Office of the Information and Privacy Commissioner for Nova Scotia

REVIEW REPORT 20-02

February 26, 2020

Nova Scotia Health Authority

Summary: The Nova Scotia Health Authority, as a personal health information custodian, responded to a privacy breach and gave notice to 2841 affected individuals. One individual, the complainant in this case, requested a review of the custodian's privacy breach response and notification under the *Personal Health Information Act*. The reviewing officer makes four findings and six recommendations under the provisions of s. 100(1) of the *Personal Health Information Act*.

Statutes Considered: *Personal Health Information Act* SNS 2010, c.41 as amended 2012, c.31; 2014, c.32, s.151; *Personal Health Information Regulations* O.I.C. 2012-371, N.S. Reg. 217/2012 as amended O.I.C. 2017-265, N.S. Reg. 159/2017; *Shared Services Act* SNS 2014, c.38 as amended 2016 c.2, ss 17-19; 2018, c.1, Sch A, s.149.

Authorities Considered: Nova Scotia Justice (Re), 2016 NSOIPC 14 (CanLII); BC Lottery Corporation (Re), 2017 BCIPC 21 (CanLII); Sobeys National Pharmacy Group (Re), 2018 NSOIPC 13 (CanLII); Department of Health and Wellness (Re), 2018 NSOIPC 12 (CanLII); Department of Internal Services (Re), 2019 NSPIPC 2 (CanLII); 2013-IR-02, 2013 CanLII 82405 (AB OIPC); Order H2016-06 (Re), 2016 CanLII 104927 (AB OIPC); Order H2014-02 (Re), 2014 CanLII 41751 (AB OIPC); Eastern Health (Re), 2016 CanLII 85236; A Public Hospital, 2017 CanLII 88475 (ON IPC); London Health Sciences Centre (Re), 2017 CanLII 31432 (ON IPC); Group Health Centre (Re), 2017 CanLII 87957 (ON IPC); Heartland Regional Health Authority (Re), 2015 CanLII 85349 (SK IPC); Regina Qu'Appelle Regional Health Authority (Re), 2013 CanLII 5640 (SK IPC); L&M Pharmacy Inc (Re), 2010 CanLII 17914 (SK IPC); Manitoba Ombudsman Case 2014-0500; Electronic Health System (Re), 2010 BCIPC 13 (CanLII).

Other Sources Considered: Susan Yellin, "Cybercriminal increasingly target personal health information" September 3, 2015, https://insurance-portal.ca/article/cyber-criminals-increasingly-target-personal-and-health-information/ (accessed December 13, 2019). Caroline Humer and Jim Finkle, September 26, 2014, "Health Care Firms At Risk; Hackers Value Medical Records Over Credit Data" *Insurance Journal* https://www.insurancejournal.com/news/national/2014/09/26/341691.htm; Infosec, Hackers Selling Healthcare Data in the Black Market https://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/; Proofpoint, "State of the Phish" 2019 Report, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish; Office of the Privacy

Commissioner of Canada, "Recognizing threats to personal data online" https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/phishing/; Infosec, "Phishing Attack Overview" https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-attack-overview/ (accessed December 13, 2019); Volume 24, January – December 2018, https://www.microsoft.com/en-us/security/operations/security-intelligence-reporthttps://www.isaca.org/resources/news-and-trends/isaca-now-blog; BC Investigation Report F06-01; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order H2005-IR-00; Ontario Order MC09-9; Alberta Order P2013-04; BC Investigation Report F12-02; Canadian Centre for Cyber Security https://cyber.gc.ca/en/; "Chapter 1: Health and Wellness; Internal Services; IWK Health Centre; and Nova Scotia Health Authority: Management and Oversight of Health Sector Information Technology." Auditor's Report, Office of the Auditor General, December 2018; https://arstechnica.com/information-technology/2020/02/four-plus-years-later-ashley-madison-hack-is-used-in-new-extortion-scam/; http://www.ibm.com; J Henriksen Bulmer and S Jeary, 'Re-Identification Attacks – A Systematic Literature Review' (2016) 36 Int'l J Information Management 1184.

INTRODUCTION:

[1] On or about May 8, 2019, a Nova Scotia Health Authority (NSHA) employee responded to a fraudulent email. The employee clicked a link and supplied account login and password information to an attacker. The employee's email account was then accessed by the attacker who is an unknown person or persons with malicious intent. This scenario is known as a successful phishing attack and it resulted in the employee's email account being compromised for a period of approximately five days.

[2] Individuals were affected by the incident because documents containing their sensitive personal health information were attached to emails in the email account at the time it was compromised. On June 6, 2019, the NSHA sent letters notifying 2841 individuals of the attacker's unauthorized access to their personal health information. The NSHA also issued a press release about the privacy breach on June 10, 2019. The complainant in this case received an individual letter notifying him that his information was among the personal health information in the email account. The complainant contacted the NSHA with his concerns and then requested that the Office of the Information and Privacy Commissioner (OIPC) independently review the NSHA's response to the privacy breach, the notification he received, and the NSHA's practices and policies in place to protect patient privacy.

ISSUES:

[3] The issues arising from this privacy complaint are:

1. Did the NSHA take reasonable steps in response to the privacy breach as required by the *Personal Health Information Act (PHIA)*?
2. Does the NSHA have reasonable information practices in place for its email system as required by s. 62 of *PHIA*?

DISCUSSION:

Background

[4] Under Nova Scotia's *Shared Services Act*, the Nova Scotia Health Authority is required to obtain its digital and information technology services from the provincial government's Information Communication and Technology Services (ICTS).[1] ICTS provides the NSHA with network technology and infrastructure, email services, and digital security services. ICTS was the first to be alerted to the employee's compromised email account. It took initial steps to secure the email account and notified the NSHA of the incident. ICTS provided technical services to the NSHA during its response to the privacy breach.

[5] At the time of the phishing attack, it was a component of the employee's role to receive system-generated reports about care provided to patients for the purpose of tracking wait times and resource utilization across the NSHA system. The reports this employee regularly received contained aggregated information about procedures and care provided to many individual patients. The information about individuals was combined into reports that included the type of procedure or care provided, the date it was performed or scheduled, the medical staff assigned, and identifying information about the patient including name, date of birth, and health card number.

Health information practices required

[6] The Nova Scotia Health authority is a custodian within the meaning of the *Personal Health Information Act (PHIA)*. Custodians under *PHIA* are required to implement, maintain, and comply with information practices that are reasonable in the circumstances. For information practices to be considered reasonable, they must also comply with the requirements of *PHIA* and its regulations. Custodians are responsible to ensure that the personal health information in their custody or under their control is protected against theft or loss and unauthorized access, use, disclosure, copying, or modification of the information.[2]

[7] *PHIA* places responsibility on custodians to implement additional safeguards for electronic information systems because of the additional risks associated with rendering and conveying information in a digital format.[3]

[8] The information practices required by *PHIA* include having procedures in place to manage a privacy breach. The generally accepted components of managing a privacy breach are containment and investigation, risk assessment, notification, and prevention.

[9] A privacy breach is defined as occurring when personal health information in the custody or control of the custodian is stolen, lost, or subject to unauthorized access, use, disclosure, copying

---

[1] At the time of the privacy breach and during most of the review of this complaint, the provincial government group providing information technology (IT) services was called Information Communication Technology Services (ICTS), a division of the Department of Internal Services. The provincial government entity responsible for providing digital information technology services is now known as Nova Scotia Digital Services under the responsibility of the Department of Service Nova Scotia and Internal Services. I refer to this group as ICTS throughout the report for ease of reference. For clarity, the Department of Service Nova Scotia and Internal Services was not a respondent under this review.

[2] *PHIA* s. 62(1)

[3] *PHIA* s.65, Regulation 10.

or modification.[4] Custodians under *PHIA* are required to notify individuals affected by a privacy breach at the first reasonable opportunity if as a result of the breach there is potential for harm or embarrassment to the individual.[5]

Jurisdiction

[10] *PHIA* sets out the authority and framework for the independent review of complaints arising from the privacy provisions.[6] The complainant requested that the Office of the Information and Privacy Commissioner[7] conduct an independent review after contacting the NSHA with concerns. The acting Information and Privacy Commissioner duly delegated the authority to conduct and complete the review of this complaint to the acting director of investigations and mediation on October 31, 2019.

[11] *PHIA* authorizes the Information and Privacy Commissioner to make any recommendations with respect to the matter under review that she considers appropriate.[8] This report completes the review and is being issued under s. 100(1) of *PHIA*.

Burden of proof

[12] *PHIA* is silent on the issue of burden of proof. In the absence of a statutory burden of proof, there is an evidentiary burden on the person who lodges the complaint. The usual principle of "she who alleges must prove" applies. This is an evidential burden, not a legal burden, and it requires only that the complainant provide prima facie evidence of the alleged privacy complaint. Such evidence may be satisfied without doing anything other than pointing to evidence already on the record. Once the evidentiary burden is satisfied, the burden shifts to the custodian to establish that it acted in compliance with the requirements of the legislation.[9]

Investigation process

[13] During the review of this privacy complaint, the complainant supplied the OIPC with statements and submissions during the investigation process and was interviewed by telephone. The complainant did not submit written representations to the formal review.

[14] The NSHA responded to two telephone interviews and answered written questions relating to the incident and follow-up. The NSHA also facilitated a telephone conference between the NSHA and the provincial government's Information Communication Technology Services.

---

[4] *PHIA* ss. 69; 70.
[5] *PHIA* s. 69.
[6] *PHIA* s. 92(2)(a).
[7] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*.
[8] *PHIA* s. 100(4).
[9] This approach in privacy complaint matters was adopted in Nova Scotia by the Information and Privacy Commissioner in Review Report 16-06 [Nova Scotia Justice (Re), 2016 NSOIPC 14 (*Canlii*)]. It is consistent with, for example, BC OIPC Order F13-04 [BC Lottery Corporation (Re), 2017 BCIPC 21 at para. 5].

[15] The NSHA submitted more than 33 documents for the review including relevant policies, a summary of its privacy breach investigation and follow-up, communications to the complainant, and documents of its phishing awareness campaign. The NSHA made written representations to the formal review process.

[16] Both the NSHA and the complainant were provided an opportunity to comment on and dispute findings of fact prior to the completion of this report. On the eve of this report being completed, the NSHA and the Department of Service Nova Scotia and Internal Services (the Department responsible for the former ICTS) brought forward significant new and clarified facts which delayed the completion of the report. The facts as presented in this report are accurate and confirmed as of the date of publication.

ANALYSIS & FINDINGS

Did the NSHA take reasonable steps in response to the privacy breach as required by *PHIA*?

[17] The information practices required by *PHIA* include having procedures in place to manage a privacy breach. The generally accepted critical steps of managing a privacy breach are containment and investigation, risk assessment, notification, and prevention.

[18] The NSHA has a Privacy Breach Management Protocol that formalizes the four key steps of managing a privacy breach into policy. The NSHA investigated, assessed the risks from the breach, notified the affected individuals, and identified prevention strategies. The reasonableness of the NSHA's actions under the first three steps are analyzed within this issue section.

Step 1: Contain the breach and investigate

[19] The first warning sign of a problem with the employee's compromised email account was when some NSHA users contacted ICTS about suspicious messages sent from the employee's compromised email account on May 10, 2019. Messages were sent to approximately 6000+ recipients between 2:45 p.m. and 4:13 p.m. on May 10, 2019.

[20] The ICTS network firewall is a technical safeguard that tracks inbound and outbound traffic with pre-programmed settings to detect suspicious activity. The unusually high volume of outgoing messages from the employee's email account caused the firewall to set off an alert to ICTS on May 13, 2019, three days after the volume of messages were sent. After receiving this alert, ICTS changed the employee's password for the compromised email account which effectively ended the attacker's access to the account. ICTS also alerted the NSHA about the attack on Monday, May 13, 2019.

[21] The NSHA's investigation confirmed that on May 8, 2019, the employee received a fraudulent email asking her to click a link to a website and confirm her username and password, which she did. The attacker had access to the account from the time the attacker had the employee's login credentials, until the time the password was changed on May 13, 2019, a period of approximately five days.

[22] The safeguards in place did not detect the attack at the first opportunity and the firewall appears to have been delayed in sending an alert about the volume of outgoing messages. The safeguards did eventually detect and then end the attack. ICTS received an early warning from other users who received suspicious messages from the email account that did not trigger action. ICTS did not act until its firewall sent an alert on May 13, 2019, three days later.

[23] The five days that the attacker had access to the email account is enough time for a motivated person to take, copy, disclose, distribute, or otherwise mine information available in an email account. In order to fully contain the privacy breach, the NSHA needed to determine what personal health information was in the email account and what access, use, or disclosure it suffered at the hands of the attacker.

[24] The NSHA's investigation focused on reviewing the contents of the email account that was available to the attacker. Its investigation discovered 95 documents containing sensitive personal health information in Microsoft Excel and Adobe PDF formats attached to emails within the email account.

[25] The documents the NSHA discovered were sent to the employee by an automated information update process called an RSS feed.[10] An RSS feed takes information from a selected source, puts it into a machine-readable format, and pushes it to a user. In this case, it was set to automatically push updated reports of information to this employee's email account. The NSHA's investigation concluded that the employee saved the documents she needed to a network storage location and there was no continuing purpose for them to be stored in the email account. The NSHA's investigation summary document also notes that for at least some of the documents, the employee did not appear to be aware that that they were stored in the email account.[11]

Investigating the attacker's activity

[26] ICTS confirmed that the attacker accessed the email account on the internet via the NSHA's webmail application. The webmail application generates a record of user login information such as IP address,[12] login time stamps, and logout time stamps. The NSHA confirmed that the employee did not access the account at all during the five days the account was compromised; therefore, all webmail activity during May 8 – 13, 2019 can be attributed to the attacker.

[27] ICTS also confirmed that the email system keeps the standard activity logs of deleted, sent, and received messages, but it does not log if an email message has been read. ICTS further confirmed that mass downloading or copying of all information in the email account by making a copy of all items such as emails, address books, calendars, notes, and tasks is not enabled for NSHA users and therefore the attacker could not have used the email program to, in one step, take a copy of everything in the email account.

[10] RSS stands for "Really Simple Syndication" or "Rich Site Summary" per: https://en.wikipedia.org/wiki/RSS
[11] NSHA-19-PO-043 Breach Investigation Summary Document, at p. 3.
[12] IP address refers to the location of an internet connection and can be used to track the location of a machine's connection location and internet activity.

[28] Between May 13 and May 22, the NSHA had phone and email contact with ICTS and sought to understand as much as possible about the attacker's activities, including requesting a copy of the outgoing messages sent by the attacker. On May 23, 2019, the NSHA submitted a formal request for information about the attacker's activities via the ICTS ticketing system. The NSHA did not receive very much information about the attacker from ICTS and what it did receive was not provided in a timely manner.

[29] The IP address of the attacker was not investigated at all because ICTS advised the NSHA that it would be unlikely to reveal the attacker's true location since the attacker could have used other technologies to mask their true location.

[30] ICTS did not provide a copy of the outgoing messages sent from the compromised email account to the NSHA for its investigation of the breach. ICTS provided the NSHA with a summary that email messages were sent in alphabetical order from the employee's address book. The outgoing message was a plain text message asking the recipient to "write me back" at a Hotmail or Gmail email account.

[31] After further follow-up by the NSHA, but after the investigation, containment, risk assessment and notification were completed, on June 11, 2019, ICTS provided the NSHA a copy of the outgoing messages sent by the attacker. The NSHA verified that the outgoing messages did not contain personal health information. No other intelligence from the record of outgoing messages, such as the email addresses used by the attacker, patterns in the email addresses of the recipients, or the timestamps on the outgoing messages was investigated.

[32] ICTS did not provide a copy of the webmail application logs to the NSHA for its investigation of the breach. The NSHA submitted that it was not aware that the application log data existed, but once it became aware it requested the data on June 11, 2019, over a month after the attack. ICTS confirmed that webmail application logs regularly overwrite the previous log data in order to save storage space on its servers. ICTS did not maintain a copy of the log data of the attack and by the time the NSHA requested it, it had already been overwritten.

[33] As a result, the NSHA is not able to make conclusions about the location or affiliation of the attacker, the motivations of the attack, the number of times the attacker logged in, or the amount of time the attacker spent logged in to the account. The NSHA is not able to conclusively say what the attacker did with the information that was exposed in the employee's email account.

[34] In order to access the sensitive information contained within the email account, the attacker would have had to individually open emails and read them and separately open and read any attachments. The attacker had enough access over five days to steal the information in the email account by:

- using the Outlook search functions to quickly locate all attachments,
- taking screen shots of the information contained in emails or attachments,
- printing or saving individual emails or attachments to a local computer.

[35] Perhaps those methods would be time consuming. It is also possible that the attacker executed a computer program, a script, to selectively scrape the contents of the email account. Email parsing software is readily available and suited to the task.[13] The NSHA does not have evidence that the attacker did use these methods to steal the information, however, the NSHA also does not have evidence to rule out these reasonable possibilities.

[36] The webmail application log information could have provided details of the dates and times the attacker logged into the email account and the total length of time the attacker was logged in. Leveraging and analyzing all the log and activity information could have provided insight into the risk that the attacker stole the information that was in the email account. The IP address logged on the webmail application may have provided information about the location or affiliation of the attacker.

Responsibility for lack of evidence

[37] Previous investigation and review reports by the Information and Privacy Commissioner for Nova Scotia highlight that the requirements for safeguarding electronic information systems are contextual and depend on the type of system, access, and sensitivity of the information.[14] Cases involving personal health information have emphasized the importance of activity logs to assess the risks of a privacy breach involving electronic systems.[15]

[38] The Information and Privacy Commissioner's investigation report about Nova Scotia's freedom of information website portal privacy breach emphasized the importance of using application access logs during an investigation to determine the activity patterns and extent of a privacy breach, as well as using the information to identify the responsible individuals.[16] That report recommended that the provincial government department responsible, the Department of Internal Services (the same Department responsible for ICTS), strengthen its privacy leadership.

[39] The Office of the Privacy Commissioner of Canada, in a report of its first year with mandatory data breach reporting, published that roughly 25% of the privacy breaches reported involved social engineering attacks such as phishing and impersonation. The same report advises organizations responsible for protecting personal information to, "Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action."[17]

---

[13] http://www.ibm.com

[14] Sobeys National Pharmacy Group (Re), 2018 NSOIPC 13 (CanLII); Department of Health and Wellness (Re), 2018 NSOIPC 12 (CanLII); Department of Internal Services (Re), 2019 NSPIPC 2. These reports adopt a summary of the 12 factors commonly considered when evaluating the reasonableness of a custodian's security.

[15] 2013-IR-02, 2013 CanLII 82405 (AB OIPC); Order H2016-06 (Re), 2016 CanLII 104927 (AB OIPC); Order H2014-02 (Re), 2014 CanLII 41751 (AB OIPC); Eastern Health (Re), 2016 CanLII 85236; A Public Hospital, 2017 CanLII 88475 (ON IPC); London Health Sciences Centre (Re), 2017 CanLII 31432 (ON IPC); Group Health Centre (Re), 2017 CanLII 87957 (ON IPC); Heartland Regional Health Authority (Re), 2015 CanLII 85349 (SK IPC); Regina Qu'Appelle Regional Health Authority (Re), 2013 CanLII 5640 (SK IPC); L&M Pharmacy Inc (Re), 2010 CanLII 17914 (SK IPC); Manitoba Ombudsman Case 2014-0500.

[16] Department of Internal Services (Re), 2019 NS OIPC 2 (CanLII).

[17] Office of the Privacy Commissioner of Canada, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know" https://www.priv.gc.ca/en/blog/20191031/

[40] The NSHA submitted for this review the following statement:

> "NSHA relies upon NS government cybersecurity protections for the security of its e-mail system. Prior to this incident, it would be reasonable in this circumstance to assume that the Nova Scotia government has appropriate cyber protection mechanisms in place to protect the wealth of information that the government collects, uses and discloses on Nova Scotians on a daily basis…"

[41] The NSHA believes that it was reasonable to rely on ICTS because it is the same service provider that is responsible for other government systems involving Nova Scotians' personal information. It based its understanding of this privacy breach on the assumptions and information supplied by ICTS without question and without obtaining the evidence it requested.

[42] Under *PHIA*, if a custodian relies on a service provider for part of its operations, the service provider is viewed as the agent of the custodian.[18] The custodian must maintain oversight of its agents and must ensure that its agents' services render the custodian in compliance with *PHIA*. The custodian is still responsible under *PHIA* and *PHIA* sets a high bar for custodians who use electronic information systems.

[43] It is challenging for custodians to implement safeguards for electronic information systems and they must often rely on the expertise of digital service providers. The NSHA is required by Nova Scotia's *Shared Services Act* to use the centralized digital infrastructure and services of ICTS. However, in managing a privacy breach, the custodian must ultimately take responsibility and ensure that it has effective oversight of its service provider.

[44] This privacy breach has the appearance of falling into the kind of information technology governance weakness addressed more than five months prior by the Auditor General for Nova Scotia in his audit, "Management and Oversight of Health Sector Information Technology".[19] The Auditor General found in his audit that key agreements to formalize roles and accountabilities were not finalized, risk management frameworks were not adequate, the collective risk to the health sector was not adequately managed, and the health sector did not adequately monitor IT service levels.

[45] In this case, there was a delay in ICTS taking action on the early warnings of suspicious messages sent from the compromised email account and critical evidence about the attacker's activities was not maintained and provided to the NSHA. The NSHA recognized that there were weaknesses in how this breach was managed and identified as a "lesson learned" that a protocol for the management of security breaches is needed.[20]

[46] Under *PHIA*, the NSHA has ultimate responsibility for its technical safeguards and privacy breach response. Because of the failures in the investigation, important aspects of this privacy

---

[18] *PHIA* s. 3(a).
[19] "Chapter 1: Health and Wellness; Internal Services; IWK Health Centre; and Nova Scotia Health Authority: Management and Oversight of Health Sector Information Technology." Auditor's Report, Office of the Auditor General, December 2018 https://oag-ns.ca/sites/default/files/publications/FullDec2018_0.pdf.
[20] NSHA-19-PO-043 Breach Investigation Summary Document, at p.11.

breach remain unknown and must be accounted for in the assessment of risk for the affected individuals.

[47] I find that the safeguards in place failed to act at the first signs of the compromised email account and the NSHA's investigation failed to obtain critical evidence necessary to assess appropriate containment action and the risks from the privacy breach.

Step 2: Risk assessment

[48] Assessing the risk associated with a privacy breach involves assessing the components involved in the breach and the potential for harm or embarrassment to affected individuals. The NSHA's assessment of the risks associated with this breach hinges on its assessment of the motivation of the attacker. Following its investigation and in consultation with ICTS, the NSHA believed that the attacker's main motivation was to use the email account to send out another round of phishing messages to the account's contacts list and that "the threat actors would not be interested in other information."[21]

[49] This assessment of the attacker's motives and the corresponding assessment that the personal health information in the email account was not at risk permeated the notification that the NSHA provided to the affected individuals and the follow up actions it took.

[50] My risk assessment, based on the totality of information that is known about the breach, and based on documented sources of information about phishing attacks, is presented here. My analysis follows the structure of an OIPC privacy breach risk assessment.[22]

Personal health information involved

[51] The personal health information of identified individuals that was in the employee's email account was in the form of lists in Microsoft Excel and Adobe PDF documents. The information was highly sensitive personal information that included name, date of birth, health card number, procedure/care provided, as well as date and location of the service. The information of the individuals was combined into aggregated lists in machine-readable document format.[23]

[52] The personal health information involved could be used for fraud and has value on the black market for personal information. Insurance companies and cybersecurity professionals in Canada and the United States have been warning of the black market value of healthcare data since at least 2014 - 2015.[24] Personal health information is viewed as more valuable than credit

---

[21] NSHA representation to the formal review process, at p. 3.

[22] *Key Steps to Responding to Privacy Breaches* https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20to%20Responding%20to%20Privacy%20Breaches%20-%20OIPC%20-2019%2012%2002.pdf

[23] Machine-readable format refers to an electronic format, usually broken into fields or categories of information, that a computer program can scan and draw from.

[24] Susan Yellin, "Cybercriminal increasingly target personal health information" September 3, 2015, https://insurance-portal.ca/article/cyber-criminals-increasingly-target-personal-and-health-information/ (accessed December 13, 2019). Caroline Humer and Jim Finkle, September 26, 2014, "Health Care Firms At Risk; Hackers Value Medical Records Over Credit Data" *Insurance Journal* https://www.insurancejournal.com/news/national/2014/09/26/341691.htm (accessed December 13, 2019); Infosec, Hackers Selling Healthcare Data in the Black Market https://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/ (accessed December 13, 2019).

card data because it does not expire. When a breach of credit card or financial data occurs, the old card or number is cancelled rendering the stolen information inert. With health data, individuals cannot cancel or otherwise reissue their personal health information. It remains accurate and valuable in perpetuity. The risks involving personal health information are not identical to the risks associated with identity theft or credit fraud.

[53] Personal health information can be used by malicious actors to perpetrate frauds and other schemes. False claims to health insurance plans are well documented in the United States.[25] Other scams involve putting the information together with other available information to target an individual directly or by selling the information to brokers who utilize personal data for a variety of purposes.

[54] Social engineering is a technique of scammers using a small amount of personal information to obtain additional personal information from another source or to make a fraudulent plea appear legitimate. The Office of the Information and Privacy Commissioner for Nova Scotia has received unverified reports (unconnected with this privacy breach) of individuals receiving solicitations for medications and medical products where the caller used accurate personal health information collected from an unknown source to make the sales pitch sound legitimate. Some patients, such as seniors and other vulnerable individuals may be more susceptible to this type of fraud.

[55] Information from a privacy breach can be put together with other available information, including publicly available information, other datasets such as published research data, or data obtained from other privacy breaches to further identify individuals to target or to enhance the profile known about an individual. The ability to match both identifiable and de-identified data is increasing with advances in computing capability and the availability of other data sets.[26]

[56] In this case, the fact that the information was aggregated into sets of data about many individuals and already in a machine-readable format increases the black market and target value of the data because it is a volume of information in relatively few files and it is easier to extract and use than individual email messages about one person.

[57] The risk associated with the compromised personal health information involved in this case is very high.

Relationships

[58] The copy of the outgoing messages sent by the attacker, eventually supplied to the NSHA, shows that 6000+ messages were sent to a variety of email accounts (mostly Hotmail accounts) between 2:45 p.m. and 4:13 p.m. on Friday, May 10, 2019. The outgoing messages do not appear to have been sent to any NSHA institutional email accounts.

[59] At the time of the NSHA investigation of the privacy breach, rather than provide a copy of the outgoing messages, ICTS provided a summary of the outgoing message activity, saying that

[25] Ibid.

[26] J Henriksen Bulmer and S Jeary, 'Re-Identification Attacks – A Systematic Literature Review' (2016) 36 Int'l J Information Management 1184.

the attacker sent approximately 4400+ messages in alphabetical order to recipients in the employee's address book.

[60] When it finally received the copy of the attacker's outgoing messages on June 11, 2019, the NSHA reviewed the file to confirm that no personal health information was contained in the outgoing messages. The NSHA did not verify or clarify the difference between what its copy of the outgoing messages shows and the summary provided by ICTS. The difference in the profile of the recipient addresses is significant.

[61] A reasonable reading of the summary provided by ICTS, together with the fact that ICTS received reports from other NSHA employees about the suspicious messages on Friday, May 10, suggests that NSHA email accounts were the recipients of the outgoing messages. An industry report on phishing found that this type of tactic of using a stolen mailbox to phish others within the same organization "is a prevalent tactic when stealing research and intellectual property."[27] It is a way to learn about an organization's defenses and gain access to information contained in the email accounts of employees.

[62] Recognizing the actual recipient email addresses in the copy of outgoing messages eventually supplied helps reduce the risk that the attacker was specifically targeting the NSHA as an organization because the attacker targeted personal Hotmail email addresses to send the next round of spam messages, not the NSHA institutional email addresses.

[63] The relationship of the attacker to the employee and to the recipients of the outgoing messages is unknown. It is thought, based on the ICTS summary, that the recipients were in the employee's address book but none of them appears to be an NSHA institutional address. They may be patients, service providers, employees using Hotmail email accounts, or they may be unrelated to the NSHA.

[64] No conclusion can be drawn from these relationships and it is neutral with respect to assessing the risk that the personal health information in the employee's email account was stolen.

Cause and extent of the breach

[65] The breach was caused by a successful phishing attack that exposed an employee's email account. Phishing attacks are frequently used by malicious actors to try to gain entry to password protected systems.[28]

[66] The NSHA investigation confirmed that the employee had already saved the files containing personal health information on a secure network location and/or was not aware that the messages containing personal health information were in the email account. There was no established and valid purpose for the personal health information to be stored in the email account when it was exposed.

---

[27] F5 LABS, "2019 Phishing and Fraud Report: Simple Yet Effective Attacks You Can't Afford to Ignore" https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

[28] Office of the Privacy Commissioner of Canada, "Recognizing threats to personal data online" https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/phishing/ (accessed December 13, 2019).

[67] Because the NSHA investigation failed to obtain critical evidence, significant information about the extent and motivation of the breach is unknown. The attacker had access to everything in the email account and had ample opportunity to steal the information. The primary risk assessment question is, what is the likelihood that the attacker did or did not mine the compromised account for anything of value before or after using the account to send the next round of phishing messages?

[68] The NSHA's risk assessment concluded that the risk of the attacker having viewed or stolen the information in the email account was so low that it described the breach as only a potential privacy breach. The NSHA told affected users in its notification letter that it believed that the access gained during the phishing attack "is often obtained so that users can send out spam e-mails." The belief that the attacker most likely only wanted to use the account to send out more messages was reiterated by the NSHA and ICTS during the review process.

[69] The NSHA could not provide any basis for this risk assessment or its statements about the likely motives of the attacker other than to say that this was the information provided by ICTS.

[70] In my view, these risk statements about the attacker's motives are unreasonable because they do not accord with what the information security industry has published about phishing attacks.

[71] Industry professionals warn that phishing attacks are on the rise and are most often aimed at gleaning sensitive information about the target, such as login credentials or other sensitive information. They indicate that phishing attacks are also associated with downloading malware (software designed to cause damage to the recipient's computer or network), or ransomware (software that locks and encrypts the recipient's computer or network files subject to receiving a payment in exchange for the keys to unlock the information).[29] They are often the work of organized syndicates of malicious actors.[30]

[72] Microsoft's most recent Security Intelligence Report[31] indicates that phishing attacks on its platforms increased by 250% between January and December 2018 and that phishing remains "one of the top attack vectors used to deliver malicious zero-day payloads to users." The report goes on to describe phishing attacks as varying "from targeted to broad-based, generic attacks. Although highly sophisticated attacks yield greater monetary gains per account phished, more generic attacks yield less money per compromised account but target a broader set of users."[32]

[73] The Information Systems Audit and Control Association (ISACA), which sponsors information technology security certifications programs and the Control Objectives and Information Related Technology (COBIT) framework for information technology governance, is a respected source of information technology standards and trends. ISACA has published

---

[29] Office of the Privacy Commissioner of Canada, "Recognizing threats to personal data online" https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/phishing/ (accessed December 13, 2019).
[30] Infosec, "Phishing Attack Overview" https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-attack-overview/ (accessed December 13, 2019).
[31] Volume 24, January – December 2018, https://www.microsoft.com/en-us/security/operations/security-intelligence-report (accessed December 18, 2019) at p. 20.
[32] Ibid., at p. 21.

numerous articles and blogs about the threat from phishing for nearly a decade. A certified auditor with the organization recently blogged about the risks and the increasing targeting of Microsoft's Office 365 email systems "because of the amount and value of the information contained within them."[33]

[74] The Canadian Centre for Cyber Security published from its 2018 National Cyber Threat Assessment that "cyber threat actors have both the intent and capability to acquire sensitive information." In its assessment, databases and aggregated data remain attractive targets for cyber threat actors seeking to sell information or support state-sponsored espionage. The assessment goes on to describe different types of data of interest to threat actors and that stolen information is often held for ransom, sold, or used to gain a competitive advantage.[34]

[75] Given what is known about the value of personal health information and what is known about attackers who perpetrate phishing attacks, it is not plausible, nor realistic to think that a malicious actor who gained access to an email account did so for the sole purpose of sending more phishing messages. It is not reasonable to conclude that the attacker did not also look around within the email account to steal any useful or valuable information.

[76] On a balance of probabilities, given all the circumstances, the risk assessment must conclude that the risk that the personal health information was stolen by the attacker is high.

[77] The cause and extent of this privacy breach is a high risk.

Scope

[78] This privacy breach affected 2841 identified individuals. This is a high number of affected individuals.

[79] Although it was only one email account compromised, the fact that it contained the identified personal health information of so many individuals aggregated into 95 machine-readable reports is significant. This is a large volume cache of valuable personal health information readily transported and utilized by malicious actors. This makes it an attractive target to the attacker that gained access to this email account.

[80] The scope of this privacy breach is a high risk.

Containment efforts

[81] ICTS worked quickly to secure the email account once it recognized the issue on May 13, 2019. Once the NSHA was alerted it took steps to determine what personal health information was contained in the email account and deployed its Privacy Breach Management Protocol.

[82] Another critical early containment step taken by the NSHA was to audit its medical records system, which is separate from the email system but relies on the same username and password. This was done to determine if there was any suspicious activity within that system using the compromised username and password. The audit process was repeated during the next

[33] https://www.isaca.org/resources/news-and-trends/isaca-now-blog published 7, January 2020.
[34] Canadian Centre for Cyber Security: "Data Breaches" and "Cyber Threats to Canadian Businesses" information sheets https://cyber.gc.ca/en/.

six months and a suspicious activity alert was placed on the user's access. No suspicious activity was discovered in the remainder of the medical records system stemming from the compromised username and password.

[83] The residual risk to the personal health information contained in the compromised email account is high. The NSHA consulted the provincial agency responsible for health card numbers who declined to issue new health card numbers to affected individuals citing that it has processes in place to monitor for fraudulent use of health card numbers.

[84] The NSHA did not take any steps to further contain the privacy breach. Further steps to contain the breach could take the form of monitoring whether the breached personal health information surfaces on the internet or the dark web or within markets for the sale of personal information.

[85] The initial containment steps taken were reasonable, but because of the unreasonable assumption about the motives of the attacker, the NSHA did not take additional reasonable steps.

Foreseeable harm from the breach

[86] The primary harm that is foreseeable from this breach is that the attacker stole the personal health information and will make it available for further malicious activity. The risk of further malicious activity is difficult to predict, even if it could be conclusively determined that the attacker stole the information. Stolen information can surface and cause harm even years later.[35]

[87] Based on what is known about those who perpetrate phishing attacks, it is reasonably foreseeable that the information will surface and be used for malicious purposes. The affected individuals must be made aware of the risk and how they can protect themselves. It is reasonable for the NSHA to take steps to address the risk of resurfacing and malicious use of the information.

Risk assessment conclusion

[88] I find that the NSHA's risk assessment relied on an unreasonable assumption about the attacker's motives. As a result, the NSHA did not properly assess the residual risk to individuals as high and did not take additional reasonable steps to contain the privacy breach.

Step 3: Notification

Notification required

[89] Section 69 of *PHIA* requires custodians to notify an individual at the first reasonable opportunity if the custodian believes on a reasonable basis that the information is stolen, lost, or subject to unauthorized access, use, disclosure, copying, or modification and as a result, there is potential for harm or embarrassment to the individual. *PHIA* does not specify what information must be provided to affected individuals. It only requires that individuals be notified if there is a privacy breach that has the potential for harm or embarrassment.

[35] https://arstechnica.com/information-technology/2020/02/four-plus-years-later-ashley-madison-hack-is-used-in-new-extortion-scam/ The type of extortion reported in this case is not the type of harm that could be anticipated if the information at risk in NSHA's privacy breach resurfaced. This example is provided only as an example of stolen information laying latent for years before resurfacing.

[90] The decisions of privacy commissioners across the country, including the Information and Privacy Commissioner for Nova Scotia, emphasize that the purpose of notifying affected individuals of a privacy breach is to allow affected individuals to take precautions to protect themselves.[36] To accomplish this purpose, the notification must provide affected individuals with accurate and sufficiently detailed information about the nature of the breach and the risks arising from the breach.

[91] Privacy is at its heart about trust. When privacy is breached, it damages trust between the person affected and the organization that was responsible for maintaining the privacy. The complainant submitted to this review that his trust in the NSHA was damaged by this privacy breach and by the letter of notification he received from the NSHA. The complainant found that the statements in the letter of notification were not believable and did not provide comfort that the privacy breach was properly handled or that a similar breach would be prevented in the future.

[92] The NSHA was guided in its notification to affected individuals by its Privacy Breach Management Protocol. The protocol states that the information included in a privacy breach notification "should help the individual reduce or prevent the harm that could be caused by the breach" and sets out the categories of information to be included.

Notification vague and inaccurate

[93] The NSHA notification letter does not provide the actual date of the breach or the length of time the email account was compromised. It provides the date that the NSHA was notified of the breach by ICTS. This was a vague and inaccurate account of the timeline of the privacy breach.

[94] The notification does not identify two critical risk assessment factors. First, it does not notify affected individuals that the NSHA audited the employee's account within the NSHA medical record system, which did not find any suspicious activity, and which concluded that the breach was limited to this one employee's email account. This is important contextual information to understand the extent of the breach and containment steps taken by the NSHA.

[95] Second, the notification does not clearly notify affected individuals that the personal health information was in the form of aggregated data reports belonging to many individuals attached to emails. These facts are also important for understanding the total context and risks from this incident.

[96] The complainant in this case specifically had concerns about the vague information provided. He described difficulty having follow up communication with the NSHA and difficulty determining specifically what personal health information of his was affected in this privacy breach.

[97] The complainant also specifically takes issue with the characterization of the incident as a "potential privacy breach". The NSHA notification letter describes the breach as a "potential privacy breach", that personal health information "may" have been accessed, and states that the

[36] Sobeys National Pharmacy Group (Re), 2018 NSOIPC 13 (CanLII); Department of Health and Wellness (Re), 2018 NSOIPC 12 (CanLII); Department of Internal Services (Re), 2019 NSPIPC 2.

unknown party's access to the email account "does not mean that anyone has gained access or viewed those mailbox contents." The notification did not provide any information about how affected individuals could protect themselves from potential harm from the privacy breach.

[98] The factors used to describe the breach as a "potential privacy breach" are factors relevant to the assessment of risk and potential for harm from the privacy breach. These factors do not erase the basic fact that the attacker enjoyed unauthorized access to the personal health information of the affected individuals over a five-day period and that the NSHA cannot confirm what the attacker did with the information.

[99] Privacy was breached the moment the attacker gained access to the employee's email account containing personal health information. By calling it a "potential" privacy breach, the NSHA perpetuated inaccurate and confusing information to affected individuals that appears to be designed to manage the message about the severity of the breach and the level of residual risk. It had the effect of undermining the purpose of providing affected individuals with accurate information about the privacy breach and how to protect themselves from harm.

[100] The NSHA developed a Key Messages document for staff tasked with responding to questions from affected individuals if they called following receipt of the notification letter. This document further demonstrates the NSHA's view of the privacy breach and its approach to notification if an affected individual questioned what was in the notification letter.

[101] No key messages conveyed any information about the risk that the information in this privacy breach was stolen by the attacker and what individuals should do to protect themselves from that reasonable possibility. The key message developed if an individual questioned the possibility of the information being misused was, "in the context of this situation we do not think there is a great risk for misuse of the information."

Notification not adequate

[102] The NSHA notification letter provided information that roughly falls into each of the categories set out in its Privacy Breach Management Protocol, but it did not accurately describe the breach that occurred and the residual risk. Some important information was not included.

[103] In my view, the NSHA attempted to convey to a large number of affected individuals that the risk from this privacy breach was low by using the language of "potential", "possible", and "may" to describe what happened and the risk. However, by taking this approach, and by not providing information for how individuals could protect themselves, the NSHA did not clearly describe the breach that occurred and did not convey a realistic assessment of the residual risk.

[104] The individuals affected by this privacy breach should remain on alert and on guard. Reliable information about the nature of malicious syndicates and organized criminals who perpetrate phishing scams could have assisted affected individuals to understand what the potential harm is and that they should remain on guard if they get unexpected solicitations from individuals who appear to have their personal health information. This information could also assist individuals to discuss with their family and friends to remain on guard if they get unexpected solicitations from individuals who appear to know personal information about the affected individuals.

[105] The residual risk may not require active credit monitoring for individuals because the information at risk was not financial information. However, the residual risk is also not such that no steps should be taken to mitigate the potential harm. The residual risk from this breach requires individuals be notified to remain alert to potential malicious activity and harm flowing from this privacy breach.

[106] For a notification to meet the purpose of notification required by s. 69 of *PHIA*, the custodian must transparently describe what occurred, what information was at risk, and in what form. The custodian must help the individual understand the factors leading to a final risk assessment. The steps taken to eliminate higher risk possibilities should be explicitly stated and specific information that can help an affected individual take steps to protect themselves must be provided.

[107] I find that the NSHA notification to affected individuals did not accurately describe the privacy breach that occurred, did not provide a realistic assessment of the residual risk to individuals, and did not provide individuals with useful information for how to protect themselves against the reasonable possibility of harm from the privacy breach. As such, the notification was not adequate to meet the purpose of providing notification under s. 69 of *PHIA*.

Does the NSHA have reasonable information practices in place for its email system as required by s. 62 of *PHIA*?

The standard of information practices required

[108] Custodians are required by s. 62 of *PHIA* to implement, maintain, and comply with information practices that:

(a) meet the requirements of this Act and the regulations;
(b) are reasonable in the circumstances; and
(c) ensure that personal health information in the custodian's custody or control is protected against
    i. theft or loss of the information, and
    ii. unauthorized access to or use, disclosure, copying or modification of the information.[37]

[109] In order to comply with s. 62(a) of *PHIA*, a custodian must consider s. 25 of *PHIA*, which requires that the minimum of amount of personal information be used in the course of the custodian's operations and providing of health services.

[37] *PHIA* s. 62(1).

[110] Further, in order to comply with s. 62(a) of *PHIA*, a custodian who maintains an electronic information system must also consider s. 65 of *PHIA*, which requires additional safeguards for an electronic information system.[38] The regulations require the custodian to implement the following additional safeguards for an electronic information system:

(a) protection of network infrastructure, including physical and wireless networks, to ensure secure access;
(b) protection of hardware and its supporting operating systems to ensure that the system functions consistently and only those authorized to access the system have access; and
(c) protection of the system's software, including the way it authenticates a user's identity before allowing access.[39]

[111] The regulations further require a custodian to create and maintain written policies to support and enforce the implementation of the safeguards required by the regulations.[40]

What are reasonable information practices that ensure personal health information is protected?

[112] The contextual factors generally acknowledged by Canadian information and privacy commissioners and adopted within Nova Scotia are set out below.[41] I adopt these considerations in the analysis that follows.

1. **Contextual:** Reasonable information practices and reasonable security are 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.[42] Generally, personal health information is viewed as being among the most sensitive of personal information.
3. **Not technically prescriptive:** Reasonable information practices and reasonable security are 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.[43]
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.[44]
5. **Trust:** For custodians delivering health care services, reasonable information practices and reasonable security also include reasonable assurances to the public that privacy protections are given serious attention. The risk of broken trust in the health care setting

[38] *PHIA* s. 65.
[39] *PHIA* Regulation 10(1).
[40] *PHIA* Regulation 10(2).
[41] Sobeys National Pharmacy Group (Re), 2018 NSOIPC 13 (CanLII); Department of Health and Wellness (Re), 2018 NSOIPC 12 (CanLII); Department of Internal Services (Re), 2019 NSPIPC 2.
[42] *Electronic Health System (Re)*, 2010 BCIPC 13 (CanLII) at para 130.
[43] *Electronic Health System (Re)*, 2010 BCIPC 13 (CanLII) at para 129.
[44] BC Investigation Report F06-01; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order H2005-IR-001.

is that individuals may avoid seeking medical treatment. This creates a high standard for custodians to ensure information practices and security measures to protect personal information 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 service provider is following industry standards or blindly accepting third party expertise does not demonstrate reasonable security.[45]
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. However, a custodian cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable measures in another.[46]
8. **Life cycle:** Information practices and reasonable security apply to the entire life cycle of the records.
9. **Format:** The medium and format of the records will dictate the nature of the physical, technical, and administrative safeguards.
10. **Timing:** Reasonableness requires a proactive and speedy response to known or likely risks.[47] Time is of the essence in any privacy breach. The safeguards must ensure that should a privacy breach occur, the custodian and the individual will learn of the breach and have response measures in place quickly and efficiently.[48] The generally accepted components of managing a privacy breach are containment and investigation, risk assessment, notification, and prevention.
11. **Documentation:** Procedures for establishing information practices and reasonable security must be documented and custodians must be prepared to respond to the idea that employees won't always follow the documented procedures.[49]

The NSHA's information practices following this privacy breach

NSHA awareness campaign prevention strategy

[113] The NSHA's prevention work following this privacy breach focused on education strategies. The individual employee involved in this incident was provided one-on-one training about phishing activities and email hygiene practices to securely destroy email messages that are no longer needed.

[114] On June 5, 2019, the NSHA sent a memo via an organization-wide newsletter alerting all email users of the fact that phishing emails had been reported within the NSHA and warning them of the risks.

---

[45] Ontario Order MC09-9; BC Investigation Report F06-01.
[46] BC Investigation Report F06-01.
[47] BC Investigation Report F06-01; Alberta Order P2013-04; BC Investigation Report F12-02.
[48] Alberta Order H2005-IR-001.
[49] Alberta Order H2005-IR-0010; Ontario Order HO-001; BC Investigation Report F06-01; Alberta Order P2010-008.

[115] The organization-wide message was followed up further on June 11, 2019, by launching a targeted phishing education awareness campaign. The campaign included the tag line "Don't Get Reeled in by Phishing Scams" and provided information about what phishing is and common signs that an email or text message is a phishing attempt. The campaign also included providing NSHA employees with a central email address where they can forward any suspected phishing messages they receive. This allows for cyber security safeguards to check the message for malware or ransomware, identify if it is false, and block the sending address if it is.

[116] The NSHA's phishing awareness campaign has catchy phrasing and engaging graphics. Ensuring employees are aware of the risks of phishing and how to detect it is very important, particularly if the NSHA is going to continue to use email to transact personal health information.

Electronic Messaging of Personal Health Information policy – alternatives to email

[117] The NSHA relies heavily on email for its operations. In its representations for this review, the NSHA stated:

> "Given the provincial nature of our [NSHA] structure, the large number of employees, students, and physicians who utilize our systems on a daily basis (+/- 30,000) and over 5 million patient encounters on a yearly basis (not including over 3 million Primary Care visits or Continuing Care services), it would not be reasonable in these circumstances to expect that PHI not be present in our Microsoft Outlook e-mail system. Without Outlook the people providing care to Nova Scotians and the people supporting those care providers would not be able to perform their work in a timely and efficient manner." [emphasis in original]

[118] In May 2019, the NSHA implemented, its Electronic Messaging of Personal Health Information policy as an administrative safeguard to protect personal health information. In its notification letter to affected individuals, the NSHA stated that "communication of personal health information via e-mail is a standard practice which was recently formalized by NSHA's Electronic Messaging of Personal Health Information policy."

[119] The circumstance of running a busy provincial health services system is important to consider and if there is no alternative for the efficient communication and coordination that email provides, it may not be reasonable to expect there to never be any personal health information in the email system. However, where other safeguards or alternatives exist that can minimize the presence of personal health information within an email system and minimize copies of personal health information being stored unnecessarily in email accounts, they must be utilized.

[120] The NSHA's Electronic Messaging of Personal Health Information policy recognizes there is a risk to using email to convey personal health information.[50] The policy sets out a guiding principle that "E-Messaging use needs to be balanced with the risks it can pose to the privacy of individuals and to the security of their PHI. These need to be considered prior to using E-Messaging to determine if the benefits outweigh the risks."

[50] Electronic Messaging of Personal Health Information at Policy Statement 3.

[121] The policy appears to set up a framework within which decisions are made to use lower risk alternatives to email where possible and to convey only the minimum amount of personal health information via email.

[122] One alternative available to the NSHA is its secure file transfer system which allows sensitive information to be conveyed via a secure VPN (Virtual Private Network). The system grants the recipient a link to access and download documents which expires after a set period of time. Unlike email attachments sitting in an email account, there is no extra copy of files sitting in the conveyance system after it has been delivered and downloaded and the attachment does not enter the email account or the email transmission system.

[123] Another alternative available to the NSHA is its shared network file system where users at different locations can access and store documents on shared network folders protected by the digital security infrastructure without engaging the email system. This system effectively allows the sharing of data and documents within the NSHA without having to send documents via email.

[124] The NSHA did not fully take the opportunity of this privacy breach incident to review its practices for consistency with its Electronic Messaging of Personal Health Information policy. In its notification to affected individuals, the NSHA called the communication of personal health information via email, including the types of reports exposed during this privacy breach, "standard practice".

[125] In an internal email following the privacy breach, the following statement was made:

> "In addition to an education push on Phishing that will need to occur there also needs to be a push on cleaning up ones inbox to remove PHI that is no longer required. If reports need to be saved they should be saved in network drives.
>
> Further to that we will need to consider in general how we use and share reports containing PHI as an organization. This is a huge source of risk for breach whether they are printed or emailed and over the years the mishandling of lists has been the source of many breaches, often containing sensitive PHI. If there are ways to work differently in the future that could greatly reduce the need for these lists those options should be explored."[51]

[126] Based on this statement, the NSHA has identified ongoing challenges with maintaining the security of lists of aggregated personal health information. Despite this recognition, the NSHA told affected individuals that it is standard practice to continue sending these lists via email. The NSHA provided no clear plan or steps taken to improve its information practices in relation to aggregated lists of personal health information. It did not provide evidence that it has quantified how widespread is the practice of using email to send aggregated data, reports, and attachments with personal health information across the NSHA's operations.

[51] Submitted by the NSHA.

[127] The NSHA's response to this privacy breach does not demonstrate the application of the guiding principles of its policy. The continuing practice of sending aggregated reports and data containing personal health information via email when lower risk options are available is not a reasonable information practice within the meaning of s. 62 of *PHIA*.

Electronic Messaging of Personal Health Information policy – deleting emails

[128] Given its heavy general reliance on email for communication, the NSHA's Electronic Messaging of Personal Health Information policy sets out a procedure that emails containing personal health information must be deleted after they are no longer required.[52] This procedure recognizes the risk of leaving personal health information in an email account and the lack of authority under *PHIA* to store personal health information within an email account without a purpose.[53] However, the NSHA's records retention policies do not consistently support this procedure as a safeguard.

[129] The NSHA currently has multiple retention policies applicable to different types of records and emanating from the former regional health authorities. The policies have similar provisions in defining "transitory records" as records that have a temporary period of usefulness. An email that is no longer needed once it has conveyed the information it was designed to convey or has been saved somewhere else meets the definition of a transitory record. The retention policies permit transitory records to be disposed of through appropriate means but do not require it.

[130] The inconsistency between the Electronic Messaging of Personal Health Information policy and the records retention policies on whether users are required to or just permitted to securely destroy emails containing personal health information once they are no longer required creates confusion.

[131] In its notification letter to affected individuals, the NSHA stated that a prevention step implemented following this privacy breach was to "put forth a recommendation that all employees review and remove historic mailings from within their mailboxes on a regular basis." Since that time, the NSHA has formalized this recommendation by updating its Privacy Policy and sending a memo to all NSHA email users on February 14, 2020, clarifying that they must delete messages containing personal health information from their email accounts once they are no longer required. It is not clear from this memo if email users will understand that secure destruction requires deleting emails from the account folders and then also emptying the "deleted emails" folder.

[132] The revised Privacy Policy and memo to email users remain inconsistent with the NSHA's records retention policies on the issue of the requirement to securely destroy email messages containing personal health information once they are no longer required. Policies should provide consistency, particularly when action is required. The inconsistency of the records retention policies does not demonstrate a reasonable information practice within the meaning of s. 62 of *PHIA*.

[52] Procedure 1.1.4.
[53] *PHIA* s. 25.

NSHA email practices not reasonable under PHIA

[133] For information practices to be reasonable within the meaning of s. 62, they must also comply with the requirements of *PHIA* and its regulations. *PHIA* places the responsibility on a custodian to implement additional safeguards to an electronic information system and the regulations require that a custodian maintain written policies to support and enforce the implementation of the safeguards.[54] *PHIA* also requires that a custodian use only the minimum amount of personal information at any time.[55]

[134] The NSHA has a standard practice of using email to convey aggregated data and reports containing personal health information when other lower risk options are available. This practice does not appear to comply with the NSHA's Electronic Messaging of Personal Health Information policy and resulted in 2841 individuals' sensitive personal health information being exposed to an attacker in this case.

[135] The NSHA has taken some steps to resolve inconsistency in the policy and practice about whether users are required to securely destroy email messages containing personal health information after they are no longer needed. The longstanding practice, and the NSHA's internal communication, demonstrates that there is an ongoing risk of large caches of personal health information sitting in NSHA email accounts.

[136] The NSHA must anticipate that phishing will be successful again in the future and must work to minimize the personal health information within email accounts, especially large caches of personal health information aggregated into machine-readable formats which pose a high value target for information thieves. This privacy breach highlights two key information practices that expose personal health information to risk and are not adequately addressed by the NSHA's safeguards.

[137] I find that two of the NSHA's information practices, the practice of using email to deliver aggregated data and reports containing personal health information when other lower risk options are available, and the inconsistent policies and practices on the secure destruction of messages containing personal health information in email accounts after they are no longer needed, are not reasonable information practices within the meaning of s. 62 of *PHIA*.

FINDINGS & RECOMMENDATIONS

Privacy breach containment and investigation

[138] I find that the safeguards in place failed to act at the first signs of the compromised email account and the NSHA's investigation failed to obtain critical evidence necessary to assess appropriate containment action and the risks from the privacy breach.

[54] *PHIA* s. 65; Regulations 10(2)
[55] *PHIA* s. 25.

[139] **Recommendation #1:** I recommend that within 30 days of accepting this recommendation, the NSHA establish written and specific service standards and protocols required of its network service providers to ensure:

- quicker response to signs of cyber threats,
- that the NSHA will be always be immediately notified of a security breach,
- all evidence relevant to a privacy breach investigation will be maintained and provided to the NSHA immediately, and
- realistic and informed risk assessments will be performed.

Privacy breach risk assessment

[140] I find that the NSHA's risk assessment relied on an unreasonable assumption about the attacker's motives. As a result, the NSHA did not properly assess the residual risk to individuals as high and did not take additional reasonable steps to contain the privacy breach.

[141] **Recommendation #2:** I recommend that beginning immediately, the NSHA monitor whether the personal health information at risk in this privacy breach surfaces on the dark web or within the markets for trading in personal information for a minimum of two years.

Privacy breach notification to individuals

[142] I find that the NSHA's notification to affected individuals did not accurately describe the privacy breach that occurred, did not provide a realistic assessment of the risks to individuals, and did not provide individuals with useful information for how to protect themselves against the reasonable potential for harm from the privacy breach. As such, the notification was not adequate to meet the purpose of providing notification under s. 69 of *PHIA*.

[143] **Recommendation #3:** I recommend that within 30 days of accepting this recommendation, the NSHA provide a revised notification to the affected individuals to correct the deficiencies in its first notification.

NSHA information practices following the privacy breach

[144] I find that two of NSHA's information practices, the practice of using email to deliver aggregated data and reports containing personal health information when other lower risk options are available, and the inconsistent policies and practices on requiring email users to securely destroy personal health information in email accounts after they are no longer needed, are not reasonable information practices within the meaning of s. 62 of *PHIA*.

[145] **Recommendation #4:** I recommend that the NSHA immediately end the practice of using email to deliver system-generated reports and other aggregated reports or data containing personal health information within the NSHA or between the NSHA and outside parties.

[146] **Recommendation #5:** I recommend that within 30 days of accepting this recommendation, the NSHA initiate an awareness campaign to highlight to NSHA email users that they are required to securely destroy emails containing personal health information once they are no longer needed and to prompt users to immediately remove the caches of personal health information stored unnecessarily in their email accounts.

[147] **Recommendation #6:** I recommend that within six months of accepting this recommendation, the NSHA revise its records retention policies to be consistent with the Electronic Messaging of Personal Health Information policy by requiring the secure destruction of transitory records containing personal health information after they are no longer required.

February 26, 2020

Janet Burt-Gerrans
Director of Investigations and Mediation (acting)
Office of the Information and Privacy Commissioner for Nova Scotia

OIPC File Number: 19-00344