what medications have been prescribed and dispensed anywhere in the province by any prescriber. This information is distinct from the information stored in NSH's electronic information systems and is contributed to by custodians outside of NSH. As of the writing of this report, the OIPC could not confirm if the employees' access to the provincial DIS has been audited. Separate audits of this system are warranted to determine if these employees are responsible for privacy breaches within that system.

[101] The employees also had access to a wide range of other electronic information systems, some of which contain sensitive personal health information, including diagnostic imaging systems and laboratory information systems.[38] NSH did not definitively state what personal health information was contained in all the systems the employees had access to. NSH identified some systems that had limited or no capability to log user activity, and it identified others where

---

[35] NSH records show that Employees A, C, D and G were granted access to the Province of Nova Scotia's Drug Information System.
[36] The Nova Scotia Drug Information System (DIS) was reviewed in depth in *NS IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII).
[37] NSH Privacy Office oral representations March 12, 2021.
[38] A list of the access granted to each employee was submitted to the OIPC by NSH on September 30, 2020. Further detail about the nature of the access granted was provided in oral representations on January 18, 2021 and in written representations on March 3, 2021.

audit functionality was possible but not enabled.[39] When asked why these other systems were not audited, the NSH Privacy Office representative stated that they focused on the two systems they considered to be the highest risk (Meditech and One Content), because they contain the most comprehensive volume and type of personal health information.[40]

[102] Given the widespread snooping activity uncovered by some of its employees, it is warranted for NSH to audit all electronic information systems containing personal health information that the employees had access to.

[103] **Finding #3:** I find that NSH failed to follow its *NSH Privacy Breach Protocol* by not obtaining lists of all the electronic information systems the employees had access to and by not auditing the employees' access to all systems containing personal health information. As a result, there may be privacy breaches yet undiscovered.

[104] **Recommendation #3:** I recommend that within three months of the date of this report, NSH take the following actions to audit additional electronic information systems that the employees had access to:

a) Request that the Department of Health and Wellness conduct audits for a one-year period prior to the flagged privacy breaches of the employees who had access to the Drug Information System to determine if there are any additional privacy breaches by these employees.
b) Complete audits for a one-year period prior to the flagged privacy breaches of the employees' access to all as of yet unaudited NSH electronic information systems that have audit capability.

Step 2: Evaluate the risks

[105] The second step in appropriately managing a privacy breach is to evaluate the risks. The purpose of this step is to ensure that the custodian fully understands what took place and the extent of the identified risks to inform any further actions it may take. Evaluating the risks may lead to identifying additional containment steps or may point toward appropriate preventative strategies.

[106] To evaluate the risks, a custodian must consider the type, extent, and sensitivity of the personal information involved, the context of the privacy breach and what caused it, the individuals affected and the foreseeability of the harm.[41]

[39] NSH written representations received March 9, 2021. A complete analysis of NSH's auditing of user activity program is done under Issue 2.
[40] NSH Privacy Office oral representations on January 25, 2021.
[41] *NS OIPC Key Steps Document* at pp. 4-6.

Nature of the personal information involved

[107] The personal information involved is highly sensitive personal health information. The NSH audit reports show that the employees accessed varying degrees of personal health information, ranging from registration information (such as name, date of birth, health card number, appointment schedule and location, as well as reason for visit) to detailed and highly sensitive medical records generated in clinics or parts of NSH far outside the geographic location and subject matter of their work.

[108] Social relationships and engagement in social life is one of the main drivers of unauthorized access by authorized users. The OIPC has reported about this dynamic and its influence on employee behaviour before.[42] The group of employees responsible for the privacy breaches identified here demonstrates the wide range of personal relationships and curiosities that can inspire snooping behaviour. It seems that almost any kind of relationship can inspire a targeted lookup of health information. Each employee's unauthorized access was driven by a desire to look up a specific person's health records.

[109] Employees B, C and D looked up individuals they read about in the media and who were or who they thought were patients of theirs. However, it is the purpose of the lookup which determines if it is authorized or not. Even if there is or was a clinical relationship with an individual, if no care is being provided to the individual by the employee or there is no valid purpose associated with the employee fulfilling their job responsibilities, then access is not authorized. An employee who is curious about a former patient or is looking for some type of closure are acting for their own purposes, and therefore their access is not authorized under *PHIA*.

Cause and extent of the breaches

[110] The cause of these privacy breaches was employees accessing personal health information contained in NSH's electronic information systems without a valid purpose related to their work and in contravention of NSH policies and *PHIA*.

[111] The breaches were extensive in terms of the sensitivity of the information breached, the number of individuals affected and the time period over which some of the employees were able to access personal health information without a valid purpose.

[42] *NS IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII); and *NS IR18-02, Sobeys National Pharmacy Group (Re)*, 2018 NSOIPC 13 (CanLII).

[112] It might be possible to conclude that the employees caught snooping here were just a few bad apples among thousands of good employees. However, it is critical to recognize some common themes that can be seen in the reasons provided by some of the employees for their unauthorized access.

- Employee A mentioned that their family member was in the area of the tragic events that took place in April 2020 and they were scared their family member could have been a victim.
- Employee B mentioned a previous conversation with a paramedic about an individual they had treated and thought that person could be one of the individuals associated with the April 2020 tragedy. Employee B then looked up that person's information to see if it was the same person (which it was not).
- Employee C mentioned that one of the individuals associated with the April 2020 tragedy was a former patient and looked up that patient to see how their health was at the time of death.
- Employee D mentioned thinking that one of the individuals associated with the April 2020 tragedy might be a former patient and looked up that person's information to determine if it was (which it was not).
- Employee G mentioned that everyone was curious and talking about one of the individuals associated with the April 2020 tragedy that day, but Employee G was the one "that bit the bullet" and looked them up.

[113] The common themes here point to risks in NSH's workplace culture that allow employees to believe they are using their access for benign or understandable reasons. The reasons given by these employees demonstrate a culture that blurs the lines between what employees technically have access to and what they are authorized to access.

[114] NSH did not follow up when Employee B mentioned the conversation with the paramedic. In Employee B's statements to the OIPC, it was clarified that in addition to inspiring Employee B to look up the information about one of the individuals associated with the April 2020 tragedy, the paramedic also shared disturbing personal health information about the individual with Employee B. Then, at the request of the paramedic, Employee B looked up the individual they were discussing and gave the paramedic information about their status. This was done after the paramedic's clinical relationship with the patient had already ended and there was no need to know. The impact of workplace gossip and employees' desire to know what happened to former patients is evident in its influence on how employees use their access to electronic health records. These features of the workplace culture create risks for personal health information in NSH's custody or control.

Individuals affected by the breaches

[115] NSH records show that collectively, the eight employees investigated here breached the privacy of 270 individuals over 1200 times spanning several years.

Employee	Number of identified privacy breaches
A	3 patients accessed multiple times between August 2019 and April 21, 2020
B	1 patient accessed 8 times on April 20, 2020
C	1 patient accessed 25 times on April 22, 2020
D	1 patient accessed 21 times on May 1, 2020
E	4 patients accessed 26 times between December 5, 2018 and May 9, 2020
F	146 patients accessed 612 times between October 1, 2017 and June 8, 2020
G	13 patients accessed between July 2019 and April 2020
H	101 patients accessed 525 times between June 1, 2018 and May 22, 2020

Foreseeable harm from the breaches

[116] Reported cases from across the country[43] demonstrate that personal health information is highly susceptible to authorized users intentionally using their workplace access for unauthorized purposes.

[117] The harms from intentional abuse of access by employees are foreseeable. The harms range from emotional harm to other harms that might come from the employee acting based on the information or disclosing the information to others, including the harm of worry or anxiety about who else the information may have been shared with.

[118] The main harms that result from this type of privacy breach flow from the fact that the affected individual is personally targeted by the employee for their own purposes. This may cause emotional harms of feeling violated, hurt or humiliated. Other harms may also follow, depending on how the information is used, and could include damage to reputation, relationships, or employment and social and relational harm. For example, the risk of the disclosure of an individual's prescription history or medical conditions could impact on reputation and self-esteem and if disclosed, could lead to bullying or other forms of social stigma.

[119] Individuals who learn that someone in the healthcare system has abused their access to health records for the purpose of looking up medical information about them without a valid

---

[43] *AB 2013-IR-02, Report 2013-IR-02 (Re)*, 2013 CanLII 82405 (AB OIPC); *AB Order H2016-06, Alberta Health Services (Re)*, 2016 CanLII 104927 (AB OIPC); *AB Order H2014-02, Alberta Health Services (Re)*, 2014 CanLII 41751 (AB OIPC); *NL Report PH-2016-001, Eastern Health (Re)*, 2016 CanLII 85236 (NL IPC); *ON PHIPA Decision 64, A Public Hospital (Re)*, 2017 CanLII 88475 (ON IPC); *ON PHIPA Decision 44, London Health Sciences Centre (Re)*, 2017 CanLII 31432 (ON IPC); *ON PHIPA Decision 62, Group Health Centre (Re)*, 2017 CanLII 87957 (ON IPC); *SK IR 142-2015, Heartland Regional Health Authority (Re)*, 2015 CanLII 85349 (SK IPC); *SK IR H-2013-001, Regina Qu'Appelle Regional Health Authority (Re),* 2013 CanLII 5640 (SK IPC); and *SK IR H-2010-001, L & M Pharmacy Inc. (Re)*, 2010 CanLII 17914 (SK IPC). This represents a sample of the total reported cases.

purpose often feel a strong emotional response. There is a deep sense of violation that comes from learning that you have been targeted in this way.

[120] Once privacy related to personal health information has been violated, it is near impossible to restore it and avoid the harm from the information being accessed in the first place. This is the nature of personal health information. Credit protection services are a common harm mitigation strategy employed in situations where financial information has been breached. However, there is no equivalent mitigation strategy for personal health information. Affected individuals cannot subscribe to a protection service to mitigate rumours, whispers, stares, or other social harms, especially if it is not known for certain what information was shared with whom. It is virtually impossible to undo the harm and sense of violation individuals feel when the intimate details of their personal health information have been breached.

[121] One affected individual explained to the OIPC that learning about the breach caused a cascade of reliving a traumatic event that the employee had looked up records about. The traumatic event was so serious that the individual themself had never read the medical reports about it. However, upon learning about the unauthorized access, the affected individual obtained the records that had been looked at by the employee to understand the full extent of the privacy breach. In doing so, the individual was confronted with detailed medical reports about the traumatic incident for the first time. This individual was shocked and appalled that the details of an incident that almost no person would ever have the need or authority to look up, were readily available to the employee without any controls. For this individual, the knowledge that the employee, an acquaintance through their children, knew more detail about the traumatic event than they did, was very upsetting. It also caused significant anxiety and worry about who the employee shared the information with. Other affected individuals similarly had concerns about who the employee that looked at their information had shared the information with.

[122] All the employees investigated here denied sharing any information they looked up with anyone. Despite the implausibility that none of these employees shared any of the information they looked up with anyone,[44] identifying the actual existence and extent of any disclosure can be challenging. NSH acted to further investigate by looking for emails sent from employee email accounts to determine if the employees had shared information in that way and found none.

[123] The *NSH Privacy Breach Protocol* suggests obtaining notarized affidavits that explain the purpose, use and disclosure of accessed information from employees found to have abused their access. Affidavits are a straightforward tool for minimizing the residual risk that the employee shared information because it requires the employee to swear an oath in front of a commissioner of oaths which has consequences if the employee is not truthful. It also provides an additional assurance to affected individuals that can help alleviate their worry and anxiety and thereby work to mitigate harm.

---

[44] Especially with Employee A, who gave as one of the reasons for looking up the information that a neighbour (the mother) was looking for information about her adult son; and also with Employee G who admitted to biting the bullet and looking up information about an individual associated with the April 2020 tragedy when several staff were curious.

[124] **Finding #4:** I find that the harm from these privacy breaches is significant and was foreseeable.

[125] **Recommendation #4:** I recommend that within three months of the date of this report, NSH implement training for all positions that have roles to play in responding to privacy breaches as set out in the *NSH Privacy Breach Protocol*, specifically regarding their role to obtain signed and notarized affidavits from employees found to have abused their access to electronic information systems. This training should then be ongoing annually.

Step 3: Notification

[126] 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 an affected individual at the first reasonable opportunity if the custodian believes on a reasonable basis that, because of the breach, there is potential for harm or embarrassment to the individual.

[127] Notification conveys respect to the affected individuals and allows them to take steps to mitigate any potential harm. Former Nova Scotia Information and Privacy Commissioner Tully said, "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."[45]

[128] My concerns with the notification are three-fold: timing; accuracy and sufficiency of information provided; and employee interference with notification.

Timing

[129] *PHIA* requires notification at the "first reasonable opportunity" but that is the extent of its instruction in terms of timing. Guidelines and laws tend to be imprecise about time limits on notification because various circumstances must be accounted for. In that light, the reasonableness of the timing can be measured by whether it is objectively diligent and prudent in the circumstances.[46]

[130] NSH identified the first privacy breaches when it generated audits on April 27, 2020. Other privacy breaches were identified during the weeks that followed. NSH sent the majority of notifications from these eight investigations by August 2020. However, two groups of notifications were significantly delayed.

[131] The notifications to two individuals in relation to Employee A's privacy breaches were not sent in a timely manner. NSH appears to have overlooked the final steps in the breach management process with regard to Employee A. NSH did not complete its standard privacy breach report as it did for the others. In following up to answer the OIPC question as to why there was no privacy breach report for the investigation of that employee, NSH discovered that it

---

[45] *NS IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII) at para. 145.
[46] *NS IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII), at para. 133.

had also unintentionally not sent the notification letters to the affected individuals. The notifications were sent November 27, 2020.

[132] The notifications to 12 individuals in relation to Employee G's privacy breaches were delayed because NSH couldn't decide if the access was authorized or not. Employee G never admitted to any unauthorized access in relation to these 12 individuals. The privacy breaches were identified by a process of eliminating from the audit reports all access that NSH could determine was reasonable for the employee's position. Following this there remained 12 individuals whose information had been accessed by Employee G but who had no connection to the clinic where Employee G worked and there was no known valid reason for the access. NSH eventually notified those individuals after December 7, 2020.[47]

[133] In these cases, the notification was not done at the first reasonable opportunity. It is not clear if notification would have been provided in these cases had the OIPC not followed up with this investigation.

[134] **Finding #5:** I find that the notification provided to individuals affected by the privacy breaches by Employees A and G were not done at the first reasonable opportunity, but that notification has now been provided.

Accuracy and sufficiency of information provided in the notification

[135] NSH notified affected individuals in letters sent by mail using a template signed by the zone privacy officer assigned to the zone where the employee who caused the breaches worked. The template letter informed the recipient that a privacy breach was discovered as a result of regular audits and follow-up investigation. The template letter confirmed that an employee accessed their personal health information contained within the scheduling module, but the letter did not name the employee. The letter stated that the employee "did, within this system on one or multiple occasions, enter your name and did view the following information without an authorized reason:

- Medical Record Number (MRN)
- Name
- Birthdate
- Sex (Gender)
- Mother's Name
- Last Visit Date
- Address
- Phone number
- Age in Years
- Health Card Number
- Other Name (Nickname/Maiden name, etc)
- Other Numbers (Other NSHA Site MRNs)
- The date, type of visit, account number, location, provider and discharge date of the last three registrations."

[47] NSH Privacy Office oral representations January 25, 2021.

[136] The next paragraph added additional statements "for clarity" including, "This shows you the type of demographic information that would have been viewed by the employee."

[137] If the employee also viewed the individual's detailed electronic health records, an additional statement was added that said, "In the case of EMR access, the information varies depending on what type of account was accessed." There was also an additional bullet on the bullet list that stated:

- EMR Access – may have viewed specific visit information (details available upon request)

[138] The template letter also contained the statement, "While we do not have reason to believe that the information viewed by the employee was shared with anyone else, we cannot rule out that possibility." The template letter also included a general statement that NSH had taken steps to address the situation with the employee. The letter gave a phone number to contact and an encouraging invitation statement that said, "I am able to give you more information, such as a list of the specific visits that would have been affected by this privacy breach and can help you decide how best to protect yourself in this circumstance."

[139] Prince Edward Island's (PEI) Information and Privacy Commissioner described the contents of notification letters in a similar situation of serial snooping. In that case, the Commissioner accepted that a letter containing the following information constituted reasonable notification:

- The number of times the patient's personal health information was accessed by the employee, and the date of the most recent access;
- The type of personal health information which was accessed by the employee;
- That the access to their personal health information by the employee was in violation of Health PEI policy;
- That the Information and Privacy Commissioner had been notified; and
- A toll-free phone number to contact Health PEI with any questions or concerns. [48]

[140] In that case, the custodian did not initially give the affected individuals the name of the employee in their notification letters. However, the PEI Commissioner noted that patients have an enhanced need to know the identity of a snooper to mitigate any potential malicious intentions. She recommended that in future, the custodian reference the existence of audit logs in the notification letters and enclose at least an excerpt of those logs to highlight the access reflecting the breach and the name of the employee.[49]

[141] NSH did provide a phone number for affected individuals to call and gave substantially more information to those who followed up. They were told the identity of the employee who breached their privacy and whether that person was actively employed by NSH at the time of the

---

[48] *Prince Edward Island (Health) (Re)*, 2018 CanLII 130517 (PE IPC), at para. 69.
[49] *Prince Edward Island (Health) (Re)*, 2018 CanLII 130517 (PE IPC), at paras. 68-74.

notification. If the affected individual filled out an additional form, they were given a copy of the actual records that the employee accessed so that they could know what the employee viewed. If the affected individual did not contact NSH as recommended in the letter, they did not receive this additional information.

[142] While NSH's notification letters contained many important pieces of information, there is room for improvement. NSH's letter could have been more specific and precise in its notification, particularly where the employee viewed detailed electronic health records. The letter possibly obscured the nature and severity of the breaches because it did not name the employee. Sometimes custodians worry about causing additional privacy breaches by naming employees in letters to affected individuals in case letters are sent to the wrong individual or are intercepted. While I think that possibility is fairly remote, if that is a real concern for custodians, they need to ensure that information is supplied in some way to the affected individual. This task should not be delegated to an affected individual to call the custodian. Rather, the custodian must take the onus of informing the affected individual, either in written format or verbally. Furthermore, the NSH letter only stated the employee accessed the information "one or multiple" times. Specific information such as the number of times the employee accessed the patient's information as well as a definitive statement about what was accessed would be more helpful. The letter also glossed over the distinction between information looked up in the scheduling module and detailed medical information looked up in the electronic health records. Finally, the letter did not define the acronym it used (EMR) which stands for Electronic Medical Record (containing the most detailed and substantive personal health information) and it listed this type of information as a bullet along with the information viewed within the scheduling module.

[143] **Finding #6:** I find that the information NSH provided in the notification letters was too generic and not detailed enough for the affected individuals to grasp the extent or severity of the privacy breaches.

[144] **Recommendation #5:** I recommend that NSH ensure its future privacy breach notifications in cases of intentional unauthorized access by an employee are sufficiently personalized and specific to the matter. This includes ensuring that:

- all terms used are defined (e.g., any acronyms or jargon);
- notifications identify the name of the employee who engaged in the unauthorized access;
- notifications accurately describe the type of information accessed by the named employee;
- notifications give affected individuals specific information about what components of their personal health information were accessed and the number of times it was accessed by the named employee;
- notifications clearly identify if the affected individual was looked up and/or targeted by name;
- notifications provide context for the breaches and avoid the use of generic statements that may or may not apply to the affected individuals.

Employee interference with notification

[145] One affected individual gave detailed statements to the OIPC and NSH about being contacted by Employee H just before the NSH notification letter arrived. The affected individual described that Employee H phoned to say a letter would soon arrive from NSH, but that it was nothing to worry about. The explanation Employee H provided to the affected individual was that the access was only to look up phone numbers. The affected individual described how Employee H minimized the significance of the matter, encouraged the affected individual not to pay any attention when the NSH letter arrived and made the affected individual feel sympathy because Employee H's employment had been terminated.

[146] The affected individual received the letter from NSH soon after the phone call from Employee H. That individual told the OIPC that when they received the NSH letter, they nearly dismissed the issue because there weren't a lot of details or specifics in the letter and the letter made it sound minor or routine. However, they eventually followed up with NSH to obtain copies of the information that was accessed by Employee H. The affected individual was shocked to learn the extent of Employee H's access targeting them and their family members. Their sense of violation was deepened by having been contacted by Employee H and Employee H's effort to draw attention away from the privacy breaches.

[147] On August 25, 2021, I expressed my concern with regard to containment and suggested that NSH contact Employee H and direct them to cease contacting affected individuals. NSH responded that it had also received reports of the behaviour and had already responded. NSH asked the union representative to remind Employee H of the continued responsibility for confidentiality and that all available steps would be taken to protect confidential information and prevent further breaches.

[148] After contacting the union, NSH did no further follow-up on the matter. NSH does not know if the union delivered its message to Employee H, nor does it know the content of the message if one was delivered. NSH does not know which other affected individuals Employee H contacted, nor whether that contact had any impact on the affected individuals' understanding of the matter or their receipt of NSH's notification. NSH's responsibility to affected individuals to contain the privacy breaches and to mitigate and protect them from further harm exists independently of and extends beyond the employment relationship with Employee H.

[149] When an employee who is responsible for a privacy breach contacts affected individuals who are about to receive notification of the privacy breach, this should be considered as a continuation of the privacy breach, because the employee uses their knowledge from the original privacy breach to know who to contact. This type of conduct poses a continued risk to the custodian's containment and notification efforts. The further targeting of affected individuals is insidious behaviour by the snooper designed to protect themselves from accountability for their actions. Not only is this a nuisance and further targeting of the affected individuals, but it may also have the effect of interfering with the custodian's notification and with the affected

individuals' rights to redress or to take steps to mitigate harm from the privacy breach. This type of reaction by an employee caught breaching privacy is not unprecedented.[50]

[150] Interrupting a long-term serial snooper carries some additional risks related to how the snooper will respond. The risk of further privacy breaches by an employee on their way out the door is very real. A custodian has the responsibility to contain the privacy breaches and protect affected individuals from this type of further intrusion.

Step 4: Prevention

[151] The final step in managing a privacy breach required by the *NS OIPC Key Steps Document* is to work to prevent a future occurrence. The *Personal Health Information Regulations* also require custodians to keep a record of all corrective actions they take to reduce the likelihood of future breaches.[51]

[152] In order to prevent a similar future privacy breach, it is essential for the custodian to understand the root causes of the breach and to evaluate the factors that contributed to it occurring. This is typically done by way of the custodian conducting a comprehensive, reflective post-breach review and then developing a prevention strategy that sets out concrete responsive actions.[52] The prevention strategy developed should address privacy controls in the following four areas:

1. Physical controls
2. Technical controls
3. Administrative controls
4. Personnel controls

[153] The *NSH Privacy Breach Protocol* includes the following prevention requirement:

> Once steps have been taken to mitigate the risks associated with the privacy breach and to provide appropriate notification, the Office of Primary Responsibility (the Office where the breach occurred), the Privacy Officer and the Incident Response Team (if activated) must investigate the cause of the breach thoroughly, consider whether to develop a prevention plan, and consider what the plan might include. This could require a security audit of both physical and technical security. As a result of this evaluation, develop or improve as necessary adequate long-term safeguards against future breaches.[53]

[154] NSH took steps to contain and investigate the many privacy breaches at issue in this report. However, it is less clear whether NSH has plans for conducting a post-breach review and/or developing a prevention strategy to avoid similar occurrences in the future. Over the course of this investigation, NSH sent several updates on plans it had to ameliorate its privacy

---

[50] *NS IR18-01, Department of Health and Wellness (Re),* 2018 NSOIPC 12 (CanLII); and *NS IR18-02, Sobeys National Pharmacy Group (Re),* 2018 NSOIPC 13 (CanLII).
[51] Section 10(4), *Personal Health Information Regulations*, NS Reg 217/2012.
[52] *NS IR19-01, Department of Internal Services (Re),* 2019 NSOIPC 2 (CanLII) at para. 155.
[53] *NSH Privacy Breach Protocol*, at Step 5: Mitigation of Risks and Prevention.

breach prevention practices, but it did not inform the OIPC of any plans for a post-breach review and/or prevention plan. It may have been that NSH was waiting on this report before engaging in any such exercise. Whatever the reason, it is critical that an internal post-breach review be undertaken.

[155] **Finding #7:** I find that NSH has not implemented a comprehensive, methodical plan to prevent similar privacy breaches from occurring in the future.

[156] **Recommendation #6:** I recommend that within one year of the date of this report, NSH complete a post-breach review of these privacy breaches and develop a comprehensive prevention plan that:

- addresses physical, technical, administrative and personnel controls;
- addresses the concerns raised and recommendations made in this report;
- requires all NSH employees who were involved in responding to these privacy breaches to read this report.

4.2 Issue #2: Did NSH have reasonable security and information practices in place for its electronic information systems in compliance with ss. 61, 62 and 65 of *PHIA*?

[157] Sections 61, 62 and 65 of *PHIA* set out the security standards expected of custodians. *PHIA* requires that custodians protect the confidentiality of personal health information and that they do so by implementing information practices[54] (such as policies) that are reasonable in the circumstances. 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 *Personal Health Information Regulations*, such as implementing safeguards that ensure only those authorized to access electronic information systems have access.[55]

Reasonable security

[158] The meaning of "reasonable security" in Nova Scotia's privacy laws has been canvassed by this office on several occasions.[56] Below are 12 factors commonly considered when

---

[54] Information practices are defined in s. 3 of *PHIA* as:
"information practices", in relation to a custodian or a prescribed entity, means the policies of the custodian or a prescribed entity for actions in relation to personal health information, including
(i) when, how and the purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information, and
(ii) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[55] *Personal Health Information Regulations*, NS Reg 217/2012, at s. 10.

[56] *NS Report IR17-01, Cape Breton-Victoria Regional School Board (Re)*, 2017 NSOIPC 9 (CanLII); and *NS Report IR16-02, Nova Scotia Health Authority and Private Practice Physicians (Re)*, 2016 NSOIPC 16 (CanLII) for example. In both reports, former Commissioner Tully noted that the summary of considerations supplied above are consistent with every other jurisdiction in Canada. The issue was further canvassed in *NS Report IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII), *NS Report IR18-02, Sobeys National Pharmacy Group (Re)*, 2018 NSOIPC 13 (CanLII), *NS Report IR19-01, Department of Internal Services (Re)*, 2019 NSOIPC 2 (CanLII); and *NS Review Report 20-02, Nova Scotia Health Authority (Re)*, 2020 NSOIPC 2 (CanLII).

evaluating the reasonableness of a custodian's security. These considerations overlay 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.[57]
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.[58]
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.[59]
5. **Trust:** For public sector custodians such as NSH, reasonable security also includes reasonable assurances to the public that the custodian is taking privacy protections seriously. Where custodians hold personal information, the public has an increased level of trust that their personal information is being protected. This creates a high standard for custodians 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.[60]
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 custodian to ensure against a minute risk at great cost. A custodian cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable security in another.[61]
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.

---

[57] *BC Report F10-02, Electronic Health System (Re)*, 2010 BCIPC 13 (CanLII) at para. 130.
[58] *BC Report F10-02, Electronic Health System (Re)*, 2010 BCIPC 13 (CanLII) at para. 129.
[59] *BC IR F06-01, Sale of Provincial Government Computer Tapes Containing Personal Information, Re*, 2006 CanLII 13536 (BC IPC); *Canada OPC, Report of an Investigation into the Security, Collection and Retention of Personal Information*, 2007 CanLII 41283 (PCC); (2005), online <https://oipc.ab.ca/wp-content/uploads/2022/01/H2005-IR-01.pdf>.
[60] *ON Report MC09-9, Niagara (Regional Municipality) (Re)*, 2010 CanLII 61927 (ON IPC); *BC IR F06-01, Sale of Provincial Government Computer Tapes Containing Personal Information, Re*, 2006 CanLII 13536 (BC IPC).
[61] *BC IR F06-01, Sale of Provincial Government Computer Tapes Containing Personal Information, Re*, 2006 CanLII 13536 (BC IPC).

10. **Timing:** Reasonableness requires a proactive and speedy response to known or likely risks.[62] Time is of the essence in any privacy breach. The safeguards must ensure that should a privacy breach occur, the custodian and the affected individual will learn of the breach and have response measures in place quickly and efficiently.[63]
11. **Documentation:** Procedures for establishing reasonable security must be documented, and custodians must be prepared to respond to the idea that employees won't always follow the documented procedures.[64]
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.[65]

Securing personal health information against employee abuse of access

Access to electronic information systems

[159] NSH's electronic information systems contain a wealth of personal health information. Not all employees should have access to all health information stored in these systems. Rather, there should be practices, policies and procedures in place that limit access. Once that is done, there needs to be continuous action on the part of the custodian to ensure proper employee training. Finally, the custodian should have practices in place for auditing electronic information system access to catch abuse that may happen despite the implementation of policies and training.

Role-based access practices

[160] The foundational factor to consider when assessing whether NSH had reasonable security measures in place is the process for how access is granted to the electronic information systems. Who decides which employees get access to which systems and what their role-based access should be? Appropriate and effective access controls, which include technical measures to restrict user access, are a key safeguard for preventing employee snooping.

---

[62] *BC IR F06-01, Sale of Provincial Government Computer Tapes Containing Personal Information, Re*, 2006 CanLII 13536 (BC IPC); *AB Order P2013-04, TD Insurance (Re), 2013 CanLII 69088 (AB OIPC); BC IR F12-02, University of Victoria (Re)*, 2012 BCIPC 7 (CanLII).
[63] *AB IR H2005-IR-001, Report on Investigation into Missing Computer Tape Containing Health Information*, (2005), online: <https://oipc.ab.ca/wp-content/uploads/2022/01/H2005-IR-01.pdf>.
[64] *AB IR H2005-IR-001, Report on Investigation into Missing Computer Tape Containing Health Information* (2005), online <https://oipc.ab.ca/wp-content/uploads/2022/01/H2005-IR-01.pdf>; *ON IPC PHIPA Order HO-001*; *BC IR F06-01, Sale of Provincial Government Computer Tapes Containing Personal Information, Re*, 2006 CanLII 13536 (BC IPC); *AB Order P2010-008, Staples Canada Inc. (Re)*, 2011 CanLII 96635 (AB OIPC).
[65] *AB Report 2013-IR-02 (Re), 2013-IR-02*, 2013 CanLII 82405(AB OIPC); *Order H2016-06, Alberta Health Services (Re)*, 2016 CanLII 104927 (AB OIPC); *Order H2014-02, Alberta Health Services (Re)*, 2014 CanLII 41751 (AB OIPC); *NL Report PH-2016-001, Eastern Health (Re)*, 2016 CanLII 85236; *ON PHIPA Decision 64, A Public Hospital (Re)*, 2017 CanLII 88475 (ON IPC); *ON PHIPA Decision 44, London Health Sciences Centre (Re)*, 2017 CanLII 31432 (ONIPC); *ON PHIPA Decision 62, Group Health Centre (Re)*, 2017 CanLII 87957 (ON IPC); *SK IR 142-2015, Heartland Regional Health Authority (Re)*, 2015 CanLII 85349 (SK IPC); *SK IR H-2013-001, Regina Qu'Appelle Regional Health Authority (Re)*, 2013 CanLII 5640 (SK IPC); *SK IR H-2010-001, L&M Pharmacy Inc. (Re)*, 2010 CanLII 17914 (SK IPC).

[161] Role-based access ensures employees have access only to the information they need to do their jobs. In a role-based access control model, access privileges to electronic information systems are restricted based on what personal health information is needed to fulfill the functions of a given role. Employees (users) are then granted access privileges associated with their role.

[162] Role-based access controls are the industry standard for limiting employee access to personal health information stored within electronic information systems.[66] They are also a requirement under *PHIA*. In 2010, then Minister of Health Maureen MacDonald spoke about the legislators' intent regarding *PHIA*:

> The bill requires role-based access to personal health information, which means that you only have access to information you need to do your job. This will support appropriate user access in electronic health records, while protecting the patient's privacy. [67]

[163] When considering standards for role-based access, Information and Privacy Commissioners have supported the following:

- Limits on employee access to electronic information systems should be well defined and based on their job description/role.[68]
- Job titles or professional designations are not necessarily determinative of the actual health services the user provides or supports.[69]
- Roles should be as specific and granular as possible, incorporating both the principle of least privilege[70] and the need-to-know principle. Roles cannot be defined so broadly that these principles are violated.[71]
- Roles must be documented, updated regularly, and should be assigned by a central authority with program and privacy expertise to ensure objectivity and consistency.[72]

---

[66] *BC Report F10-02, Electronic Health System (Re),* 2010 BCIPC 13 (CanLII), at para. 72*; NWT Report 19-HIA13, Northwest Territories Health and Social Services Authority (Re)*, 2019 NTIPC 9 (CanLII); Canada Health Infoway, *Privacy & Security Requirements and Considerations for Digital Health Solutions V2.0* (2014), online: <https://www.infoway-inforoute.ca/en/component/edocman/2154-privacy-and-security-requirements-and-considerations-for-digital-health-solutions/view-document?Itemid=0 > at p. 71; AB OIPC, BC OIPC and Office of the Privacy Commissioner of Canada (OPC), *Getting Accountability Right with a Privacy Management Program* (April 2012) at p. 11, online: OPC <https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf>.

[67] Maureen MacDonald, Hansard 10-46 (November 18, 2010), online: Nova Scotia Legislature <https://nslegislature.ca/legislative-business/hansard-debates/assembly-61-session-2/house_10nov18> at p. 3642.

[68] *MB Ombuds Case 2014-0500,* (2017), online: <https://www.ombudsman.mb.ca/uploads/document/files/case-2014-0500-en.pdf> at p.12; OPC, *Ten Tips for Addressing Employee Snooping* (March 2016), online: OPC <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/02_05_d_65_tips/> at pt. 4.

[69] *BC Report F10-02, Electronic Health System (Re),* 2010 BCIPC 13 (CanLII), at para. 76.

[70] The principle of least privilege is a security principle that requires users be granted "the most restrictive set of privileges (or lowest clearance)" possible that will still permit them to carry out authorized duties. Government of British Columbia, *Information Security Glossary* (undated), online: Government of British Columbia <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary?keyword=least&keyword=privilege#L>; *British Columbia Health Authority Privacy Breach Management (Re)*, 2015 BCIPC 66 (CanLII).

[71] *BC Report F10-02, Electronic Health System (Re),* 2010 BCIPC 13 (CanLII), at para. 75.

[72] *NFLD Report PH-2013-001, Western Regional Health Authority (Re),* 2013 CanLII 52470 (NL IPC), at para. 78. *BC Report F10-02, Electronic Health System (Re),* 2010 BCIPC 13 (CanLII), at paras. 88-90.

[164] The Manitoba Ombudsman described the preferred approach to determining and documenting access permissions in a role-based access control model as follows:

> The preferred approach is to carefully assess [access permissions] at an organizational level, job function by job function, in order to determine which employees truly need access to personal health information, the extent of that access (field by field), and the nature of the access (read-only, read-write). The end result should be an organization-wide role-based access matrix. The matrix should identify data fields, roles and functions, the nature of the access, and the reasons why access is necessary, role by role.[73]

[165] As PEI's Information and Privacy Commissioner noted in a report involving employee snooping at Health PEI:

> Although the policies against accessing electronic databases for anything other than work purposes are clear, and although there are penalties for unauthorized access, a small percentage of individuals will snoop anyway. For this reason, it is important to limit the access that employees may have to only what they need to carry out their duties of employment.[74]

[166] Technical access controls that proactively limit what employees can view are necessary because administrative policies and penalties are not always sufficient on their own.

[167] For the purposes of this investigation, the OIPC reviewed NSH's access control practices as they existed at the time of the privacy breaches. Interviews with privacy and IT personnel were conducted and supporting documentation was reviewed, including role-based access matrices for NSH's One Content and Meditech electronic information systems which were submitted to OIPC as undated, electronic spreadsheet documents.

[168] The major concern in this investigation was not that NSH did not have a role-based access matrix or that the employees had been assigned the wrong user profile within it. Rather, it was that despite this, users were able to access detailed electronic health records of patients to whom they were not providing care. NSH submitted that its ability to manage access controls is specific to each application or electronic information system, because each one has its own unique access controls and permissions. The ability of an electronic information system to ensure only those authorized to access the information it contains is a functional feature of the system which I will discuss in the heading below.

[169] There are two areas where NSH could improve its role-based access practices: administrator level permissions should be restricted to IT personnel; assignment of and updates to user roles should be more rigorous.

---

[73] *MB Ombuds Case 2014-0500,* (2017), online: <https://www.ombudsman.mb.ca/uploads/document/files/case-2014-0500-en.pdf> at p. 12.
[74] *PEI Report HI-18-005, Prince Edward Island (Health) (Re)*, 2018 CanLII 130517 (PE IPC), at para. 45.

Administrator level permissions should be restricted to IT personnel

[170] Four of the eight employees whose conduct was reviewed in this investigation had administrator level permissions for their computers. Administrator level permissions allow the user to make changes to default settings, configurations and software. It is uncommon for end users within a large organization to have this type of permission, unless they are employed by the organization's IT department, because this type of permission can be exploited to install malware or other malicious software. Typically, administrator level permissions are restricted to IT personnel.

Assignment of and updates to user roles should be more rigorous

[171] When asked about the parameters for approving requests for electronic information systems access, the NSH IT Office explained that the approval process for granting access is done by each employee's supervisor. The IT Office said that it is up to each supervisor to request access for an employee from the menu of possible access options set out in the NSH access matrices.[75] The IT Office confirmed that there is no central process for managing or vetting the access granted to employees and that there are no default profiles for any NSH positions. It said that supervisors know what their employees need to access, and they manage the approvals for access on an ad hoc basis.[76]

[172] In addition, NSH explained that users' access to electronic information systems may not be consistently getting updated when an employee changes roles within NSH. This is because when an employee changes roles, the new supervisor must request any new required access and the former supervisor must request the termination of the old access. This is not something that happens automatically, it depends on the diligence of both the new and former supervisors.

[173] There is no process to verify that updates are made when employees change roles in every case. NSH's representative could not say how often this occurs but noted that it does regularly result in situations where employees' current department membership within the system is out of date.[77]

[174] In 2010, the British Columbia Information and Privacy Commissioner (BC Commissioner) conducted a review of Vancouver Coastal Health Authority's primary access regional information system (PARIS). In that review, the BC Commissioner recommended that access privileges not be assigned on an ad hoc basis but rather should be granted by a central body that includes privacy and program expertise.[78] The BC Commissioner said that this central body should make decisions based on recommendations from senior managers who have knowledge about the tasks and services provided by each of their staff and based on workflows. The central body should also have senior privacy expertise membership including the chief privacy officer and the chief information officer.

---

[75] NSH Information Technology oral representations January 18, 2021.
[76] NSH Information Technology oral representations January 18, 2021.
[77] NSH Privacy Office oral representations March 12, 2021.
[78] *BC Report F10-02, Electronic Health System (Re)*, 2010 BCIPC 13 (CanLII), at paras. 88-90.

[175] NSH's approach to approving electronic information systems access is too informal. It is important to remember that when a user is granted access, they are typically granted access to a huge amount of information with very few limitations. The amount of access that gets granted at the outset is an important front-end decision that has significant ramifications for the remainder of the user's employment.

[176] Additionally, the practice of not regularly reviewing access granted to ensure it is consistent with an employee's current job is concerning. By regularly reviewing and revising role-based access controls, a custodian can ensure that access permissions are up-to-date and acting as a reasonable, effective safeguard against employee snooping. When that is not done, access permissions can be too broad and give unnecessary access to users.

[177] **Finding #8:** I find that NSH's current practice for approving and updating user access to electronic information systems does not provide reasonable security for personal health information stored in its electronic information systems.

[178] **Recommendation #7:** I recommend that within nine months of the date of this report, NSH implement a user access request and approval process (or policy) for its electronic information systems. The process or policy must correspond to an established criteria and to standard user profiles. It must also set out verification and validation practices for every new user's access, and for when an existing employee changes roles.

Electronic information system functionality

Limiting access to detailed information based on clinical relationship

[179] Section 10(1)(b) of the *Personal Health Information Regulations* requires a custodian to have additional safeguards for personal health information held in electronic information systems to ensure only those authorized to access the system have access.

[180] The way that the users in this case accessed the electronic information systems in a fashion prohibited by *PHIA* was that they abused their access and looked at information of patients they were not treating. They did not need to know this information for work purposes. The question becomes, is there a way to limit users' access to records of patients they are treating, in accordance with the need-to-know principle so that employees do not have access to the electronic health records of patients they do not have a clinical relationship with?

[181] In both the One Content and the Meditech systems, users can look up any patient by name and the system will return records for that patient according to the record type permissions granted to the user. This open-ended search function is a powerful tool that allows a user to search for a patient by name. That search will give the user access to all record types the user was granted access to in the role-based access matrix, regardless of whether the user is involved in that patient's care, and regardless of whether the patient has any connection to the employee's work or workplace at all.

[182] NSH maintained that this type of open-ended search function is necessary because the electronic information systems do not have the capability to tailor the search function to patient types or patients who are being seen by the clinical area where the user works. NSH said that users need to be able to broadly look up any patient, so that when a new patient comes to their area, the patient can be found in the system.[79]

[183] The problem here though is that while an ability to search by name to find a patient may be necessary, it is not also necessary that the user can then also see all the detailed record types that user was granted access to in the role-based access matrix if the user is not actively providing care to the individual. If there are means to include a functionality component that allows a user role to only have access to detailed medical information in situations where they are providing that patient with care, those options should be explored.

[184] NSH explained that the Meditech system offers the ability to limit access within a facility or zone, but this function is rarely used in practice. One example given of its use is that the nurse positions in the Intensive Care Unit (ICU) are limited to accessing patients who are assigned to the ICU. No other examples were provided of this limitation being used in practice.[80]

[185] NSH also said that it may be limited in its ability to manage access controls by the functionality available within each application or electronic information system and that sometimes this is controlled by the vendor of the systems.

[186] The degree to which custodians can technically limit user access within an electronic information system depends on what access control options are offered by the system's vendor. For example, a custodian may be able to limit a role's access to those who have a clinical relationship with the patient, as well as to specific modules within an electronic information system (e.g., the admissions module), specific types of records or portions of records (e.g., registration information), certain functions within these records (e.g., read, write, delete), and/or specific geographic locations (e.g., a zone, hospital or medical unit). The ability to technically limit how patient searches are conducted, such as the search criteria an employee can use and what personal health information those searches return, as well as what reports can be run by an employee, can also impact what personal health information a role can access.

[187] It is not clear to me that NSH has fully explored if there are functional upgrades that could be made to its electronic information systems to implement the ability to restrict user access based on the clinical relationship with the patient. Have upgrades been developed since NSH last engaged with the electronic information system vendors? There is also the possibility that Meditech and One Content or another software company could create a custom solution to restrict user access to detailed information of those patients the user has an active clinical relationship with.

---

[79] NSH Information Technology Office oral representations January 18, 2021.
[80] NSH Information Technology Office oral representations January 18, 2021.

[188] **Recommendation #8:** I recommend that within three months of the date of this report, NSH begin to work with its vendors to:

a) Explore whether user access in existing electronic information systems to detailed electronic medical records can be limited to those users who are actively providing care to a particular patient.
b) Ensure that any new electronic information systems it purchases have this capability.

Telephone number search function

[189] A second concern with the functionality of one of the electronic information systems is that users can search for patients based on phone number. This function is limited to Meditech.

[190] As described above, Employee H was twice able to find out the names of a targeted individual's family members by first finding the individual's phone number in the electronic health records and then using the phone number to search for any other people associated with that same phone number in the electronic information system. Employee H then performed targeted lookups of those related individuals' electronic health records.

[191] NSH agreed that the phone number search function has no necessary purpose but believed that the control over that functionality rests with the vendor. NSH privacy representatives stated that they had previously attempted to have the phone number search function disabled because there was no known need for it.[81] NSH Information Technology claimed that it had made every effort to disable the phone number search function but could not because it is control by the vendor.[82] The phone number search function in NSH's Meditech system remains functional to this day.

[192] Given the prominence that these search functionalities play in facilitating employees abusing their access to personal health information, this is an area of significant concern regarding the custodian having reasonable safeguards in place to protect the personal health information in its custody or control.

[193] NSH appears to have struggled with the limitations in Meditech in terms of disabling the phone number search function. However, it is possible that solutions may develop over time. In 2014, Ontario's former Information and Privacy Commissioner (ON Commissioner) addressed search functionality as part of his investigation of unauthorized access to newborn and maternity records by Rouge Valley Health System employees in its open-ended search functionality Meditech system.[83] In addition to being able to search by things like name or health card number, the user could also do things like add the term "baby" to the search and in that way get a list of newborns who had not yet been named and so were termed "baby" in Meditech. In that case, the user generated a list of parents of newborns and then gave out their contact information for the

[81] NSH Privacy Office oral representations January 25, 2021.
[82] NSH Information Technology Office oral representations January 18, 2021; NSH written representations March 9, 2021.
[83] *ON PHIPA Order H0-013*, (2014), online: <https://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/169162/index.do>.

purpose of selling them Registered Education Savings Plans. In response to these privacy breaches, the hospital explained that the Meditech system did not have built-in functionality to limit open-ended searches and argued that disallowing open-ended searches that returned lists of patients who partially match the search criteria would affect their ability to schedule appointments and procedures. The ON Commissioner found that disallowing these searches would not adversely impact the hospital and was a reasonable measure in the circumstances to protect patient information from unauthorized use. The hospital was ordered to work with Meditech or another software provider to create a solution that limits the open-ended search functionality in the system.

[194] I am not aware whether the Rouge Valley Health System was able to implement the ordered changes to search functionality, but it is worth speaking with other health authorities to see if they have been able to achieve limitations to their search functionality that could be applied at NSH.

[195] **Finding #9:** I find that NSH allowing the telephone number search function in Meditech is not a reasonable security and information practice.

[196] **Recommendation #9:** I recommend that within six months of the date of this report, NSH:

a) Find a solution to disable the phone number search function with Meditech or with another software service provider.
b) Reach out to other health authorities to determine how they were able to disable this function.

Privacy training and confidentiality pledge content and frequency

[197] Proper onboarding of users to electronic information systems is not the only relevant information practice to protect against unauthorized access to personal health information. Employees also need proper training about what they can look up within the access granted to them. Just because a user has system access does not mean that they are authorized to look at everything they have access to. This is where the role of training becomes important. *PHIA* specifically makes the custodian's contact person accountable for "ensur[ing] that all agents of the custodian are appropriately informed of their duties under the Act."[84]

[198] The *NSH Privacy Policy* requires staff to complete online privacy training and sign a confidentiality pledge upon hiring and repeat annually thereafter.[85] NSH confirmed that in 2020, only 49.5% of its staff had completed the online privacy training by November 23rd when it was reported.[86] In 2019, about 52.5% of employees had taken this annual training. Of the eight employees investigated for this report, training records show that four never completed the NSH

[84] *Personal Health Information Act*, SNS 2010, c 41, s. 67(1)(b).
[85] *NSH Privacy Policy*, at Procedure 1.1 and at Safeguards 5.3.2. This policy was approved in 2017, but only became effective on February 13, 2020.
[86] NSH written representations November 24, 2020.

privacy training module, and three had completed it only once prior to the discovery of their unauthorized access. One individual had completed the training at least twice prior to the incidents. Despite the fact that this training is mandatory, more than half the employees in 2020 hadn't taken it.

[199] In addition, NSH developed privacy training sessions for managers and those in a leadership position, which have been delivered since 2017. NSH confirmed these training sessions are not mandatory.

[200] Records also show inconsistent adherence to employees' annual signing of the confidentiality pledge. Two of the eight employees investigated for this report had signed pledges at former regional health authorities but had not signed a current NSH pledge.

[201] NSH confirmed that there is no mechanism in place to force the annual completion of the privacy training module and signing of confidentiality pledge, and that it is "up to each manager to run reports for their team and verify that they have completed the mandatory modules."[87] NSH stated that they "were developing reports for Senior Leaders but then the leadership restructuring took place and we have to re-develop them."[88]

[202] Privacy training cannot be an effective preventative measure unless it is taken regularly by staff throughout their career. Ongoing competency requirements exist in many aspects of health care. Privacy training should be considered an annual competency. Providing it only sporadically is not sufficient.

[203] There must also be meaningful consequences for non-compliance with privacy training requirements such as suspending access to the electronic information systems until such time as the annual privacy training has been taken. Otherwise, training may be neglected.

[204] In terms of the training and confidentiality pledge content, one glaring topic missing from training and the confidentiality pledge is the issue of prosecutions for privacy breaches.[89] When the OIPC investigator asked an employee found to have breached privacy whether they were aware that prosecution was a potential consequence of employee snooping, they indicated they were not. The employee explained that this knowledge would have influenced their decision to snoop. It should be plain in any training going forward that prosecution could be a direct consequence of employee snooping, including adding it to the list of actions that may be taken for violations contained in NSH's confidentiality pledge.

[205] In addition, real life examples of snooping at NSH should be part of the training, including examples from this report to help employees contextualize and understand their authority to look up information within the boundaries of the need-to-know principle. The experience of individuals who have been harmed by employee snooping should be emphasized

---

[87] NSH written representations November 24, 2020.
[88] NSH written representations November 24, 2020.
[89] Pursuant to s. 106 of *PHIA*, the willful collection, use or disclosure of health information is considered an offence. Persons found guilty are liable on summary conviction to a fine of not more than ten thousand dollars or imprisonment for 6 months, or both (s. 107, *PHIA*).

and given voice, as well as the consequences for NSH and its employees, such as the possibility that an employee could have their employment terminated for unauthorized access or that they could be prosecuted for the behaviour.

[206] Finally, incorporating a message from a senior executive about the seriousness of employee snooping may also help reinforce the message that employee unauthorized access of personal health information is not tolerated.

[207] **Finding #10:** I find that there are shortcomings in NSH's security and information practices in terms of privacy training and confidentiality pledge content and frequency.

[208] **Recommendation #10:** I recommend that within one year of the date of this report, NSH:

a) Update the *NSH Privacy Policy* to set out clear consequences for the non-completion of privacy training and confidentiality pledge signing on an annual basis, including the suspension of electronic information systems access if training or confidentiality pledge signing is not completed within a set timeframe.
b) Strengthen the content of its online privacy training module by clearly stating that employee snooping is a prosecutable offense under *PHIA*, by adding additional real-life examples of snooping at NSH and its impact on patients, employees and NSH and by adding a message from NSH senior executive leadership about the seriousness of snooping in electronic information systems.
c) Update the NSH confidentiality pledge to reflect that employee snooping is a prosecutable offense under *PHIA*.

Audit plans and functionality

[209] Finally, an important information practice to prevent unauthorized user access to electronic information systems is to monitor user access. Even when custodians have reasonable role-based access onboarding procedures and implement training to teach employees what access is unauthorized, it is possible that some employees may still snoop. That is why access still needs to be continually monitored. With electronic information systems, this monitoring is typically done by way of system auditing.

[210] In 2014, former ON Commissioner Brian Beamish noted the dual detection and deterrence functions of audits:

> Audits are essential technical safeguards to protect personal health information. They can be used to deter and detect collections, uses and disclosures of personal health information that contravene the *Act* [Ontario's *Personal Health Information Protection Act*] In this way, they help maintain the integrity and confidentiality of personal health information stored in electronic information systems. The Hospital's failure to implement

full audit functionality in its Meditech system meant it could not comply with its own policies and that it did not comply with the requirements of the *Act.*[90]

[211] Cases dealing with intentional unauthorized access and use of personal health information by authorized users highlight the need for technical infrastructure to keep track of and log each user's access within electronic information systems and the need for an ongoing program of proactive auditing to address the general risk of intentional abuse of access by authorized users.[91]

[212] For audits to work as a technical safeguard, electronic information systems must first be able to log all instances where users have viewed personal health information. Then, the audit reports must be monitored proactively for high-risk behaviors on a regular basis, as well as in response to complaints. These measures are required information practices under s. 62 of *PHIA*.

[213] As part of this investigation, the OIPC requested a complete list of all NSH electronic information systems that the eight employees had access to, information on whether these systems could log all instances of user access, and finally, whether these logs could then be audited. NSH is the custodian of the personal health information held in more than 500 electronic information systems. Many systems do log user access and can be audited, to varying degrees. In response to the OIPC's questions about audit capacity of the systems the eight employees had access to, NSH identified some electronic information systems that lack logging or auditing capacity:

- Some systems can only log instances where a user has modified personal health information. Instances where a user only viewed information are not logged.
- Some systems have logging and audit capacity, but the functionality is not being used either because it was not bought at the time of purchase or was not activated after it was purchased.[92]

[214] A custodian the size and scope of NSH may need to maintain a higher number of electronic information systems to achieve its mission. However, those systems must comply with *PHIA*. If NSH's current electronic information systems cannot be made compliant through the purchasing of upgraded functionality or customization, then a plan for replacing them with systems that can meet *PHIA*'s requirements should be developed as soon as practicable.

---

[90] *ON PHIPA Order H0-013*, (2014), online: <https://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/169162/index.do> at p. 1.

[91] *AB IR 2013-IR-02*, 2013 CanLII 82405(AB OIPC); *AB Order H2016-06, Alberta Health Services (Re)*, 2016 CanLII 104927 (AB OIPC); *AB Order H2014-02, Alberta Health Services (Re)*, 2014 CanLII 41751 (AB OIPC); *NFLD Report PH-2016-001, Eastern Health (Re)*, 2016 CanLII 85236; *ON HR15-115, A Public Hospital (Re)*, 2017 CanLII 88475 (ON IPC); *ON HC14-16, London Health Sciences Centre (Re)*, 2017 CanLII 31432 (ON IPC); *ON HC14-112 and HC15-14, Group Health Centre (Re)*, 2017 CanLII 87957 (ON IPC); *SK IR 142-15, Heartland Regional Health Authority (Re)*, 2015 CanLII 85349 (SK IPC); *SK IR H-2013-001, Regina Qu'Appelle Regional Health Authority (Re)*; 2013 CanLII 5640 (SK IPC); *SK IR H-2010-001, L&M Pharmacy Inc (Re)*, 2010 CanLII 17914 (SK IPC); *MB Ombuds Case 2014-0500, Manitoba Health, Seniors and Active Living Provincial Drug Program*.

[92] *20-00324 2021 03 09 User Access List for OIPC,* NSH written representations March 9, 2021.

[215] The *NSH Auditing Policy* sets out guiding principles and values, as well as statements about the importance of auditing as a safeguard for personal health information. The policy calls for the NSH Privacy Office to prepare an annual audit plan setting out types of proactive audits and their frequency.

[216] NSH submitted for this review its *Annual Audit Plan* for 2019 and information about results of audits performed. The audit plan sets out eight types of audits. There is a column showing the frequency for how often the audits should be conducted, and a heading entitled "plan 2019". Despite the audit plan mandating various audits at specified frequencies, audits were largely not done.

[217] For example, audits can flag users who access the electronic health records of someone that user shares a home address with. Looking up the information of someone within the user's own household without that person's consent is a privacy breach and is unauthorized under *PHIA*. This audit relies on the electronic information systems being able to compare a patient's home address with a user's home address. NSH reported that it has never performed this audit. When the audit plan was initiated there remained barriers with being able to compare the patient's home address with a user's home address in a manner that allowed for auditing. Since that time, NSH has resolved the issue and confirmed that this audit is now possible, but has not been done.[93]

[218] Another example is with respect to co-worker lookups. This audit flags users who access a co-worker's electronic health records. This audit relies on the electronic information systems being able to match an employee with their department and their health records and compare it to a user's department. NSH reported that it has never performed this audit. NSH identified that the barriers to performing this audit are that users' departments are often not up to date in the systems and it has not established a way to match a list of employees in a department with their electronic health records for the purpose of this auditing.[94]

[219] Another type of audit checks for users who look up patients that are not registered to their clinic or department. This is a proposed audit type, but there is no current plan to implement it. During oral representations, the NSH privacy representative identified this as a potential audit type that would not face some of the barriers identified with other audits. This proposed audit would randomly select specific departments at regular intervals and audit all access by users within the department compared to a list of patients registered to that department. This would highlight any access to electronic health records of patients who are not registered to the department or clinic where the user works.

[220] The NSH privacy representative further commented that beyond the audits which were planned but could not be performed because of the barriers identified above, the NSH Privacy Office does not have sufficient resources to fully comply with its auditing plan or to pursue new auditing which may be effective in identifying unauthorized access. The representative identified that with no additional resources, the NSH Privacy Office must ask clinical areas to complete the

[93] NSH Privacy Office oral representations March 12, 2021.
[94] NSH Privacy Office oral representations March 12, 2021.

reviewing of audit results, but there is not always support or commitment from clinical areas to do this work because it is time consuming. At the time of this investigation, the NSH Privacy Office had no dedicated resources for auditing. It relies on zone privacy officers for all proactive audit functions. The privacy representative estimated that to operate an effective proactive audit program for the whole of NSH, at least one dedicated audit employee who can establish subject matter expertise in auditing of NSH's complex systems is required and that an additional two generalist positions to support the work may also be necessary.[95] There is no point in having an audit plan without providing sufficient resources to implement it. The privacy team needs sufficient resources not only to develop a realistic audit plan but also to follow through on it.

[221] **Finding #11:** I find that the *NSH Audit Plan* is based on best practices and risk-based audits, but it has been only partially implemented. NSH has not dedicated sufficient resources to complete required proactive auditing.

[222] **Recommendation #11:** I recommend that within one year of the date of this report, NSH take the following actions to strengthen its auditing of users:

a) Review and update its *NSH Audit Plan* to include the proposed regular audit of users looking up patients not registered to the users' departments or clinics.
b) Provide sufficient resources to ensure that it can fully implement its *NSH Audit Plan* and routinely and consistently conduct proactive audits.

Privacy Management Program

[223] A privacy management program is a system of interconnected activities used to manage and protect personal health information in a custodian's custody or control. The reasonable security provisions found in most Canadian privacy legislation, such as s. 62 of *PHIA*, are generally held to require organizations to implement a privacy management program.[96] Assessing the health of one's overall privacy management program after a breach can help ensure systemic issues and/or resource needs are not overlooked when developing prevention strategies for a specific breach.

[224] A privacy management program requires organizational commitment (e.g., resources, leadership, reporting), and ongoing assessment and revision activities (e.g., monitoring and adapting program controls to meet changing needs).[97] These components are interconnected.

---

[95] NSH Privacy Office oral representations March 12, 2021.
[96] *NS Report IR16-01, Nova Scotia (Office of the Premier) (Re)*, 2016 NSOIPC 15 (CanLII), at para. 79.
[97] For more information regarding privacy management program requirements, see NS OIPC guidance document, *Privacy Management Program Toolkit Health Custodians*, online: NS OIPC <https://oipc.novascotia.ca/sites/default/files/publications/Full%20PHIA%20PMP%20Toolkit%202015%2010%2002%202%20.pdf>.

Organizational commitment

[225] The Office of the Privacy Commissioner of Canada has stated that "[p]erhaps the most important element in the prevention of employee snooping is an organization's culture of privacy, as it supports the effectiveness of all other measures."[98]

[226] The strength of an organization's culture of privacy is tied to the ability of its privacy management program to embed privacy as a core organizational value into day-to-day operations.[99] If an organization's privacy management program is weak, then privacy may not be perceived as important by employees, increasing the likelihood that the workplace culture will tolerate snooping behavior and that adherence to other safeguards will be lacking.

[227] Organizational commitment also includes resource considerations. For a custodian's privacy management program to operate effectively and, at a minimum, demonstrate compliance with *PHIA*, the executive team must ensure the necessary resources are in place. Former British Columbia Information and Privacy Commissioner Elizabeth Denham made this compelling statement about resourcing:

> To actively champion a privacy management program, the executive should ensure that all resources necessary to develop, implement, monitor and adapt the program are available…. Public bodies face competing demands for public resources, which can be scarce. However, compliance with provincial privacy law is not discretionary; adequate funding and support needs to be devoted to privacy compliance.[100]

[228] While all leadership roles should support privacy management programs, another important component to demonstrating organizational commitment is to identify which leadership positions have specific roles in the privacy management program.

[229] One important leadership role is that of a chief privacy officer. To quote former Nova Scotia Information and Privacy Commissioner Tully, "A strong, modern privacy management program begins with strong leadership. Appointing a Chief Privacy Officer who occupies an executive-level position provides that leadership."[101]

[230] It appears that NSH either does not have a chief privacy officer, or if it does, that role is not an executive-level position at NSH. While NSH's executive team includes vice-presidents who act as the chief nursing executive and the chief finance officer, no vice-president (VP) appears to be designated as the chief privacy officer.[102] The *NSH Privacy Breach Protocol* states

---

[98] Office of the Privacy Commissioner of Canada, *Ten tips to address employee snooping* (March 2016), online: OPC <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/02_05_d_65_tips/>.
[99] AB OIPC, BC OIPC and OPC, *Getting Accountability Right with a Privacy Management Program* (April 2012) online: OPC <https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf> at p. 4.
[100] *British Columbia Health Authority Privacy Breach Management (Re)*, 2015 BCIPC 66 (CanLII), at s. 4.3.
[101] *NS Report IR16-01, Nova Scotia (Office of the Premier) (Re)*, 2016 NSOIPC 15 (CanLII), at para. 99.
[102] NSH, *Executive Team*, online: <https://www.nshealth.ca/about-us/executive-team>. Note this webpage is not dated but was last checked on October 25, 2022.

in its internal notification section that the "VP of Quality & System Performance (oversees Privacy and Legal)" is to be notified of major breaches. Appendix A of the *NSH Privacy Breach Protocol* includes a table that sets out in one column the position title and in the second column, that position's responsibilities. The general counsel position title is followed in brackets with "(NSHA Chief Privacy Officer)."[103] It may be that the general counsel also acts as chief privacy officer but that is not clear to me. In any event, general counsel is not a member of the executive team, according to NSH's website.[104]

[231] As part of the executive team, a chief privacy officer is responsible for privacy management and compliance at a strategic level. They ensure a privacy lens is applied during discussions of major strategic initiatives, such as the One Person One Record initiative.[105] They champion the mitigation of major privacy risks, such as employee snooping, and advocate for the resources and workplace alignment needed for the privacy management program to succeed. In addition to providing clear executive leadership and accountability for privacy, a chief privacy officer at the executive level would have the visibility and relationships with other strategic leaders needed to help ensure NSH's privacy management program is compliant with *PHIA* and effectively implemented.

[232] A well-developed reporting and internal governance structure for privacy is also part of a strong privacy management program. The *NSH Privacy Breach Protocol*'s internal notification and escalation process states that the VP of Quality & Systems Performance must always be notified of a "major" breach. That person decides whether the chief executive officer (CEO) will be notified. The CEO, in turn, decides whether the organization's board of directors should be notified. However, the policy is silent on what criteria the VP and CEO use respectively to determine which breaches are escalated.

[233] The *NSH Privacy Breach Protocol* also includes Appendix A which is a table that broadly defines roles and responsibilities for all levels of the organization except the board of directors. Executive leadership's responsibilities are stated as receiving and reviewing reports of "major" privacy breaches they receive; activating an incident response team under advisement of the privacy manager; appointing a person to chair an incident response team; participating in decision-making as required and following up with the privacy officer and others to ensure containment, notification and prevention actions are done.

[234] In my view, there is a foundational problem in that the *NSH Privacy Breach Protocol* limits executive involvement to "major" breaches, which is a term that is not defined in the *NSH Privacy Breach Protocol*. Instead, the terms "minor, unintentional breaches",[106] "major,

---

[103] Note that the NSHA acronym is no longer used and has been replaced with NSH.
[104] NSH, *Executive Team*, online: <https://www.nshealth.ca/about-us/executive-team>.
[105] One Person One Record is a project to modernize Nova Scotia's health information systems. See Department of Health and Wellness, *One Person One Record Project Moves to Next Phase* (December 2016), online: Government of Nova Scotia <https://novascotia.ca/news/release/?id=20161206001>.
[106] Defined as "A minor breach is a breach that involves limited PHI and a limited number of patients. It is unintentional because it is caused by an error or oversight. An error leading to an unintentional breach may not even be caused by NSHA (i.e., receiving wrong information from patient or referring provider), but may lead to a breach nonetheless and must be reported."

unintentional breaches"[107] and "intentional breaches"[108] are defined. But what about intentional breaches? As currently drafted, the *NSH Privacy Breach Protocol* could be interpreted to mean that executive involvement is not engaged when there is an intentional snooping incident. Better wording is needed to ensure executive involvement when snooping breaches occur.

[235] Furthermore, there is room for magnifying and clarifying executive leadership's roles and responsibilities. NSH may wish to look to its *Enterprise Risk Management Policy (NSH ERM Policy)*[109] for guidance in this area. The *NSH ERM Policy* clearly states the responsibilities of the board of directors and the CEO in relation to enterprise-wide risks. It states the board of directors has governance over NSH's enterprise-wide risks and that it is accountable for reviewing and approving action plans for their mitigation on an annual basis. The CEO is responsible for providing input into risk identification, assessment, and mitigation activities. The CEO is also responsible for updating the board of directors on the status of risk mitigation activities at least twice a year. There is a risk mapping tool that is used to determine who needs to be informed of enterprise-wide risks and how they are treated.

[236] In addition, external reporting mechanisms serve an important accountability and transparency function and can drive change. Section 69 of *PHIA* requires NSH to notify affected individuals if their personal health information is subject to unauthorized access, use or disclosure and as result, there is a potential for harm or embarrassment to the individual. Employee snooping is considered unauthorized access and possibly use or disclosure, depending on the circumstances. However, NSH is not required to report publicly on the number of employee snooping breaches it uncovers or the number of audits it runs. NSH is also not required under *PHIA* to report employee snooping breaches to the OIPC. Custodians are only required to notify the OIPC in circumstances where personal health information has been subject to unauthorized access but it is unlikely that there was a breach of personal health information or there is no potential for harm or embarrassment to the affected individual. It did so voluntarily in this case, but the legislation does not require this. The OIPC may become aware of the breach after an affected individual has made a complaint to the OIPC or contacts the media. Without consistent reporting, it is challenging for the OIPC to fulfill its monitoring and oversight functions under *PHIA*. Legislative change is needed in this area, but until that occurs, NSH should report all future employee snooping breaches to the OIPC.

Ongoing assessment and revision activities

[237] As part of its investigation into the theft of personal information by an employee at Desjardins that affected 9.7 million Canadians, the Office of the Privacy Commissioner of Canada (OPC) noted that while Desjardins had a number of policies, procedures and directives to

---

[107] Defined as "A major breach is a breach that either involves extensive or sensitive PHI and/or a large number of patients. It is unintentional because it is caused by an error or oversight."
[108] Defined as "A breach is intentional when someone sets out to collect, use, access or disclose health information for a purpose for which it was not authorized and/or is not required for their work."
[109] NSH, *Enterprise Risk Management Policy (NSH ERM Policy*) (Approval date: May 12, 2016; Effective Date: July 1, 2016), online: <http://policy.nshealth.ca/Site_Published/nsha/document_render.aspx?documentRender.IdType=6&documentRender.GenericField=&documentRender.Id=86812>.

protect personal information, it had failed to adequately implement them in some cases.[110] The OPC emphasized that "vigilance and a holistic approach are important when deploying measures to address and mitigate the impact" of insider threats.[111] The OPC then recommended that Desjardins engage a qualified external auditing firm to undertake a full assessment of its security and privacy program, including the allocation of resources to privacy protection.

[238] This report sets out a number of concerns with NSH's privacy management program. Policy documents are at times outdated and unclear and, in many cases, not being followed. Program controls must be regularly assessed and updated in a timely way for them to remain relevant, effective and compliant with *PHIA*. A critical review of whether NSH's privacy management program is sufficiently resourced to ensure compliance with *PHIA* is needed. Such a review should be accompanied by the resources needed for ongoing assessment and revision activities, as compliance is not a static activity.[112]

[239] Similarly, a detailed and holistic assessment of NSH's privacy management program should be conducted. The Office of the Auditor General of Nova Scotia reported in its December 2021 report that an external consulting firm had been engaged to conduct an independent review of NSH's cybersecurity environment.[113] NSH could also use an independent qualified auditing firm to review its privacy management program.

[240] **Finding #12:** I find that NSH's privacy management program has deficiencies that impair its ability to properly mitigate the risk of employee snooping.

[241] **Recommendation #12:** I recommend that within one year of the date of this report, NSH take the following actions to strengthen its privacy management program:

a) Ensure there is a clearly identified executive-level position designated as chief privacy officer to provide ongoing strategic privacy leadership.
b) Amend the *NSH Privacy Breach Protocol* to more clearly define the roles and responsibilities of executive leadership in responding to intentional snooping privacy breaches, considering the comments made in this report.
c) Annually report to all NSH employees, the board of directors, the public and the OIPC, the key indicators related to unauthorized employee access to electronic health records, including:
    (i) the percentage of employees who completed their annual privacy training and confidentiality pledge;
    (ii) the total number of proactive audits of user activity completed by NSH;
    (iii) the total number of employees detected as having abused their access to electronic health records.

---

[110] *OPC Report 20-005, Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019*, 2020 CanLII 99211 (PCC), at para. 56.
[111] *OPC Report 20-005, Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019*, 2020 CanLII 99211 (PCC), at para. 123.
[112] AB OIPC, BC OIPC and OPC, *Getting Accountability Right with a Privacy Management Program* (April 2012), online: OPC <https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf > at p. 2.
[113] Office of the Auditor General of Nova Scotia (NS OAG), *2021 Financial Report* (December 7, 2021), online: NS OAG <https://oag-ns.ca/sites/default/files/publications/2021FinancialFullWeb.pdf> at para. 1.66.

5.0 Summary of Findings and Recommendations

5.1 Findings

[242] The summary of my findings is provided below.

Finding #1: I find that NSH's initial response of conducting additional audits of employees whose access was flagged on audit reports was reasonable and required by the circumstances. However, I further find that NSH failing to conduct additional audits of Employee D and the doctor associated with the ninth unidentified employee was not reasonable in the circumstances.

Finding #2: I find that NSH failed to contain the privacy breaches by not suspending some employees' electronic information systems access once their unauthorized accesses were being investigated. This resulted in two employees continuing to view electronic health records without authority, which affected an additional seven individuals.

Finding #3: I find that NSH failed to follow its *NSH Privacy Breach Protocol* by not obtaining lists of all the electronic information systems the employees had access to and by not auditing the employees' access to all systems containing personal health information. As a result, there may be privacy breaches yet undiscovered.

Finding #4: I find that the harm from these privacy breaches is significant and was foreseeable.

Finding #5: I find that the notification provided to individuals affected by the privacy breaches by Employees A and G were not done at the first reasonable opportunity, but that notification has now been provided.

Finding #6: I find that the information NSH provided in the notification letters was too generic and not detailed enough for the affected individuals to grasp the extent or severity of the privacy breaches.

Finding #7: I find that NSH has not implemented a comprehensive, methodical plan to prevent similar privacy breaches from occurring in the future.

Finding #8: I find that NSH's current practice for approving and updating user access to electronic information systems does not provide reasonable security for personal health information stored in its electronic information systems.

Finding #9: I find that NSH allowing the telephone number search function in Meditech is not a reasonable security and information practice.

Finding #10: I find that there are shortcomings in NSH's security and information practices in terms of privacy training and confidentiality pledge content and frequency.

Finding #11: I find that the *NSH Audit Plan* is based on best practices and risk-based audits, but it has been only partially implemented. NSH has not dedicated sufficient resources to complete required proactive auditing.

Finding #12: I find that NSH's privacy management program has deficiencies that impair its ability to properly mitigate the risk of employee snooping.

5.2 Recommendations

[243] The summary of my recommendations is provided below.

Recommendation #1: I recommend that within 60 days of the date of this report, NSH conduct additional audits of electronic information systems access by Employee D and the doctor associated with the ninth unidentified employee for the one-year period prior to the identified privacy breach and conduct any investigations required as a result of those audits.

Recommendation #2: I recommend that within three months of the date of this report, NSH implement training for all positions that have roles to play in responding to privacy breaches about their respective roles and responsibilities in the *NSH Privacy Breach Protocol*, specifically regarding the responsibility to immediately suspend access to electronic information systems pending investigation. This training should then be ongoing annually.

Recommendation #3: I recommend that within three months of the date of this report, NSH take the following actions to audit additional electronic information systems that the employees had access to:

a) Request that the Department of Health and Wellness conduct audits for a one-year period prior to the flagged privacy breaches of the employees who had access to the Drug Information System to determine if there are any additional privacy breaches by these employees.
b) Complete audits for a one-year period prior to the flagged privacy breaches of the employees' access to all as of yet unaudited NSH electronic information systems that have audit capability.

Recommendation #4: I recommend that within three months of the date of this report, NSH implement training for all positions that have roles to play in responding to privacy breaches as set out in the *NSH Privacy Breach Protocol*, specifically regarding their role to obtain signed and notarized affidavits from employees found to have abused their access to electronic information systems. This training should then be ongoing annually.

Recommendation #5: I recommend that NSH ensure its future privacy breach notifications in cases of intentional unauthorized access by an employee are sufficiently personalized and specific to the matter. This includes ensuring that:

- all terms used are defined (e.g., any acronyms or jargon);
- notifications identify the name of the employee who engaged in the unauthorized access;
- notifications accurately describe the type of information accessed by the named employee;
- notifications give affected individuals specific information about what components of their personal health information were accessed and the number of times it was accessed by the named employee;
- notifications clearly identify if the affected individual was looked up and/or targeted by name;
- notifications provide context for the breaches and avoid the use of generic statements that may or may not apply to the affected individuals.

Recommendation #6: I recommend that within one year of the date of this report, NSH complete a post-breach review of these privacy breaches and develop a comprehensive prevention plan that:

- addresses physical, technical, administrative and personnel controls;
- addresses the concerns raised and recommendations made in this report;
- requires all NSH employees who were involved in responding to these privacy breaches to read this report.

Recommendation #7: I recommend that within nine months of the date of this report, NSH implement a user access request and approval process (or policy) for its electronic information systems. The process or policy must correspond to an established criteria and to standard user profiles. It must also set out verification and validation practices for every new user's access, and for when an existing employee changes roles.

Recommendation #8: I recommend that within three months of the date of this report, NSH begin to work with its vendors to:

a) Explore whether user access in existing electronic information systems to detailed electronic medical records can be limited to those users who are actively providing care to a particular patient.
b) Ensure that any new electronic information systems it purchases have this capability.

Recommendation #9: I recommend that within six months of the date of this report, NSH:

a) Find a solution to disable the phone number search function with Meditech or with another software service provider.
b) Reach out to other health authorities to determine how they were able to disable this function.

Recommendation #10: I recommend that within one year of the date of this report, NSH:

a) Update the *NSH Privacy Policy* to set out clear consequences for the non-completion of privacy training and confidentiality pledge signing on an annual basis, including the suspension of electronic information systems access if training or confidentiality pledge signing is not completed within a set timeframe.
b) Strengthen the content of its online privacy training module by clearly stating that employee snooping is a prosecutable offense under *PHIA*, by adding additional real-life examples of snooping at NSH and its impact on patients, employees and NSH and by adding a message from NSH senior executive leadership about the seriousness of snooping in electronic information systems.
c) Update the NSH confidentiality pledge to reflect that employee snooping is a prosecutable offense under *PHIA*.

Recommendation #11: I recommend that within one year of the date of this report, NSH take the following actions to strengthen its auditing of users:

a) Review and update its *NSH Audit Plan* to include the proposed regular audit of users looking up patients not registered to the users' departments or clinics.
b) Provide sufficient resources to ensure that it can fully implement its *NSH Audit Plan* and routinely and consistently conduct proactive audits.

Recommendation #12: I recommend that within one year of the date of this report, NSH take the following actions to strengthen its privacy management program:

a) Ensure there is a clearly identified executive-level position designated as chief privacy officer to provide ongoing strategic privacy leadership.
b) Amend the *NSH Privacy Breach Protocol* to more clearly define the roles and responsibilities of executive leadership in responding to intentional snooping privacy breaches, considering the comments made in this report.
c) Annually report to all NSH employees, the board of directors, the public and the OIPC, the key indicators related to unauthorized employee access to electronic health records, including:
    (i) the percentage of employees who completed their annual privacy training and confidentiality pledge;
    (ii) the total number of proactive audits of user activity completed by NSH;
    (iii) the total number of employees detected as having abused their access to electronic health records.

6.0 Conclusion

[244] Custodians such as NSH have a legal duty to protect personal health information from unauthorized access under *PHIA*, which is an extension of their duty to protect patients from harm. This investigation found deficiencies in NSH's breach response, such as the failure to suspend employee access to electronic information systems while under investigation. In many cases, NSH did not follow recommended actions in its own privacy breach protocol. Key safeguards for preventing employee snooping, such NSH's role-based access controls and auditing programs were not fully implemented. A common theme emerged in which multiple privacy controls required by *PHIA* and NSH policies were not being implemented in practice.

[245] This pattern indicates that systemic issues may be negatively affecting NSH's ability to maintain *PHIA* compliance. Safeguards must be appropriately resourced and reflected in actual practice to comply with *PHIA*. They must also be monitored for effectiveness and updated regularly to maintain compliance.

[246] Only by adopting a holistic and coordinated approach can NSH take the host of actions needed to mitigate the risk of employee snooping. NSH needs to ensure its privacy management program is properly structured, resourced and implemented in practice to comply with the law. By doing so, NSH can create what is perhaps the most important preventative measure of all - a culture of privacy that is vigilant and does not tolerate this unlawful behavior.

[247] The consequences of inaction are many. Patients will continue to be harmed by acts of serial snooping in a healthcare system meant to heal them. It's likely that NSH will continue to face further legal action in relation to employee snooping. Public trust in NSH's future electronic health records initiatives will continue to be negatively impacted at a critical juncture in this province's journey toward creating a digital healthcare records system.

[248] NSH assured affected individuals in its notification letters that "NSHA takes its responsibilities with respect to the protection of patient confidentiality very seriously." Executive leadership, resources and concrete action are needed to support this statement. This report's recommendations provide a course of action for NSH to follow to achieve *PHIA* compliance. *PHIA* compliance is not discretionary. Employee snooping is not an acceptable risk or an unavoidable side effect of facilitating healthcare workers' access to electronic health records for the purpose of enhancing health care.

7.0 Acknowledgements

[249] I would like to thank NSH for its cooperation with this investigation. The purpose of investigation reports is to look for and share lessons learned for the benefit of Nova Scotians and for the education of all custodians subject to *PHIA*.

[250] I would also like to thank Janet Burt-Gerrans, who led this investigation and the drafting of this report, as well as Alison Shea who also contributed to its drafting.

February 8, 2023

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia