OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

P-2023-001/PH-2023-002

May 23, 2023

Newfoundland and Labrador Centre for Health information, Eastern Health Authority, Labrador-Grenfell Health Authority, and Central Health Authority

(now combined into the Provincial Health Authority)

AND

Department of Health and Community Services

EXECUTIVE SUMMARY

The 2021 cyber attack was by far the largest of its kind ever experienced in this province, and one of the largest in Canadian history to date, in terms of the number of people whose information was stolen, and the impact that it had across the health system.

Some members of the public may be under the impression that they were not impacted by the cyber attack if they did not receive direct notification by mail. This is not the case. While **over a hundred thousand individuals were directly notified**, for a variety of practical reasons, the remaining notifications were instead issued through various public channels, including media briefings and websites. For the sake of greater clarity, it bears repeating that the following groups of people had their patient information accessed and taken in the cyber attack who may not have received a direct notification letter:

- Patients of Central Health from 2006-2021;
- Patients of Labrador-Grenfell Health from 2013-2021;
- Patients of Eastern Health from 2010-2021;
- All patients across our province who had their blood work/specimens sent to Eastern Health for specialized testing from 2010-2021; and
- All patients who had COVID-19 testing within and across our province (up to 2021).

All current employees of the impacted Regional Health Authorities were notified by their employers that their personal information was stolen in the cyber attack, as well as those whose employment concluded within approximately 14 years prior to the attack. Labrador Grenfell did not retain employee information past 8 years, so it was able to send notification to all its impacted former employees. Central Health and Eastern Health determined that the contact information in their possession for people who ended their employment long ago was unlikely to be reliable, so the following groups of former employees were also notified solely via the public notification channels noted above:

- Eastern Health Past Employees (~1993 - 2006);
- Central Health Past Employees (~1993 - 2007).

To put this in context, it is likely that the vast majority of the population of the province had some amount of personal information or personal health information taken by the cyber attackers, although the specific number may never be known.

In March 2023, the Government of Newfoundland and Labrador released its Report which outlines the events in October and November of 2021 and subsequent actions in response to the cyber attack. That report is available publicly, and key details of it are quoted in this Report. The purpose of this Report is not merely to repeat those details, however. The purpose of this Report is to carry out our statutory mandate, having investigated the breach of privacy involving the theft of personal health information and personal information resulting from the cyber attack, in accordance with the *Personal Health Information Act* (*PHIA*) and the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*).

Our role in this matter is grounded in our independence as a Statutory Office of the House of Assembly. As such, we do not report to a Minister, and political considerations do not impact how we carry out our duties. While the Report issued by Government in March 2023 is important and useful, with the issuance of this Report the public can be assured that an *independent* body has, within the powers and jurisdiction available to it, investigated this matter and published a report of its findings and recommendations.

There were two areas of focus for this investigation. The first was the response to the breach: did the Newfoundland and Labrador Centre for Health Information and the impacted Regional Health Authorities (Central Heath, Labrador-Grenfell Health, and Eastern Health) respond effectively to the cyber attack in compliance with their statutory obligations? In this respect, we made a number of key findings, as well as recommendations. We found for example, that while the breach response was by and large carried out well, some details about the nature of the breach were not disclosed at the first reasonable opportunity, as required by law. It should also be noted that the Department of Health and Community Services took on a significant role particularly as it relates to what information was disclosed to the public and when. There are a number of findings and recommendations in relation to this aspect of the investigation, including:

- The length of time that elapsed prior to the public being notified of this being a ransomware cyber attack is concerning, and the rationale provided for such a delay was insufficient to justify it.
- The Department of Health and Community Services' role in overseeing and managing public notifications and the Centre for Health Information's role in investigating the cyber attack and resulting privacy breach were reasonable in the circumstances.
- The public was not informed of this being a ransomware cyber attack, nor of this attack being perpetrated by the HIVE ransomware group at the first reasonable opportunity.
- Notifications about the privacy breach should have included more details about the nature of the attack, namely that it was a ransomware cyber attack together with other general details, such as confirmation that a Threat Actor exfiltrated/stole data containing personal information and/or personal health information for malicious purposes.
- The necessary forensic investigations were conducted to determine, to the extent possible, the root causes of the privacy breach and the cyber attack as a whole.

The second area of focus relates to the security and information practices of the Centre for Health Information and the impacted Regional Health Authorities, the questions being focused on whether those entities had reasonable security and information practices in place at the time of the cyber attack as required by *ATIPPA* and *PHIA*. The biggest question at the outset of this investigation for us was whether this cyber attack succeeded despite these entities having cyber security practices that met recognized international standards, or if it succeeded because those standards were not being met at the time. Unfortunately, we found the latter.

Our assessment concluded that the security of our health information system, at the time of the attack, was lacking in a number of important areas, and internationally recognized, industry-standard cyber security measures were either not in place or not fully implemented,

leaving the personal health information and personal information of citizens of the province vulnerable to cyber attack, which, under the circumstances, was almost an inevitability. Furthermore, these vulnerabilities were known within the health care system, but there was a failure to take sufficient and timely steps to remedy them, accountability for which is shared among the parties. Some key findings and recommendations flowing from this aspect of the investigation are:

- The personal health information and personal information taken in the cyber attack was highly sensitive information that deserved the highest degree of protection.
- A high impact ransomware attack against our province's health care information systems was foreseeable.
- In the circumstances, in light of the sensitivity of the information and the foreseeability and likelihood of significant harm to privacy that could result from a cyber attack, the Centre for Health Information, Eastern Health, Central Health, and Labrador-Grenfell Health did not have reasonable security arrangements in place to protect personal health information and personal information at the time of the cyber attack, contrary to section 15(1)(a) of *PHIA* and 64(1)(a) of *ATIPPA, 2015*.
- Subsequent to the cyber attack, reasonable cyber security steps have been and are being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack.

One of the things you will note from this Report is that while there are 34 findings, there are only six recommendations. That is due to the fact that an impressive amount of work has been done subsequent to the cyber attack, and is being continued, to ensure that appropriate cyber security measures are in place across the health information system. If we had found those measures lacking, we would have made recommendations to that effect, however we are pleased to say that much progress has been made. A crucial consideration, however, is that this is not a one-time fix. Cyber security is an ongoing project, and it is essential that sufficient focus and resources continue to be directed to this task.

Even though much progress has been made in preventing and mitigating the impact of future cyber attacks, an important purpose of this Report is to ensure that accountability for the cyber attack is assigned appropriately. One of the challenges with this investigation has been that there are multiple public bodies/custodians involved who were either empowered or restrained in carrying out their roles due to a web of statutory obligations overlaid by a Ministerial directive and an unsigned agreement. For the purposes of this Report, however, the accountability that matters is within the context of *ATIPPA, 2015*, and *PHIA*, the statutes that this Office has responsibility for overseeing. Accordingly, the accountability for this event is shared by the Centre for Health Information as well as Eastern Health, Central Health, and Labrador-Grenfell Health. Ultimately, however, leadership of the entire health care system falls to the Department of Health and Community Services, and it is the Minister who must ensure that the new Provincial Health Authority has the appropriate resources and direction so that cyber security within our health care information system meets internationally recognized industry-accepted standards, thereby ensuring to the extent possible that the personal health information and personal information of the people of this province is protected against future cyber attacks.

STATUTES CITED

Access to Information and Protection of Privacy Act, 2015, S.N.L. 2015, c. A-1.2, sections 63 (accuracy of personal information), and 64 (protection of personal information).

Personal Health Information Act, SNL 2008, c. P-7.01, section 13 (information practices, policies and procedures), 15 (security), 16 (duty to ensure accuracy of information), 29(3) (Collection of personal health information with consent) and 32(1) (scope of collection).

Personal Health Information Regulations, NLR 38/11, section 5 (material breach).

Management of Information Act, SNL 2005, M-1.01, section 6 (system for management of information).

AUTHORITIES RELIED ON

NL OIPC Reports: Report P-2008-001; Report P-2008-003; Report P-2009-001.

NS OIPC Reports: Review Report 20-02; Investigation Report IR19-01; Investigation Report IR23-01.

SK OIPC Reports: Report 103-2017; Report 009-2020, 053-2020, 224-2020.

AB OIPC Reports: P2022-ND-048; P2022-ND-060; P2022-ND-063; P2022-ND-065.

NWT OIPC Reports: Review Report 18-189, Review Report 19-HIA14.

PEI OIPC Report: Report HI-18-005.

BC OIPC Report: Investigation Report F06-01; Investigation Report F10-02; Investigation Report 22-02.

OTHER RESOURCES

Access to Information Policy and Procedures Manual, December 2021 from Government of Newfoundland and Labrador, Department of Justice and Public Safety; *Protection of Privacy, Privacy Breach Protocol*, March 2015 from Government of Newfoundland and Labrador, ATIPP Office, Office of Public Engagement.

Table of Contents

I. MESSAGE FROM THE COMMISSIONER'S DELEGATE

[1] A report such as this must be both retrospective and prospective. While we spent a great deal of time focusing on what happened and why, we also examined the important work that has been done subsequent to the cyber attack, and what measures are being put in place or should be put in place to prevent such a massive, impactful event from occurring again in the future.

[2] Reflecting on how things were prior to the event, in summary it can be said that there were vulnerabilities in the cyber security of our health care system that made the cyber attack possible, and that allowed its impact to be as broad as it was. It was not a situation where the attack succeeded despite there being reasonable security measures across the board, because those measures were lacking. In fact, those vulnerabilities were known to the Newfoundland and Labrador Centre for Health Information prior to the attack, in a context where the threat of cyber attack was known to be an ever-increasing risk by those in the information security field. Indeed this ransomware phenomenon was publicly notorious through widespread reporting in the news media, and should have been a more prominent item on the radar of those in leadership throughout the health care system. Under the circumstances, it was all but inevitable that we would be targeted.

[3] There were mitigating factors. Clearly, the pandemic drew the resources and attention of our health care system towards meeting the urgent needs that arose, particularly in its early stages. That would certainly have made it difficult to make the necessary progress on cyber security during that period. However, the vulnerabilities noted above were known prior to the pandemic and progress during that period was insufficient. The implementation of Shared Services by the Minister of Health and Community Services, which placed the Centre for Health Information in charge of information technology and information security for all of the Regional Health Authorities, was part of the context within which this occurred as well. Shared Services represented an opportunity to bring all of the Regional Health Authorities up to the same standard in terms of cyber security – an admittedly huge undertaking which was insufficiently prioritized.

[4] What we have learned about efforts subsequent to the cyber attack to improve cyber security is much more encouraging. A great deal of important work has progressed to strengthen the security of our health information systems so that future attacks of this magnitude will be less likely to occur, and if they do occur, they should be less impactful. Make no mistake, however, that this is not a one-time fix. Bolstering security in the short term only to see it lag again over the medium to long term will see us just as vulnerable as we were in 2021, and that is not an acceptable option.

[5] While governments and corporations around the world are becoming better prepared to prevent cyber attacks, there is every indication that phishing and other sophisticated social engineering attack vectors will become more advanced over time, particularly given the capability of artificial intelligence large language models (LLMs) to design ever more insidious means to breach our defenses. This is and will continue to be an ongoing arms race with organized crime as well as state-sanctioned actors who will not only attempt to extort us and breach our privacy but also cause us to incur significant costs to the public purse and harm actual health care delivery, potentially putting lives at risk by interrupting patient care.

[6] The health care system that we have designed and continue to develop, with electronic personal health information as its lifeblood, is the patient we are caring for. That data must continue to flow to those who need it, when they need it, unimpeded by cyber attackers, and importantly, with the trust of the people of this province that it will be appropriately protected and only collected, used or disclosed in accordance with the law.

[7] It has been said many times before that one should never waste a crisis. Indications are good so far that important lessons have already been learned. However, those lessons must be fully integrated into the underlying philosophy and operational mandate of the entire health care system, not only in word, but indeed. There will be financial costs of course, but there are also financial costs if we fail. There are also many other costs, which are more difficult to quantify, and those are the costs associated with public trust. It is hoped that this Report, by shedding light on the many relevant considerations and factors associated with the 2021 cyber attack and how our health care organizations responded to it and are working to prevent future such attacks, will help to restore some of that public trust.

[8] The primary purpose of this Report and the laws that underpin it is the protection of the personal information and personal health information of the people of this province, and that is our ultimate focus. I would be remiss, however, if I did not acknowledge the immense challenge that the cyber attack posed to the people who run our public sector health care system, from the front line employees and managers to the executives and political leadership. This was an extremely difficult time for all concerned, and their hard work in responding to this challenge deserves recognition.

[9] I also wish to acknowledge the advice and support provided at the outset of this investigation by the Office of the Privacy Commissioner of Canada, whose officials were generous in sharing their insights and practical suggestions as we prepared to launch the largest investigation ever conducted by this Office. Further, as noted in this Report, we engaged expert consultants to assist us in interpreting the technical aspects of our subject matter, and we thank them for their tremendous contribution.

[10] Finally, I wish to thank staff of the Office of the Information and Privacy Commissioner for Newfoundland and Labrador, whose dedication, determination, perseverance, and excellence made this Report possible.

II. SCOPE OF OIPC INVESTIGATION

[11] It is anticipated that some readers of this Report will be unfamiliar with our Office: who we are, what we do, and what we can and cannot investigate. The Office of the Information and Privacy Commissioner (our "**Office**" or "**OIPC**") is an independent statutory office of the House of Assembly, which means that it was created by legislation[1] and is independent from the executive branch of government. The Commissioner is an Officer of the House of Assembly.

[1] *ATIPPA, 2015*, whose full title is the *Access to Information and Protection of Privacy Act, 2015* is the statute that establishes the Office of the Information and Privacy Commissioner and charges the Commissioner with upholding compliance with the *Act* by public bodies in the Province. *PHIA*, whose full title is the *Personal Health Information Act* is the other law that we are charged with upholding, and it applies specifically to information in the health sector, and to the custodians who hold it in trust for the people of the Province.

[12] The things that our Office *can* or *must do* are set out in the *Personal Health Information Act* (*PHIA*) and the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*). This means that all of the powers and duties we exercise must specifically be included in those statutes, but equally importantly, we cannot do anything outside of the our statutory mandate.

[13] While our Office does many things, one of the most important things we do is investigate privacy breaches involving public bodies subject to *ATIPPA, 2015* or custodians subject to *PHIA*. Our role is to oversee compliance with those laws, and through the issuance of reports such as this, to hold public bodies and custodians accountable if they fail in their compliance efforts, to make recommendations for improved compliance, and also to point out where they have succeeded, if warranted. The reason our Office is investigating the 2021 cyber attack is because this attack resulted in the largest privacy breach in our province's history and involved the above named public bodies and custodians. As discussed later in this Report, public bodies and custodians are obligated to take reasonable steps to protect personal information and personal health information; this includes taking reasonable cyber security measures to prevent and mitigate the impact of a cyber attack.

[14] The cyber attack caused vast disruptions to our province's health care services and resulted in millions of government dollars being spent[2]. Our Office *did not* conduct an investigation into the extent of any health care disruptions or costs incurred from the cyber attack, because those aspects are beyond what our legislation says we can investigate.[3] This Report provides an overview of our investigation, our findings, and makes recommendations that relate to the privacy breaches that occurred as a result of the cyber attack.

[2] Examples of Media Articles referencing some costs*: N.L. cyberattack costs approach $16M, health minister says | CBC News*; and *$200K public relations aid for N.L. cyberattack didn't result in transparency, says expert | CBC News*.

[3] For an example of a broader scope post-incident review regarding a health system cyber attack, see Conti cyber attack on the HSE - Independent Post Incident Review, conducted by PricewaterhouseCoopers, commissioned by Ireland's Health Services Executive following a cyber attack on Ireland's health care system.

III. BACKGROUND

a. THE ENTITIES INVOLVED

[15] On April 1, 2023 our province's four Regional Health Authorities, namely Eastern Health Authority, Labrador-Grenfell Health Authority, Central Health Authority, and Western Health Authority, together with the Newfoundland and Labrador Centre for Health Information were all integrated into one Provincial Health Authority[4] which has been named "Newfoundland and Labrador Health Services"[5] (the "**Provincial Health Authority**"). The events leading up to the cyber attack, the cyber attack itself, and the majority of responses to the cyber attack took place while these entities were wholly separate. As such, this Report is primarily written from that perspective, with the exception of our recommendations, which are directed to the Provincial Health Authority.

[16] As described in its Annual Report, the Department of Health and Community Services (**"the Department"**):

> *is responsible for the overall strategic direction and priorities for the health and community services system throughout Newfoundland and Labrador…In keeping with its mandate, the [D]epartment works to provide leadership, coordination, monitoring and support to the regional health authorities (RHAs) and other entities that deliver programs and services. The [D]epartment also ensures the quality, efficiency and effectiveness of the healthcare system…*[6]

[17] The Minister of Health and Community Services has the authority to direct, control, and approve funding for a number of different entities, including the Regional Health Authorities[7] and the Newfoundland and Labrador Centre for Health Information[8].

---

[4] See the *Provincial Health Authority Act*, RSNL 2022, c. P-30.1.
[5] This name was announced on April 3, 2023 in the Department's news release.
[6] See the 2020-2021 Annual Report of the Department of Health and Community Services.
[7] At the time of the attack, the Department (Minister) had the power to exercise this authority under sections 3 to 5 in the *Regional Health Authorities Act*, SNL 2006, c R-7 and section 4 of the Department's Regulation *NLR 98/19*. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which includes all Regional Health Authorities) per sections 3 to 5 of the new *Provincial Health Authority Act*.
[8] At the time of the attack, the Department (Minister) had the power to exercise this authority under section 5 of the *Centre for Health Information Act*, SNL 2018, c. C-5.2. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which now includes the Centre) per sections 3 to 5 of the new *Provincial Health Authority Act*.

[18] Our province's health care services are largely implemented by our four Regional Health Authorities: Eastern Health Authority ("**Eastern Health**"), Central Health Authority ("**Central Health**"), Labrador-Grenfell Health Authority ("**Labrador-Grenfell Health**") and Western Health Authority ("**Western Health**"). The Regional Health Authorities collect and store a variety of personal health information in order to perform these health care services. As employers the Regional Health Authorities also collect and store the personal information of staff for employment purposes.

[19] In an effort to achieve greater efficiency and potentially decrease costs of an already financially burdened health care system, the Minister of Health and Community Services made the decision[9] for our province to move to an eHealth shared services model ("**Shared Services**"). On October 2, 2019, as part of Shared Services, the entity known as the Newfoundland and Labrador Centre for Health Information (also known by its acronym "*NLCHI*" and referred to as "***the Centre***" in this Report) became solely responsible for the information technology and information security of our province's four Regional Health Authorities,[10] a move that resulted from a directive of the Minister in October 2017.

[20] Prior to Shared Services, the Centre was responsible for a wide variety of functions. The Centre functioned to provide quality information to health professionals, the public, researchers and health system decision-makers. As described in earlier Annual Reports it also played a large role in some technical and data based projects:

> *Through collaboration with the health system, the Centre supports the development of data and technical standards, maintains key health databases, prepares and distributes health reports, provides data extraction and linkage*

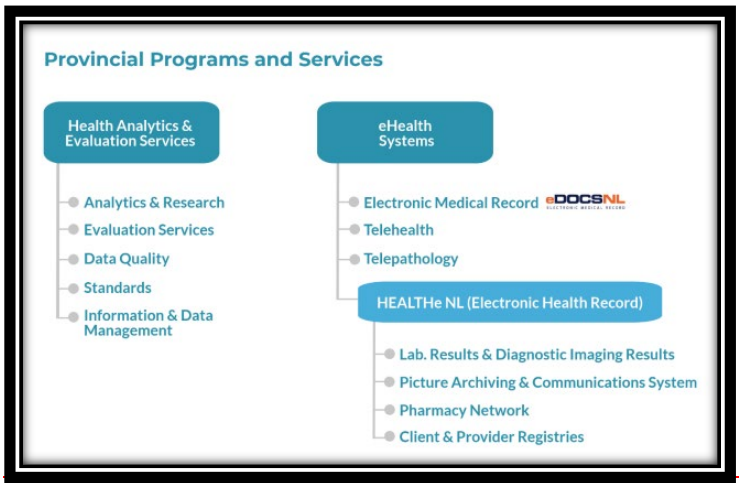
---

[9] October 4, 2017 News Release *Minister Haggie Announces Approach to Develop a Shared Services eHealth Model;* This decision was based upon the Healthtech Consultant's report provided to the Department of Health and Community Services titled *Newfoundland and Labrador eHealth Review* dated March 19, 2017. This report recommended the province "Create a new provincial eHealth model combining IT&T functions from the four regional health authorities and the entire functionality of the Newfoundland and Labrador Centre for Health Information" and detailed a number of next high-level steps to achieve this recommendation. A number of factors were listed as being "Critical Success Factors" one of which was to "Ensure Privacy Protection is a foundational building block," stating "… the inclusion of privacy and security as a major component of the eHealth model is required so that privacy of personal and personal health information is an overarching priority."

[10] In a letter dated October 5, 2017 from the Minister of Health and Community Services to the Board Chair of the Centre, the Minister outlined decisions made with respect to moving towards shared services and confirmed that agreements would need to be entered into in an effort to address things like roles, responsibilities, privacy, etc. amongst the Centre and the Regional Health Authorities; In 2018 the Centre's mandate was expanded through its legislation (see its "Objects" as set out in section 4 of the old act vs. the new act for comparison).

> *services to support health research and conducts analytic and evaluation projects…The Centre's mandate includes the development of HEALTHe NL, a confidential and secure provincial electronic health record (EHR). This work includes the change management required to support adoption by end user clinicians. The Centre is also developing the provincial electronic medical record (EMR), and is involved in the planning, design and implementation of specific provincial health information systems.*[11]

[21] Taken from the Centre's 2018-2019 Annual Report, here is a visual representation of the programs and services provided by the Centre prior to Shared Services:



[22] Prior to Shared Services, the Centre did all of the above and more, as well as being responsible for its own information technology and security. After the move to Shared Services, the Centre continued to perform all of its previous functions, and it was still responsible for its own information technology and information security. However, Shared Services resulted in the Centre *also* becoming responsible for the information technology and information security of all four Regional Health Authorities. This move to Shared Services resulted in the Centre inheriting responsibility over a vast and fragmented IT landscape, comprising hundreds of physical locations, together with thousands of workstations, software applications, network devices, and servers, which store our province's most sensitive information.

[11] Examples of older Annual Reports from the Centre explaining the role of the Centre prior to shared services: 2016-2017, 2017-2018 2018-2019; As per the Centre's 2019-2020 Annual Report, its mandate was expanded to include providing IT services to the Regional Health Authorities.

b. Launch of OIPC Investigation Into Cyber Attack

[23] *ATIPPA, 2015* and *PHIA* provide our Office with the statutory authority to investigate and make recommendations as it relates to breaches of personal information and personal health information. In general, pursuant to both *Acts*[12] a public body or custodian must take steps to protect personal information and personal health information in its custody or control. The *Acts* do not demand perfection, rather public bodies and custodians must take steps that are reasonable in the circumstances to ensure this information is protected against theft, loss and unauthorized access, use or disclosure. In the age of digital information, the protection of this information includes ensuring that there are reasonable cyber security measures in place.

[24] *ATIPPA, 2015* largely applies to the *employee information* that was accessed and taken in the cyber attack. Pursuant to *ATIPPA, 2015*, the information accessed and taken in the cyber attack included "personal information" within the meaning of the *Act* (section 2(u)) and this personal information was in the custody and/or control of the Centre, and the Regional Health Authorities which are "public bodies" (sections 2(x) and 5). The impacted Regional Health Authorities had custody and control of each entity's own employee information, *and* through its Shared Services role, the Centre also had overlapping custody and control over this information.

[25] *PHIA* largely applies to the *patient information* that was accessed and taken in the cyber attack. Pursuant to section 5 of *PHIA*, the information accessed and taken in the cyber attack was "personal health information" in the custody and/or control of the Centre, and the Regional Health Authorities who are "custodians" (section 4). The impacted Regional Health Authorities had custody or control of each entity's own personal health information (i.e. the patient information), *and* through its Shared Services role the Centre also had overlapping custody or control over this information.

[26] On November 9, 2021, the public was advised that employee information and patient information had been accessed in the cyber attack and the public was subsequently advised

[12] See section 64 of *ATTIPA, 2015* and section 15 of *PHIA*.

that this information had been taken. On December 8, 2021, Information and Privacy Commissioner Michael Harvey wrote to the Regional Health Authorities, the Department and the Centre to provide advance notice that he intended to commence an investigation into the cyber attack. On April 8, 2022 the Commissioner provided formal notice to the Regional Health Authorities, the Department, and the Centre confirming that our Office was commencing an investigation:

- into the breach of "personal information", *i.e.* the employee information, pursuant to section 73(3) of *ATIPPA, 2015* which is permitted where the Commissioner "believes that personal information has been collected, used or disclosed by a public body in contravention of this Act"; and
- into the breach of "personal *health* information", *i.e.* the patient information, pursuant to section 66(3) of *PHIA*, which permits the filing of a complaint where an individual believes that a custodian has contravened the *Act* with respect to their personal health information. A complaint was received requesting that "the Commissioner investigate what happened and ensure measures are in place to prevent this from happening again."

[27] Given the circumstances of this matter, including the sheer importance to the public at large, the Commissioner determined early on that there were reasonable grounds to proceed with a formal investigation in accordance with section 74(2) of *ATIPPA, 2015* and section 67(1) of *PHIA*.

c. Delegation of Cyber Attack Investigation

[28] During the course of our investigation, Commissioner Michael Harvey recused himself from all matters relating to the investigation and issuance of a report by this Office into the privacy breaches resulting from the cyber attack. In doing so, he delegated his authority to conduct the investigation and issue a report to a senior official in his Office. In the interest of transparency, it is necessary to now explain why he made the decision to exercise his powers of delegation during an active investigation.

[29] Prior to becoming Commissioner, Mr. Harvey was an Assistant Deputy Minister with the Department (2015-2019) and in the course of that role he served as a Director on the Board

of the Centre (2018-2019). While the cyber attack took place in 2021, well *after* the Commissioner came to our Office, the time period leading up to a cyber attack is still important from an investigation standpoint. Cyber attacks are often successful due to a variety of vulnerabilities within an organization's cyber security posture. Questions about whether cyber security vulnerabilities were previously identified, or whether any steps were taken to address known vulnerabilities, may delve into the past by months or years.

[30] The issue of potential reasonable apprehension of bias was raised twice in this matter. It was initially raised by the Regional Health Authorities early in 2022, and later by the Department in 2023. Commissioner Harvey provided decision letters confirming that after careful consideration it was determined that his past positions did not raise a reasonable apprehension of bias. The Commissioner explained that while he was a Director on the Board of the Centre, the subject matter of cyber security did not come before him in his decision-making capacity, and this was further supported through a review of the Board meeting minutes from the time period in which he served in that capacity. The Commissioner further explained to the Department that his role as an Assistant Deputy Minister within the Department did not carry with it decision-making authority nor did he have involvement in matters pertaining to the Centre's cyber security or Shared Services.[13]

[31] On March 15, 2023, our Office received an Originating Application[14] filed at the Supreme Court of Newfoundland and Labrador by the Government of Newfoundland and Labrador on behalf of the Department. In its application, the Government sought judicial review of the Commissioner's decision regarding reasonable apprehension of bias, and further sought an Order to prevent Commissioner Harvey from continuing to conduct the 2021 cyber attack investigation.

---

[13] The Commissioner relied upon *CPR v. The Information and Privacy Commissioner et al (In The Matter of the Judicial Review Procedure Act) 2002 BCSC 603* in his determination of whether or not there was a reasonable apprehension of bias in the matter before him.

[14] In filing the Originating Application, the Government of Newfoundland and Labrador made public our Office's investigation questions put to the Department, that contained information previously not released to the public as described/discussed in the following media releases *N.L. sues to halt privacy commissioner's cyberattack investigation, citing 'bias' concerns | CBC News* and *https://www.cbc.ca/listen/live-radio/1-56-st-johns-morning-show/clip/15973421-provincial-government-trying-halt-investigation-health-care-cyberattack*; The Department's decision to release this previously withheld information in its court documents also resulted in the Minister being questioned by media about the newly released information: *Haggie said a cyberthreat report raised 'no red flags.' Now it appears he didn't actually read it*.

[32] A statement released to media by the Government of Newfoundland and Labrador asserted, "We recognize the importance of investigating the cyber attack and will co-operate fully with an investigation once the court has reviewed whether there is a reasonable apprehension of bias. Given the magnitude of the cyber attack and the importance of the investigation, we are seeking direction from the court."[15]

[33] While the courts exist to adjudicate legal disputes, it must also be noted that court matters (hearings, decisions, appeals) can take years to fully resolve. Commissioner Harvey made the decision to delegate his authority and recuse himself from the 2021 cyber attack investigation in light of those factors. He issued a news release on this matter stating that:

> *The Commissioner believes it is in the public interest and in accordance with his statutory mandate to have the investigation completed in a timely manner and the report released to the public. For this reason, Commissioner Harvey has decided to recuse himself from further involvement in the investigation to avoid a lengthy and expensive court proceeding.*
>
> *…*
>
> *"While I maintain that there is no actual bias or reasonable apprehension of bias with me concluding this investigation, my priority is to avoid any further delay in the release of our Office's report," said Commissioner Harvey. "It is in the greater public interest that the report gets out, than for me to be the one to issue it. I have every confidence in our lead investigator, the technical experts that we have contracted, and Sean Murray – who has eighteen years of experience with the OIPC, to conclude this investigation."*[16]

[34] On March 21, 2023, Commissioner Harvey delegated his authority to investigate the cyber attack and issue a report on it to Sean Murray, Director of Research and Quality Assurance, in accordance with section 103 of *ATIPPA, 2015* and section 80 of *PHIA*. As described in the March 30, 2023 news release[17], our Office's cyber attack investigation continued thereafter without delay, the efforts of which have resulted in this Report.

[15] See page 20 of posted ATIPP Request made to the Department of Health and Community Services by the Minister of Justice and Public Safety.
[16] See OIPC News Release dated March 21, 2023.
[17] See OIPC News Release dated March 30, 2023.

d. Decision to Include the Department

[35] The Department participated in our investigation, and also provided submissions, documentation, and answers to most of our questions. The evidence and submissions we received in this investigation lead to the conclusion that the Department, with support from other senior Government officials, made or exerted influence over key decisions. In particular, the Department was engaged in decisions relating to notification of individuals whose personal information or personal health information was breached during the cyber attack, including through websites and statements in the media, principally as it relates to what specific information was to be disclosed at what particular juncture. While some submissions characterized this as collaboration, others characterized decisions around message content and timing to be within the control and under the direction of the Department. As noted later in this Report, we accept, given the number of entities involved and the leadership role of the Minister, that it made practical sense for the Department to co-ordinate that process.

[36] One of the challenging considerations in conducting this investigation and preparing this Report is reconciling the fact that we are investigating and assessing the actions and decisions of several separate entities, each of which has clear statutory authorities and mandates in accordance with *PHIA* and *ATIPPA, 2015*, and is fully accountable for its own actions. At the same time, these entities operate in an environment in which the Minister has ultimate authority over the health care system, "… including the supervision, control and direction of all matters relating to…the electronic health record, eHealth initiatives and the protection of personal health information" in accordance with the Department of Health and Community Services Notice, 2019[18], a regulation enacted by an Order In Council under the *Executive Council Act*.

[37] More specifically, the Minister had the authority, under the *Regional Health Authorities Act* and the *Centre for Health Information Act*[19] to direct both the Regional Health Authorities and

[18] See Regulation *NLR 98/19*.
[19] At the time of the attack, the Department (Minister) had the power to exercise this authority under section 5 of the *Centre for Health Information Act*, SNL 2018, c. C-5.2. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which now includes the Centre) per sections 3 to 5 of the new *Provincial Health Authority Act*.

the Centre[20]. While we have no evidence of a formal directive being issued, it is clear that the Department wielded authority and the other entities accepted that authority. Again, this is not necessarily a bad thing under the circumstances, and may well have been the best and most appropriate approach. Ultimately, however, in taking on that role, the Department must also bear the appropriate degree of accountability for the decisions that were made under its direction, leadership, or influence.

[38] The practical approach taken in this investigation was to simply recognize the reality that the Department played a key role in the response to the cyber attack, whether through direction or collaboration. Additionally, it was clearly perceived by the other entities and indeed the general public to hold the authority, and did in fact hold the authority, to do so. For that reason, it is important to consider the Department's actions in this investigation and to make findings as appropriate. To do anything less would be to fail in our effort to provide transparency about the circumstances surrounding this matter and accountability for the decisions relating to it by all parties.

IV. CYBER ATTACK OVERVIEW

[39] Our Office, with assistance from cyber security consultants, reviewed the cyber attack forensic reports conducted by cyber security experts together with the post-incident reports by entities such as the Canadian Centre for Cyber Security. The technical details of the overview released by the Government on March 14, 2023 as it relates to the cyber attack are accurate and provide a summary of what transpired. Due to security concerns, our Office cannot release additional in-depth details outlining how the Threat Actor moved throughout the system or provide a complete picture of what attack methods were used. The following section of this Report contains details released by the Government in its overview report, together with some additional overview information gathered by our Office.

[20] At the time of the attack, the Department (Minister) had the power to exercise this authority under sections 3 to 5 in the *Regional Health Authorities Act*, SNL 2006, c R-7 and section 4 of the Department's Regulation *NLR 98/19*. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which includes all Regional Health Authorities) per sections 3 to 5 of the new *Provincial Health Authority Act*.

a. What is Exfiltration and Ransomware?

[40] Before we outline the overview details, we caution that sometimes technical language is used and there may be some readers who are not familiar with what these words mean. There are online resources that may assist in that regard.[21] For the purposes of our Report, we believe it is important to highlight the meaning of the following terms: "exfiltrated data" and "ransomware".

[41] As described below, an "unauthorized third party," someone who did not have permission, "exfiltrated data" from some of our province's health care systems. The Canadian Centre for Cyber Security defines the word exfiltration to mean the "*unauthorized removal of data or files from a system by an intruder*"[22]. The paragraphs below describe how an intruder, the "unauthorized third party" (also referred to below as "the attacker"), removed data (took information) from our province's health care systems. The data accessed and taken from the health care system contained personal information and personal health information of employees and patients of our health care system.

[42] The "unauthorized third party" deployed something called "ransomware". The Canadian Centre for Cyber Security defines the word ransomware to mean, "*A type of malware that denies a user's access to a system or data until a sum of money is paid*".[23] As explained by our cyber security consultants:

> *Ransomware is a type of malicious software that can be used by cybercriminals to lock or encrypt a computer or network's files and demand a ransom payment in exchange for the decryption key. This means that users cannot access their files, pictures, documents, etc. Ransomware can be delivered in a number of ways, including through phishing emails, infected software downloads, and unpatched vulnerabilities in software. Once the ransomware is installed on a computer or network, it encrypts the files, making them inaccessible to the user. The cybercriminals behind the attack will then demand a ransom payment, often in the form of digital currency such as Bitcoin, in exchange for the decryption key.*

[21] Examples of Online Resources: See *Glossary - Canadian Centre for Cyber Security* or see the National Institute of Standards and Technology (more often called NIST) *Glossary | NIST*.
[22] See "d" terms in *Glossary - Canadian Centre for Cyber Security*.
[23] See "r" terms in *Glossary - Canadian Centre for Cyber Security*.

b. GOVERNMENT OVERVIEW OF CYBER ATTACK

[43] In March 2023 the Government of Newfoundland and Labrador released a Report[24] (**Government's Report**) to provide the public with an overview of the cyber attack which states in part:

> *On Saturday October 30, 2021, a cyberattack impacted IT systems supporting the delivery of healthcare services in Newfoundland and Labrador. An unauthorized third party accessed parts of the health care technology infrastructure, which resulted in an IT systems outage.*
>
> *In response to this attack, the Government of Newfoundland and Labrador activated the provincial Emergency Operations Centres (EOC), along with the Newfoundland and Labrador Centre for Health Information (NLCHI), and the four Regional Health Authorities (RHAs) to assess system impacts, coordinate their response, and focus on the continuity of care. Government officials and technical, operational, and communications teams worked together to keep Newfoundlanders and Labradorians informed about impacted systems and alternative plans for the provision of care.*
>
> *External cybersecurity experts were engaged to assist with efforts to contain, investigate, and safely retore*(sic) *health care systems. As a result of the investigation into the cyberattack, it was determined that the incident was a ransomware attack involving Hive ransomware, and that some personal information and personal health information was taken from certain systems. The appropriate authorities were notified, including the Canadian Centre for Cyber Security (CCCS), the Royal Newfoundland Constabulary (RNC), the Royal Canadian Mounted Police (RCMP), and the Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC).*
>
> *The province and RHAs provided public updates and notifications as information was confirmed regarding the personal information and personal health information involved. Identity theft and credit monitoring services were also offered and continue to be available for impacted individuals. It was also determined that certain patient health and employee information on an Eastern Health network drive was taken during the cyberattack. Eastern Health has concluded its review and notified the affected individuals as per their public statement. There continues to be no evidence that the information taken during the attack was misused.*
>
> *Clients who have received health care services at any time continue to be offered access to credit monitoring and identity theft protection services for a period of two years from the date of enrollment, at no cost to them. Patients whose Social Insurance Number and banking/financial information was*

[24] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)* Prepared by the Department of Health and Community Services and Department of Justice and Public Safety.

> *breached are offered five years of credit monitoring and identity theft protection at no cost to them. Current and former employees, physicians, and locums are also being offered access to credit monitoring services for a period of five years from the date of enrollment.*
>
> *There is no evidence to indicate that the attack was intended to specifically target NLCHI or the Newfoundland and Labrador provincial health care system. However, the attacker, Hive ransomware group, was known for its aggressive and sophisticated capabilities and its targeting of the health sector. Recently, the U.S. Department of Justice announced the successful disruption of the Hive group network.*

[44] Government's Report goes on to describe the timeline of "Initial Systems Access" stating:

> *The earliest evidence of attacker activity within the NLCHI environment occurred on **October 15, 2021**. At that time, the attacker successfully initiated a VPN connection to the NLCHI managed environment, which includes the IT domains for NLCHI and the four RHAs, using the compromised credentials of a legitimate user account. The investigation was unable to determine how these credentials were compromised prior to this activity. No attacker activity prior to **October 15, 2021** was identified.*
>
> *On **October 25, 2021**, the attacker moved laterally through the environment, escalated their privileges through an account with administrative privileges and connected to other systems.*
>
> *Between **October 26 and 29, 2021**, the attacker exfiltrated certain data from the environment, including personal information (PI) and personal health information (PHI).*
>
> *On **October 30, 2021**, the attacker deployed Hive ransomware and encrypted numerous systems, which resulted in the IT outage that caused widespread system disruption and led to the detection of the attack. Following detection, numerous steps were taken to secure systems.*

c. Additional Cyber Attack Overview Details

[45] Our Office has identified the following information that is relevant to our analysis in this matter and in grounding our findings, and also that we believe will assist with a general understanding as to what occurred at the time of the cyber attack:

> ***Removal of Over 200 Gigabytes of Data:*** The Threat Actor exfiltrated over 200 gigabytes of data from the health care systems.

Malware Deployment: In the early hours of October 30, 2021, the Threat Actor deployed malware that it had uploaded and installed within the systems and this in turn caused the widespread encryption of data and widespread system disruption.

Evidence of Exfiltration: Officials received evidence of data exfiltration between November 5, 2021 and November 9, 2021. The Centre explained the general process of how this evidence was used to draw conclusions about exfiltration scope and this approach was reasonable in the circumstances. By November 8, 2021, the Centre had made the determination that data, containing patient and employee information, was taken in the cyber attack.

Determination of Exfiltration and Privacy Breach: By November 8, 2021, the Centre states "it had been determined that the cyber attack had involved a privacy breach given the apparent exfiltration of data, which was determined to be from the Meditech data repository and a network drive for Eastern Health."

Specific Attack Vector: Although no definitive evidence exists, following a review of the forensic reports and other available evidence, and in consideration of the typical strategies employed by this Threat Actor, we conclude that initial access was likely gained through email phishing.

d. WHO OR WHAT IS HIVE?

[46] The cyber criminal community is organized like a sophisticated business and operates in a collaborative manner. Governments and organizations across the world have recognized that to stop cyber crime requires vigilance and collaboration on a global scale. Part of worldwide collaborative efforts can be seen with the sharing of cyber security threat information throughout organizations and spreading beneficial information online. The Federal Bureau of Investigation issued a Flash Alert to the world about HIVE on August 25, 2021, and additional information about HIVE continued to be released throughout 2022. As disclosed within publically available resources[25] the following information is known about the HIVE ransomware group:

[25] See Federal Bureau of Investigation (FBI) *Flash Alert* dated August 25, 2021; *News Article* dated 21 SEPT 2022 *News Article* dated December 21, 2021; Department of Health and Human Services (USA) Analyst Note dated April 18, 2022; Cybersecurity Advisory titled *#StopRansomware: Hive Ransomware* dated November 25, 2022.

HIVE - A Ransomware Group

- HIVE ransomware was first observed in June 2021.
- HIVE ransomware follows the ransomware-as-a-service[26] (RaaS) model in which developers create, maintain, and update the malware, and affiliates conduct the ransomware attacks.
- HIVE uses ransomware to target a wide range of businesses and critical infrastructure sectors, including Government Facilities, Communications, Critical Manufacturing, Information Technology, and especially Health Care and Public Health (HPH).
- Since June 2021, the HIVE ransomware group has targeted more than 1,500 victims around the world and received over $100 million in ransom payments.

HIVE – Attack Methods and Tools

- Much of Hive's operations are standard practice amongst ransomware operators.
- HIVE uses common ransomware tactics, techniques, and procedures (TTPs) to compromise victims' machines, bypass anti-malware, and then steal sensitive data and encrypt system files.
- After compromising a victim network, HIVE ransomware actors exfiltrate data and encrypt files on the network.
- The actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks."

[47] On January 26, 2023, the United States Department of Justice announced disruption of the HIVE ransomware group through global collaborative efforts by seizing control of the servers and websites that HIVE uses to communicate with its members, disrupting HIVE's

[26] As set out in Department of Justice (USA) Announcement; "*Hive used a* ***ransomware-as-a-service*** *(RaaS) model featuring administrators, sometimes called developers, and affiliates. RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.*"

ability to attack and extort victims.[27] This announcement brought good news to the world and contained a message of hope for the future:

> *"The Department of Justice's disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators," said Deputy Attorney General Lisa O. Monaco. "In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than $130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat."*
>
> *"The coordinated disruption of Hive's computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard," said FBI Director Christopher Wray.*

[48] It is important to note, while HIVE ransomware group infrastructure was dismantled, as of the date of this Report, there have been no arrests reported as it relates to the Threat Actors behind the operation. The Threat Actors who ran HIVE ransomware group and the Threat Actors who utilized its services, to the best of our knowledge, remain at large. Furthermore, there are many other organizations and networks engaged in cyber attacks, so there is no reason to assume that the individuals involved in HIVE may not already by active in ransomware through other avenues.

V. SCOPE OF IMPACT

a. WHAT WAS TAKEN IN THE CYBER ATTACK?

[49] The Threat Actors accessed and stole personal information and personal health information in the cyber attack by taking data from:

1. Eastern Health's Network Drive; and
2. Meditech Data Repositories.

[27] *Announcement* on Disruption of Hive Ransomware dated January 26, 2023; See also related News Articles: *US announces it seized Hive ransomware gang's leak sites and decryption keys (yahoo.com)* and *Industry Reactions to Hive Ransomware Takedown: Feedback Friday - SecurityWeek*

b. What is the Eastern Health Network Drive?

[50] A network drive is a form of digital shared storage that can be accessed by two or more computers on the same network. Digital files are stored on and accessed from this shared storage. Network drives exists within an organization to allow different departments/programs to easily share information with multiple people at the same time. Access to a specific area ('share') within the network drive is limited by role or purpose[28].

[51] The Threat Actor accessed and took over 200,000 files that were stored on the Eastern Health Network Drive. This Network Drive was used by several different Departments within Eastern Health: Human Resources, Cancer Care, Medicine Program, Surgery Program, Clinical Efficiency, Mental Health and Addictions, Laboratory Medicine, and Cardiology Program. Due to the sheer number of documents and document types, we cannot provide a complete list of what was stored on this Network Drive[29]. A portion of the files taken by the Threat Actor from the Eastern Health Network Drive contained personal health information and personal information.

[52] It is not possible to list all of the various types of information accessed and taken from the Eastern Health Network Drive. However, as stated in the recent report released by our province, the type of information accessed and taken includes the following[30]:

- *Medical information of current and former patients of Eastern Health (approximately 1996-2021), such as medical diagnosis, procedure type, health care number (MCP), Social Insurance Numbers and banking/financial information for some patients, and ordering health care*

[28] *Example*: Within a large organization with several departments, such a network drive can be set up so that only the staff of a Human Resources Department has access to the 'Human Resources share'. Additional restrictions can be set up to restrict further access based upon individual roles or user groups in the subfolders within that share.

[29] *Examples of Types of Files on the Eastern Health Network Drive:* Meeting minutes and agendas, polices, staff schedules, personal documentation (saved by employees themselves – e.g. tax forms, pictures), specimen logs, email and scanned letter correspondence, waitlists, surgery schedules, quality assurance data, lab requisitions, mental health and addictions referrals, cancer care databases used by epidemiologists, St. John's breast screening program spreadsheet, letters of advocacy (written by Eastern Health staff on behalf of patients to NL Housing, NL Prescription Drug Plan, etc.), attendance management correspondence to staff members, functional assessment forms for staff, letters of offer, employee immunization records, triage assessments, patients' chemotherapy protocols, cytology transportation logs, credit card authorization forms, etc.

[30] See Overview titled "Cyberattack on the Newfoundland and Labrador Health Care System" dated March 2023, released March 14, 2023, Prepared by the Department of Health and Community Services and Department of Justice and Public Safety.

provider for some health care services provided in certain Eastern Health departments and programs (e.g., Laboratory Medicine, Medicine, Surgery, Cancer Care and Cardiology).

- ***Other employee information*** *of Eastern Health employees, including disciplinary information and other human resources and administrative information.*

c. What are the Meditech Data Repositories?

[53] The company, Medical Information Technology, Inc. ("Meditech"), provides health information technology to health care providers. All four Regional Health Authorities in our province utilize Meditech as their main health care information system. The core applications utilized by this system are a suite of over 20 financial, administrative and clinical applications from Meditech's oldest platform called Magic ("Meditech Magic")[31].

[54] Eastern Health submissions explain that:

> *The Data Repository is a partial copy of the Meditech Hospital Information System "Meditech Magic". When people within the hospital system speak of using Meditech they are referring to using "Meditech Magic". While Meditech Magic is a very reliable hospital information system it is very difficult to run reports against and to extract data. To help resolve this reporting limitation, Meditech released a "Data Repository" product which takes portions of the Meditech Magic System and copies the information into a newer database format which allows for easier data extraction. Each Regional Health Authority would have its own instance of Meditech with its own instance of a Data Repository…Its primary function is to act as a reporting tool…*

[55] When our Report refers to the "***Meditech Data Repositories***", we are using this term to collectively refer to the data repositories of Eastern Health, Central Health and Labrador-Grenfell Health. Western Health's data repository was not breached in this cyber attack. The Meditech Data Repositories accessed in the cyber attack contained personal information and personal health information, which was taken by the attackers.

[31] NL eHealth Review (March 19, 2017); A memo released by the Centre on February 15, 2023 confirmed that the Centre, in conjunction with the Regional Health Authorities, will be replacing Meditech Magic and Client Server with a new Health Information System (HIS).

d. MEDITECH DATA REPOSITORIES: EMPLOYEE INFORMATION

[56] The Meditech Data Repositories contained employee information for past and (then) current employees for three Regional Health Authorities. Eastern Health and Central Health had ~28 years of employee data taken from the data repositories, and Labrador-Grenfell had ~8 years of employee data taken from its data repository. This means that:

- People who were ***employees with Eastern Health from 1993 to 2021*** had their personal information accessed and taken in the cyber attack.
- People who were ***employees of Central Health from 1993 to 2021*** had their personal information accessed and taken in the cyber attack.
- People who were ***employees of Labardor-Grenfell Health from 2013 to 2021*** had their personal information accessed and taken in the cyber attack.

[57] The type of employee information taken in the cyber attack includes name, address, contact information, Social Insurance Number (SIN), and employee user ID.

e. MEDITECH DATA REPOSITORIES: PATIENT INFORMATION

[58] The Meditech Data Repositories primarily contained patient information. The patient information stored on the Meditech Data Repositories came from information that was entered into the Meditech Admissions Module *(the "**Admissions Module**")*. When a patient is initially registered for health care services, certain patient information is collected and entered into the Admissions Module in Meditech ("***Patient Registration Information***").

[59] Each regional health authority has its own Admissions Module. A person that uses the health care services of Central Health would have their information collected and entered into *Central Health's* Admissions Module. Someone that avails of health care services from Labrador-Grenfell Health would have their information collected and entered into *Labrador-Grenfell Health's* Admissions Module. This is true for Eastern Health as well, a person who uses the health care services of Eastern Health would have certain information collected and entered into *Eastern Health's* Admissions Module as part of the regular registration process.

[60] Eastern Health's Admission Module had an expanded reach over who was impacted due to the nature of Eastern Health's functions and the specialized services it provides. It was not only the patients who entered the doors of Eastern Health who had their information accessed and taken. Eastern Health's Admission Module also contained patient information for people all across our province: it had the Patient Registration Information for everyone in our province who had ***COVID-19 testing*** and for everyone in our province who required ***specialized testing for their blood work/specimens***[32]. While Eastern Health's Admissions Module consisted of Patient Registration Information, it did not actually contain the testing results (i.e. no testing results were accessed and taken in this part of the cyber attack breach).

[61] The Patient Registration Information logged into the Admissions Module includes "basic information that is typically logged for a patient visit, such as name, address, health care number (MCP), who you are visiting, reason for visit, your doctor, phone number, and birth date, email address for notifications, in patient/out-patient, maiden name, marital status, race, and religion" and "may also include personal health information such as medical diagnosis, medical procedures, medical history, and MCP"[33]. For a small number of patients their SIN numbers were also collected at registration.

[62] The patient information accessed and taken from the Meditech Data Repositories consisted of the Admissions Modules for all three Regional Health Authorities. Eastern Health had 11 years of patient data that had been stored, Central Health having 15 years of patient data that had been stored, and Labrador-Grenfell having 8 years of patient data that had been stored. This means that:

- ***Patients of Central Health from 2006 to 2021*** had their personal health information accessed and taken in the cyber attack; and

[32] Eastern Health is the largest regional health authority and it provides specialized laboratory testing for the province of Newfoundland and Labrador. Central Health, Labrador-Grenfell Health, Western Health and private clinics will send patient blood work/specimens to Eastern Health when specialized testing is required. When the blood work/specimens are sent to Eastern Health that patient is now receiving a service from Eastern Health, i.e. they become a patient of Eastern Health, and their Patient Registration Information populates into *Eastern Health's* Admissions Module.

[33] Information and Updates on Cyber Incident - Health and Community Services (gov.nl.ca).

- *Patients of Labrador-Grenfell Health from 2013 to 2021* had their personal health information accessed and taken in the cyber attack;
- *Patients of Eastern Health from 2010 to 2021* had their personal health information accessed and taken in the cyber attack.

[63] As described above, the Admissions Module for Eastern Health also had Patient Registration Information for everyone in our province who had COVID-19 testing done and anyone who required specialized testing for their blood work/specimens. This means that:

- *All patients across our province who had their* blood work/specimens sent to Eastern Health for specialized testing from 2010 to 2021 had their personal health information accessed and taken in the cyber attack[34];
- *All patients across our province who had COVID-19 testing* (up to 2021) had their personal health information access and taken in the cyber attack.

f. How many People had their Information taken in the Cyber Attack?

[64] Our Office asked how many people had their information taken in the attack. The entities involved could not provide us with those numbers, nor did they attempt to estimate. We were provided with numbers of those who were sent direct notification (letters, emails, etc.). What follows is an explanation of who received direct notification and the numbers associated with this. This provides a partial picture of the number of people whose privacy was impacted by the cyber attack. In addition to this, we outline those impacted groups who did *not* receive direct notification, in an effort to demonstrate just how large the unknown number of people impacted is likely to be.

[65] The Threat Actor accessed and took information from two locations, one of which was the Eastern Health Network Drive. Every living person who had personal health information and/or personal information accessed and taken from the Eastern Health Network Drive was sent

[34] Patients from Central Health, Labrador-Grenfell Health, Western Health, and private clinics were impacted by this breach if their blood work/specimens had been sent to Eastern Health for specialized testing from 2010-2021.

direct notification (~66,972 letters sent to unique individuals[35]). Deceased persons (i.e. their estate representatives) were not sent notifications[36].

[66] The second part of this breach involved employee information and patient information stored within the Meditech Data Repositories. As it relates to the employee information, all current employees of Eastern Health, Central Health and Labrador-Grenfell Health at that time were sent direct notification in the form of emails, meetings, phone messaging system, etc. (~18,527 total) and some, but not all, past employees were sent direct notification letters (~19,787 total). However, not all past employees were sent direct notification letters. Therefore, while ~19,787 direct notification letters were sent to past employees, the total number of past employees who had their personal information accessed and taken from the Meditech Data Repositories is ***unknown***. Past Employees who did not receive direct notification of their information being accessed and taken in the cyber attack, fall within two groups:

- Eastern Health Past Employees (~1993 - 2006);
- Central Health Past Employees (~1993 - 2007).

[67] As it relates to the patient information stored within the Meditech Data Repositories, there was a small group of patients whose SIN information had been collected at Patient Registration. Those who were living were provided with direct notification (1,025). Deceased persons (i.e. their estates) were not sent notifications (1,489). Aside from this very small group, all other patients who had their Patient Registration Information accessed and taken in the cyber attack were not sent direct notification letters. This means that most everyone in the following categories had their patient information accessed and taken in the cyber attack, and were not sent direct notification letters:

[35] Notification letters were sent out in different batches as time went on. 281 letters were sent to employees and 68,186 letters were sent to patients for a total of 68,467 letters sent. However, a portion of patients (1,495) had previously received a letter in one of the prior batch notifications. So while 68,467 letters were sent in total, there were 66,972 unique individuals who received letters related to this portion of the breach.

[36] Our Office did receive a number of inquiries from surviving spouses indicating that their deceased spouse had received a letter. Eastern Health explained that it provided the Centre with names and MCP numbers of those who it intended to notify and the Centre would then run a "mortality clearance" using data from Vital Statistics. Eastern Health confirmed that no letters were mailed to individuals identified through this process as deceased.

- Patients of Central Health from 2006-2021.
- Patients of Labrador-Grenfell Health from 2013-2021.
- Patients of Eastern Health from 2010-2021.
- All patients across our province who had their blood work/specimens sent to Eastern Health for specialized testing from 2010-2021.
- All patients who had COVID-19 testing within and across our province (up to 2021).

[68] To understand the likely scope of the unknown number of patients who had their information accessed and taken in the attack, it is important to also note the following:

- Our province's four Regional Health Authorities provide health care services to approximately 519,000 people[37].
- The number of COVID-19 tests confirmed as being administered immediately prior to the cyber attack was 334,272 tests[38];
- The number of patient visits Eastern Health received over the 11-year period impacted in the attack is in the millions[39].

[69] We know that *approximately ~106,311* people were sent direct notifications telling them that their personal information/personal health information was accessed and taken in the attack. This number represents only a small portion of the people impacted in this breach. We know the majority of people impacted by this breach, who had their information accessed and taken in the cyber attack, did not receive direction notification. The source of notification for the majority of people impacted by this attack was through public notification measures only (indirect notification). Based upon the evidence and submissions that our Office received, the total number of privacy breaches caused by the cyber attack is unknown but is likely to be in the ***hundreds of thousands***. In other words, it is likely that the vast majority of the population

[37] Eastern Health services a population of ***313,000***, Central Health services a population of ***93,000***, Labrador-Grenfell Health services a population of ***37,000***, and Western Health services a population of ***76,600***.
[38] The October 29, 2021 website public advisory confirmed ***334,272 tests*** had been administered in our province up to that date.
[39] In lieu of providing an estimate for the number of patients impacted, in its breach reporting form to our Office Eastern Health confirmed there were approximately 22 million patient visits from 2007 to 2021. While the patient information taken from Eastern Health was from 2010 to 2021 the number of patient visits even with three years removed is still considerable. It is also acknowledged that this number would also have repeat visitors. However the number of visits taking place is still an important indicator of potential scope of impact.

of the province had some amount of personal information or personal health information taken by the cyber attackers, although the specific number may never be known.

VI. ISSUES

[70] The following issues were identified for investigation:

1. ***Response to the Privacy Breaches:*** Did the Centre and the impacted Regional Health Authorities take reasonable steps in response to the privacy breaches as required by *PHIA and ATIPPA, 2015*? In determining whether reasonable steps were taken we considered the following:
    a. Containment of the Breach;
    b. Evaluation of the Risks;
    c. Notification;
    d. Prevention.
2. ***Security and Information Practices:*** Did the Centre and the impacted Regional Health Authorities have reasonable security and information practices in place at the time of the cyber attack for its electronic information systems as required by *PHIA and ATIPPA, 2015?*

VII. LEGISLATION

[71] Under our laws, public bodies and custodians are legally required to protect personal information and personal health information. In the event of a privacy breach, our laws also address when to provide notification to impacted individuals. While the protection of information and notification were at the heart of our investigation, this cyber attack also touched upon other important considerations like records management and accuracy requirements. What follows is a breakdown of the sections of *ATIPPA, 2015* and *PHIA* relevant to our investigation.

a. PROTECTION OF INFORMATION

[72] Section 64(1) of *ATIPPA, 2015* requires public bodies to protect *personal information* (e.g. the employee information described above) which states:

> *64.(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*
>
> *(2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.*

[73] Section 15(1) of *PHIA*, worded slightly different, requires custodians to protect *personal health information* (e.g. the patient information described above) which states:

> *15.(1) A custodian shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;*
>
> *(b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.*
>
> *(2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal health information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.*

b. NOTIFICATION

[74] Sections 64(3) to 64(9) of *ATIPPA, 2015* outline the notification obligations public bodies must comply with in the event of a privacy breach or improper disposal of an individual's personal information.

> *64 (3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is*
>
> *(a) stolen;*
> *(b) lost;*
> *(c) disposed of, except as permitted by law; or*
> *(d) disclosed to or accessed by an unauthorized person.*
>
> *(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.*
>
> *(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not required, the commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.*
>
> *(6) Where a public body has received personal information from another public body for the purpose of research, the researcher may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the public body that provided the information to the researcher first obtains that individual's consent to contact by the researcher and informs the researcher that the individual has given consent.*
>
> *(7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.*
>
> *(8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.*

> *(9) The factors that are relevant to determining under subsection (7) whether a breach creates a risk of significant harm to an individual include*
>
> *(a) the sensitivity of the personal information; and*
>
> *(b) the probability that the personal information has been, is being, or will be misused.*
>
> *[Emphasis Added]*

[75] Sections 15(3) to 15(8) of *PHIA* confirm the notification obligations that custodians must comply with in the event of a privacy breach or improper disposal of an individual's personal health information:

> *15 (3) Except as otherwise provided in subsections (6) and (7), a custodian that has custody or control of personal health information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is*
>
> *(a) stolen;*
> *(b) lost;*
> *(c) disposed of, except as permitted by this Act or the regulations; or*
> *(d) disclosed to or accessed by an unauthorized person.*
>
> *(4) Where a custodian reasonably believes that there has been a material breach as defined in the regulations involving the unauthorized collection, use, or disclosure of personal health information, that custodian shall inform the commissioner of the breach.*
>
> *(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by a custodian is not required, the commissioner may recommend that the custodian, at the first reasonable opportunity, notify the individual who is the subject of the information.*
>
> *(6) Where a custodian is a researcher who has received personal health information from another custodian under section 44, he or she may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the custodian who provided the information to the researcher first obtains the individual's consent to contact by the researcher and informs the researcher that the individual has given consent.*
>
> *(7) Subsection (3) and subsection 20(3) do not apply where the custodian reasonably believes that the theft, loss, unauthorized disposition, or*

> ***improper disclosure or access of personal health information will not have an adverse impact upon***
>
> ***(a) the provision of health care or other benefits to the individual who is the subject of the information; or***
> ***(b) the mental, physical, economic or social well-being of the individual who is the subject of the information.***
>
> *(8) Notwithstanding subsection (1), a custodian that has custody or control of personal health information that is the subject of a request for access under subsection 53(1) or for correction under subsection 60(1) shall retain the information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.*
>
> ***[Emphasis Added]***

[76] Section 5 of the *Personal Health Information Regulations* provide custodians with guidance on factors to consider when determining whether a privacy breach is a "material breach" as referenced in 15(4) of *PHIA*:

> 5. ***The factors that are relevant to determining what constitutes a material breach for the purpose of*** subsection 15(4) ***of the*** Act ***include the following:***
>
> ***(a) the sensitivity of the personal health information involved;***
>
> ***(b) the number of people whose personal health information was involved;***
>
> ***(c) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and***
>
> ***(d) whether the cause of the breach or the pattern of breaches indicates a systemic problem.***
>
> ***[Emphasis added]***

c. Information Practices, Policies and Procedures

[77] While *ATIPPA, 2015* does not have an explicit provision requiring records management, most public bodies that are subject to *ATIPPA, 2015* are also subject to the *Management of Information Act*, *("**MOIA**").* Section 6 of *MOIA* requires public bodies to put in place a records management system for the personal information in their custody or control:

> ***6. (1) A permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.***
>
> *(2) A system required under subsection (1) shall provide for retention periods and disposition by*

> *(a) destruction, or*
>
> *(b) transfer to the archives,*
> *in accordance with the guidelines and schedules established by the Government Records Committee established under section 5.1.*
>
> ***(3) A permanent head of a public body shall ensure that the retention, disposal and removal of government records is carried out in accordance with this Act.***
>
> ***[Emphasis Added]***

[78] Section 13 of *PHIA* is more detailed and requires that custodians put information policies and procedures in place to protect the personal health information in the custodian's custody or control:

> ***13.(1) custodian that has custody or control of personal health information shall establish and implement information policies and procedures to facilitate the implementation of, and ensure compliance with, this Act and the regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside the province.***
>
> ***(2) The information policies and procedures referred to in subsection (1) shall include policies and procedures to***
>
> (a) protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;
>
> (b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;
>
> (c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed *by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and*
>
> (d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.
>
> ***(3) The information policies and procedures referred to in subsection (1) shall include appropriate measures to address the risks associated with***

> *the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected.*
>
> *[Emphasis Added]*

d. Complete and Accurate Information

[79] Section 63 of *ATIPPA, 2015* outlines the requirement for public bodies to ensure personal information is complete and accurate:

> *63. Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.*

[80] Section 16 of *PHIA,* which deals with personal health information, echoes these requirements and more stating:

> *16. Before using or disclosing personal health information that is in its custody or under its control, a custodian shall*
>
> *(a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purpose for which the information is used or disclosed;*
>
> *(b) clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information; and*
>
> *(c) make a reasonable effort to ensure that the person to whom a disclosure is made is the person intended and authorized to receive the information.*
>
> *[Emphasis Added]*

VIII. RESPONSE TO THE PRIVACY BREACHES

Issue #1: Did the Centre and Regional Health Authorities take reasonable steps in response to the privacy breaches as required by *PHIA* and *ATIPPA, 2015*?

[81] Pursuant to *ATIPPA, 2015* and *PHIA,* the Centre, and the impacted Regional Health Authorities (Eastern Health, Central Health, and Labrador-Grenfell Health) as public bodies/custodians were responsible for the protection of the personal information and personal health information in their custody or control (hereafter collectively the "Regional Health Authorities"). These legal obligations extend to obligations imposed by the *Acts* when

a privacy breach occurs. This means that the Centre and the Regional Health Authorities were responsible for managing the privacy breach that occurred.

[82] The topic of Shared Services will be addressed later in this Report. For the purposes of this section, it is important to note that Shared Services did not remove, shift, or alter the legal obligations set out in *ATIPPA, 2015* and *PHIA*. Shared Services implementation was not accompanied by an amendment to either of those statutes, therefore all of the accountabilities set out therein for the Regional Health Authorities and the Centre continued to apply.

[83] The Access to Information and Protection of Privacy (ATIPP) Office of the Department of Justice and Public Safety created a "Privacy Breach Protocol" to assist public bodies with making decisions when a privacy breach occurs, and in our view, this protocol is a useful framework for responding to a privacy breach[40]. The *Privacy Breach Protocol (March 2015)* identifies four key steps of managing a privacy breach:

1. Contain the Breach;
2. Evaluate the Risks;
3. Notify Affected Individuals (if appropriate);
4. Prevent Future Breaches.

[84] The Department of Health and Community Services offers a risk management tool-kit which includes privacy breach guidelines for custodians when they are faced with a privacy breach involving personal health information.[41] These guidelines mirror the key steps above, with the Department's guidance confirming that custodians must take immediate action upon learning of a privacy breach, further noting that many of the steps required to be taken "need to be carried out simultaneously or in rapid succession."

[85] The reasonableness of the actions taken by the Centre and the impacted Regional Health Authorities are analyzed within this section of the Report.

[40] See *Privacy Breach Protocol (March 2015)*.
[41] The "Privacy Breach Guidelines" are located within Item 6 of its "*PHIA* Risk Management Toolkit" which can be downloaded from the Department's website.

a. CONTAINMENT OF THE BREACH

[86] The purpose of containment is to minimize (stop or reduce) the risk or damage caused by the privacy breach. During this step, some investigation efforts take place. Information gathered through investigation(s) assist public bodies and custodians in making decisions on what containment measures to take and how to implement them. Effective and prompt containment may reduce the magnitude of a breach, and may, in some cases, reduce the risks to individuals impacted by the breach[42].

[87] Depending on the nature of the privacy breach, containment steps may include stopping an unauthorized practice, retrieving the records, shutting down or correcting weaknesses in physical, technical, or administrative security, and/or contacting law enforcement agencies.

[88] Effective containment of a cyber attack often involves extensive investigations to determine how the attack took place, if the attack is still happening, how to stop the attack and how to prevent it from spreading. Cyber security containment efforts can include things such as isolating infected systems, shutting systems down, and taking measures to eradicate and remove existing threats from the systems. Containment strategies can vary greatly and special considerations are often required. As such, decisions may impact an organization's ability to continue with critical functions or services.

[89] This Report does not disclose additional *technical* details of containment efforts beyond what has already been released to the public by Government in this matter or is otherwise publicly available, as we do not wish to reveal information about vulnerabilities and potentially place our province's health care information systems at risk of another attack. What follows in this section of the Report includes a summary of information the Government has released to the public, together with additional information gathered by our Office that is relevant to our analysis in this matter and in grounding of our findings and recommendations, and that we believe will assist with establishing a greater understanding among the public as to what containment efforts took place in response to the cyber attack.

[42] Para. 49 of Report 009-2020, 053-2020, 224-2020 (oipc.sk.ca); Para 25 of Report 120-2022, 135-2022 (oipc.sk.ca).

i. Government's Summary of Containment Efforts

[90] The Government's Report[43] released to the public in March 2023 includes a summary of many of the containment steps taken on/after **October 30, 2021**, stating in part:

- *Once the attack was detected on **October 30, 2021**, NLCHI took immediate actions to respond, including working closely with its [Managed Service Provider], initiating its internal Emergency Operations Centre, notifying the Office of the Chief Information Officer (OCIO), the Department of Health and Community Services (DHCS) and the four RHAs, and obtaining assistance from external cybersecurity experts.*
- *Efforts were undertaken immediately, and continuously thereafter, to securely contain systems and restore health care operations as soon as safely possible.*
- *On **October 30, 2021**…NLCHI's [Managed Service Provider] immediately engaged third party cybersecurity experts to conduct an investigation in the [Managed Service Provider] environment and to assist the [Managed Service Provider] and NLCHI with system recovery efforts. The [Managed Service Provider] also locked relevant accounts on the [Managed Service Provider]-managed domain and enabled accounts as needed for the response to the attack.*
- *On **October 31, 2021**, NLCHI notified the [Canadian Centre for Cyber Security], the [Royal Newfoundland Constabulary], and the [Royal Canadian Mounted Police]. Operations committees, including administration, clinical operations and communications, were established to coordinate the system recovery and restoration process. A team was assembled to review impacted applications and work to restore them to service as soon as possible. A separate team was assembled to investigate and eradicate the attacker's presence within the NLCHI-managed environment.*
- *On **November 2 and 3, 2021**, a third-party cybersecurity expert was engaged. NLCHI also continued its analysis, planning and efforts to restore health system operations and data, and worked to respond to new developments as they emerged. As a result of these efforts, there continued to be intermittent system disruption as certain systems had to be taken offline to securely restore operations.*
- *On **November 3, 2021**…steps were being taken for the deployment of commercial forensic and investigative endpoint tools, and numerous other containment and mitigation steps were being taken. Extensive work to restore the wide range of systems and services supporting health care,*

[43] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)* Prepared by the Department of Health and Community Services and Department of Justice and Public Safety.

including Meditech and email services, continued at this time and for weeks to follow.

- *On and after **November 4, 2021**, among other activities, NLCHI continued working with the RHAs to restore Meditech (and in support of RHA staff efforts to enter the backlog of paper records that were accumulating since the start of the outage) and to prioritize the sequencing of restoring and integrating systems.*
- *During the initial response to the attack, numerous containment and mitigation steps were being executed, including taking individual workstations and servers offline as needed, restricting internet access, taking services offline, reviewing privileged accounts, forensic investigation work, systems hardening planning, and other steps for securely restoring systems, including restorations from backups.*

  …
- *Continuing to **November 21, 2021**, other containment and mitigation steps taken by NLCHI included global password resets, patching of all gateway components, further enhancing use of a O365 monitoring and reporting tool, completing a vulnerability scan on all RHA and NLCHI internet accessible addresses, conducting a hardware inventory reconciliation, and taking steps towards implementing MFA for all remote access mechanisms that were previously using a single-factor authentication method.*
- *As of **December 5, 2021**, significant progress had been made on system restoration and most of the critical and priority systems had been restored or rebuilt from backups, and all devices (e.g., laptops, desktops, servers) on the NLCHI and RHA networks had been analyzed for evidence of malicious activity.*

[91] The steps identified above are consistent with good industry practices. Retaining the services of an external incident response team took advantage of specialized expertise and skills allowing for comprehensive and quick response efforts. It is clear that evidence and logs were preserved resulting in detailed forensic reports.

[92] Commissioner's Delegate Findings: I find that reasonable steps were taken to investigate and attempt to contain the privacy breach.

ii. SOURCE OF INITIAL CREDENTIAL COMPROMISE

[93] As explained in Government's Report, the earliest Threat Actor activity was found on 15 October 2021. A VPN connection was established by the Threat Actor using compromised credentials (e.g. the correct user name and password required to log on to the virtual private network). Government's Report went on to state that their investigation was unable to determine how the credentials were compromised.

[94] The RCMP conducted an investigation into this matter and held interviews including with the owner of the credentials used in the attack (a health system employee). There were no criminal charges laid, and we have no evidence that the person whose credentials were used to access the system was aware that their credentials had been used by the attackers. We are satisfied that there is no evidence of an insider threat in this matter.

[95] Forensic investigations concluded that the source of credential compromise could not be determined based on the evidence available. While investigations were unable to determine how the credentials were compromised in this particular case, we would like to note the following:

- The FBI Flash Alert advisory[44] dated August 25, 2021 on the HIVE ransomware group confirms "*Hive ransomware uses multiple mechanisms to compromise business networks, **including phishing emails with malicious attachments** to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network";*

- Department of Health and Human Services (USA) Analyst Note dated April 18, 2022 indicates that HIVE "leverage common (but effective) infection vectors such as RDP and VPN compromise as well as ***phishing***"[45].

- The Cybersecurity & Infrastructure Security Agency (USA) issued a Cyber Security Advisory November 25, 2022 confirming other potential methods HIVE utilized to gain access but noted that "*Hive actors have also gained initial access to victim networks by distributing **phishing emails***"[46]

[44] See Federal Bureau of Investigation (FBI) *Flash Alert* dated August 25, 2021.
[45] Department of Health and Human Services (USA) Analyst Note dated April 1, 2022.
[46] Cybersecurity Advisory titled *#StopRansomware: Hive Ransomware* dated November 25, 2022.

[96] When coupled with email phishing being a tool known to be used by HIVE, together with a review of the forensic reports and other evidence available to our Office, our conclusion is that the initial source of compromise was likely related to email phishing.

[97] Commissioner's Delegate Findings: I find that reasonable steps were taken to investigate the credential compromise.

iii. Prior System Alerts

[98] The average time cyber attackers stay on a network (the "dwell time") can vary widely depending on a number of factors, such as the complexity of the attack, the sophistication of the attacker, and the security measures in place on the network. There have been cases where attackers are able to remain undetected on a network for weeks or even months before being discovered. The dwell time the Threat Actor was able to operate within health care systems undetected lasted for a two-week period (October 15, to October 30, 2021). During this time, the Threat Actors navigated throughout the health care systems, and took over 200 gigabytes of data, all without being discovered.

[99] The containment efforts outlined above show what steps were taken once it was learned that the attack had occurred. By the time it was realized what had happened/was happening, it was too late to prevent, stop, or reduce the magnitude of the privacy breach.

[100] Many of the tools and techniques used by the Threat Actor in this matter were common and well known and should have been identified and responded to by an appropriate defense eco-system.

[101] Prior to October 30, 2021 some Threat Actor activities triggered alerts within the health care systems. The Centre, which had responsibility to protect information in the health care systems, failed to adequately respond to our questions regarding what, if any, steps were taken in response to these alerts, thereby failing to provide evidence of what, if any, response and investigation efforts were made during this crucial period. While our Office cannot release technical details, opportunities to prevent the successful deployment of the ransomware were missed.

[102] Commissioner's Delegate Findings: I find that prior alerts were not properly investigated and/or responded to. Had this been done it may have prevented or reduced the extent of the malicious extraction of data that followed.

iv. Full Containment Impossible

[103] As noted above, over 200 gigabytes of data was maliciously stolen in this attack. While recent international efforts resulted in the dismantling of HIVE's infrastructure,[47] this does not mean the data that was taken in the cyber attack is now safe. On the contrary, there is no way of knowing for sure whether the information may have been copied and retained in other locations or disclosed to other parties prior to HIVE being dismantled. The personal information and personal health information contained within the data can never be fully recovered/contained.

[104] Commissioner's Delegate Finding: I find that the breach of personal information and personal health information stolen in this matter was not contained.

v. Monitoring Efforts

[105] The entities involved in this matter all fully recognize the personal information and personal health information taken in this attack can never be fully recovered/contained. This is demonstrated by not only offering credit monitoring services to those impacted by the breach, but also by engaging in dark web monitoring services to provide mechanisms for ongoing attempts to contain the breach.

[106] The most likely place for stolen data to resurface is the dark web. [48] The "dark web" is used for a variety of purposes, the most notorious being "to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data"[49].

---

[47] See Department of Justice (USA) *Announcement* on Disruption of Hive Ransomware dated January 26, 2023.
[48] See para. 73 in Report 009-2020, 053-2020, 224-2020 (oipc.sk.ca); See para. 75 009-2020, 053-2020, 224-2020 (oipc.sk.ca).
[49] See Center for Internet Security "*Election Security Spotlight – The Surface Web, Dark Web, and Deep Web*" for additional information on different levels of the web; this article also explains there are good uses as well for the dark web was well stating "*there are several legitimate activities on the Dark Web as well, including accessing information, sharing information, protecting one's identity, and communicating with others. Many news organizations operate on the Dark Web to protect confidential sources.*"

[107] Government's Report confirms there "continues to be no evidence that the information taken during the attack was misused"[50]. This statement is made in reference to the engagement of dark web monitoring services. While our Office cannot provide the technical details of the exact containment measures being taken, we can confirm to the public that they are extensive, being provided on an indefinite basis, and are consistent with standard industry practices. There exists an ongoing obligation on the part of the (now) Provincial Health Authority to provide notification to those impacted should such monitoring efforts reveal evidence of the stolen data's existence on the dark web or elsewhere on the web.

[108] Individual credit monitoring services can be effective in mitigating the effects of a privacy breach by helping to protect against the risk of misuse of one's information. Alerts identifying potentially fraudulent credit applications can prompt individuals to contact the appropriate financial institutions and prevent identity theft or financial loss. As outlined in Government's Report[51], credit monitoring services are being provided to those impacted by the privacy breach between two and five years depending on what type of information was taken:

> *Clients who have received health care services at any time continue to be offered access to credit monitoring and identity theft protection services for a period of two years from the date of enrollment, at no cost to them. Patients whose Social Insurance Number and banking/financial information was breached are offered five years of credit monitoring and identity theft protection at no cost to them. Current and former employees, physicians, and locums are also being offered access to credit monitoring services for a period of five years from the date of enrollment.*

[109] Eastern Health has posted details on its website[52] about these services specifically noting that (as of the date of this Report) the **deadline** for enrolling in credit monitoring services is **September 30, 2023**. Within Eastern Health's website is a dedicated YouTube video explaining how to enroll that includes a breakdown of steps to take and phone numbers impacted individuals can call.

---

[50] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)* Prepared by the Department of Health and Community Services and Department of Justice and Public Safety.
[51] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)* Prepared by the Department of Health and Community Services and Department of Justice and Public Safety.
[52] See Eastern Health Website: Credit Monitoring & Identity Theft Protection Services – Eastern Health; YouTube Video on Enrollment: https://www.youtube.com/watch?v=ho2QKBKqUXQ.

[110] Our Office notes that insufficient duration of credit monitoring services has been used to assist in grounding class-action certification claims with those impacted by the privacy breach arguing, in part, that damages exist/will exist in the form of fees and costs paid to further protect themselves beyond the time-limited credit monitoring services being offered[53].

[111] When dealing with privacy breach matters, other Canadian privacy oversight bodies have, at times, recommended that credit monitoring services be provided to individuals who have had their personal information and personal health information taken, with recommendations varying between two and five years[54].

[112] In this matter, the difference in whether someone receives two years versus five years of credit monitoring services depends upon what type of information was taken. Those who were provided with five years of credit monitoring services had financial or SIN information taken in conjunction with their name and/or contact information, and both are known to be more valuable and useful to malicious actors.

[113] Commissioner's Delegate Finding: I find that the credit monitoring service being provided to those impacted by the cyber attack is a reasonable containment step.

vi. General Comments on Ransom Payments and Non-Payments

[114] There are several reasons why organizations may implement a policy against ransom payment when dealing with a cyber attack. Generally speaking, some reasons fall under the umbrella of "you can't trust a criminal": once criminals know you are willing to pay something, they can increase the amount they are looking for; there is no assurance decryption keys will be provided after payment; there is no guarantee the decrypted data will be perfectly restored

[53] See 2021 ONSC 7297 (CanLII) | Obodo v. Trans Union of Canada, Inc. | CanLII, 2022 BCSC 928 (CanLII) | Campbell v Capital One Financial Corporation | CanLII, 2022 QCCS 2914 (CanLII) | Zuckerman c. MGM Resorts International | CanLII.

[54] See Commissioner recommendations to offer two years of credit monitoring in 2018 NTIPC 17 (CanLII) | Northwest Territories (Education, Culture and Employment) (Re) | CanLII; See Commissioner recommendations to offer five (5) years of credit-monitoring at para. 105 in Report 009-2020, 053-2020, 224-2020 (oipc.sk.ca), at para. 88 in Report 398-2019, 399-2019, 417-2019, 005-2020, 019-2020, 021-2020, at paras. 16-18 in Report 103-2017 [Para. 18 Suggests Individuals seek legal advice on filing a law suit if the Company did not provide the five years of Credit monitoring services], at para. 39 in Report 2022 CanLII 109458 (SK IPC) | Saskatchewan Liquor and Gaming Authority (Re) | CanLII [Recommendation for extension of credit monitoring to five years as individuals at risk of identity theft.]; 2022 CanLII 84339 (SK IPC) | Dr. Davidson et al. (Saskatoon Obstetric & Gynecologic Consultants) (Re) | CanLII.

with the decryption key (data can suffer harm in the corruption process making it unrepairable, resulting in missing data); there is no guarantee the data collected will be deleted and not retained; etc.

[115] There are also moral reasons against making ransom payments as no one wants to be responsible for the harm of another. The reality is payments to ransomware groups ultimately support the "business" allowing it prosper, to then seek out the next victim. There are also issues of legality that arise in payments of ransomware. Generally speaking, payment of ransom is not illegal in Canada. However, payment of ransom runs the risk of potentially violating other laws, for example, it is a crime to give financial aid to deemed terrorists[55]. Nevertheless, organizations suffering from a ransomware attack are faced with potentially devastating effects like the crippling of critical systems, halting of lifesaving services, and complete or partial loss of important data. There are some organizations that pay ransom when faced with such difficult circumstances and there are others that do not. Some organizations may even state publicly that they have not paid a ransom when in fact they have.

[116] As it relates to the our province's cyber attack, on March 12, 2023 the Government of Newfoundland and Labrador issued a news release confirming its intention to provide the public with an update on the cyber attack. Shortly thereafter, the Government Report was released and it was finally confirmed for the public that the cyber attack was a ransomware attack. Upon its release, the Minister of Justice and Public Safety did not provide any answers on how much was requested in payment, nor whether such payment was or was not made, stating:[56]

> *"We can't disclose anything about a request for a ransom, for security purposes,"*

[55] See: Ransomware: To Pay or Not to Pay | Knowledge | Fasken; John Ridsdel execution: Why refusing to pay ransoms may not protect Canadians | CBC News; Sophisticated ransomware attacks leave lawyers scrambling to keep up | Financial Post.

[56] See News Articles: *N.L. says Hive ransomware group was behind 2021 cyberattack on health systems | CBC News; Province refuses to say whether ransom was paid to group behind 2021 attack on Newfoundland and Labrador health systems | SaltWire; Ransomware group behind N.L.'s 2021 cyberattack on health network | CTV News*.

> *"Again, that's advice we get from security agencies, legal instructions, legal advice, and other groups that have had this happen to them."*

[117] We received no evidence or submissions from the Department or the Centre supporting the position that such details cannot be disclosed. However, notwithstanding this, for reasons that follow, we are not making recommendations regarding the disclosure of that information.

[118] In the context of this investigation, whether or not a ransom payment was made is potentially relevant to the following considerations:

1. Whether or not reasonable steps were taken to contain the privacy breach; and
2. Whether or not reasonable notification was provided to individuals impacted by the privacy breach.

Containment Effort Considerations

[119] Insofar as containment efforts are concerned, payment or nonpayment of ransomware results in the same conclusion: the privacy breach not being contained. Payment of ransom cannot be relied upon as an effective containment solution as there is no way to confirm stolen data was wholly deleted and not retained. Similarly, non-payment of a ransom cannot be said to be a "bad" containment decision since payment does not necessarily equate to effective containment.[57]

Notification Considerations

[120] Reasonable notification requires that enough information be provided to allow the individual to understand the significance of the privacy breach, and should include information that might assist the individual in reducing or preventing harm that could be caused by the privacy breach. With the release of the Government's Report, the public was finally made aware that this was a ransomware cyber attack. In that report, the public was also informed that the HIVE ransomware group were the perpetrators, who are specifically known for leaving a ransom note requesting payment and threatening its victims that data will be publically disclosed or leaked if ransom is not paid[58].

[57] See para. 42 in Report 009-2020, 053-2020, 224-2020 (oipc.sk.ca).
[58] Example HIVE ransom note found on *#StopRansomware: Hive Ransomware* issued by Department of Health and Human Services (USA) Cybersecurity Advisory titled dated November 25, 2022.

[121] Knowing that this attack was ransomware provides an individual with information that they can use to make decisions when assessing their own risk. Knowing about the "HIVE ransomware group", and by extension its operations and methods, provides additional context which may assist an individual in making decisions, such as whether to seek credit monitoring or take other actions at all or more quickly.

[122] However, as stated above, payment of ransom is not a reliable containment solution in a ransomware cyber attack, as even if an encryption key is provided in exchange, there is no way to confirm that stolen data was wholly deleted and not retained by the attacker. Therefore, disclosure of information about payment of ransom cannot be fully relied upon by an individual when making decisions on how to protect themselves from risk. Ultimately, information about payment of ransom and non-payment of ransom is of marginal benefit at best, and leaves an individual with much the same risk of harm. As such, this information is not reliable or relevant for notification purposes.

[123] For the above reasons, we make no recommendations relating to the disclosure of information regarding payment or non-payment of ransom. This is not to say that questions about whether or not ransom was paid are not valid, however given my conclusion that such information is not necessary for the analysis in this Report, they are questions that must be left for another forum.

vii. Summary of Commissioner's Delegate Findings

[124] After a detailed review of the documents (including Forensic Reports, post-incident Reports, etc.) and submissions in this matter, the following findings are made as it relates to the containment measures taken:

- I find that reasonable steps were taken to investigate and attempt to contain the privacy breach.
- I find that reasonable steps were taken to investigate the credential compromise.
- I find that prior alerts were not properly investigated and/or responded to. Had this been done it may have prevented or reduced the extent of the malicious extraction of data that followed.

- I find that the breach of personal information and personal health information stolen in this matter was not contained.

- I find that the credit monitoring service being provided to those impacted by the cyber attack is a reasonable containment step.

b. Evaluation of the Risks

[125] In general, evaluating potential risks to affected individuals is important in order to understand the magnitude of the breach and impact on individuals whose information was subject to a breach[59]. As stated in prior Reports of this Office:

> *This evaluation assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the importance of notification increases and the manner in which it is done becomes more important. Once those individuals whose personal information is involved in the breach are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.* [60]
>
> ...
>
> *Further considerations in evaluating the risk include determining the cause and extent of the breach, which can indicate whether the information was lost or stolen, or whether the breach was deliberate or accidental, whether the information can be recovered, or whether the breach was due to a systemic problem or an isolated incident. The process of evaluating the risk also includes identifying who and how many people may have been affected by the breach, as well as assessing the foreseeable harm which might come from the breach.*[61]

i. The Type of Information

[126] The type of information taken in this breach is explained in depth elsewhere in this Report. In general, it includes a variety of information types, including SIN number, banking/financial information, employee disciplinary information, health care number, name, addresses, contact information, email address, phone number, race, religion, maiden name, marital status, medical diagnosis information, and medical information such as reason for visit. This

---

[59] See "*Privacy Breach Protocol*" or "Privacy Breach Guidelines" located within Item 6 of its "*PHIA* Risk Management Toolkit" which can be downloaded from the Department's website; also some of the questions within "Part 6 – Assessing real risk of Significant Harm" within the Privacy Commissioner of Canada's guidance document titled may provide additional assistance in what questions to ask in trying to assessing risk, just keep in mind that this document is addressing different legislation and use caution when using it.
[60] See Reports: P-2008-003 at para. 8, and P-2009-001 at para. 7.
[61] See Report P-2008-001 at para 20.

type of information is considered sensitive because of the specific risks to individuals when such information is lost, stolen, or disposed of improperly.

[127] The type of information accessed and stolen in this attack can be used for fraudulent and other harmful purposes. For example, Social Insurance Numbers ("SIN numbers") can be used to open fraudulent accounts, loans, credit cards, etc. Furthermore, SIN numbers are permanent and not easily canceled[62] unlike, for example credit cards, and therefore have long lasting value to malicious actors, which creates an increased risk to impacted individuals. The information taken in this cyber attack included several different pieces of information (e.g. race, religion, marital status) that can be paired with other identifying information, thereby increasing the risk to impacted individuals.[63] Health information can be used for social engineering purposes where malicious actors use the information taken to obtain additional personal information from another source or to make a fraudulent plea appear legitimate[64]. Addresses, phone numbers and emails can be used for additional phishing purposes, increasing an individual's vulnerability to identity theft and fraud[65]. Information such as medical diagnosis, or the description of reasons for requiring health care services, consists of highly sensitive information and places an individual at an increased risk of humiliation and damage to reputation or relationships.

[128] Commissioner's Delegate Finding: I find that there is a risk of significant harm that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the credit record within the meaning of section 64(8) of *ATIPPA, 2015*.

---

[62] See Social Insurance Number – Overview - Canada.ca where it states that Service Canada will not issue you a new SIN number if it was lost or stolen. This website goes on to state that Service Canada *may* issue a new SIN if there is *proof* the SIN was used fraudulently.

[63] See 2019 NTIPC 10 (CanLII) | Department of Health and Social Services (Re) | CanLII which discusses how malicious actors will use information to build profiles on an individual making it easier to commit identity theft or fraud. Within this case it is noted that very few pieces of identifying information are required to commit identity theft or fraud; See also how medical records can be valued highly by criminals Healthcare under Attack: What Happens to Stolen Medical Records? - Wiadomości bezpieczeństwa (trendmicro.com) and What hackers actually do with your stolen medical records (advisory.com).

[64] See 2020 NSOIPC 2 (CanLII) | Nova Scotia Health Authority (Re) | CanLII at paras. 54-55; Also See 2019 NTIPC 10 (CanLII) | Department of Health and Social Services (Re) | CanLII where it was noted that a health care number alone still has the potential to lead to identity theft or fraud by someone with intent and know-how.

[65] See decisions P2022-ND-060.pdf (oipc.ab.ca) and P2022-ND-048.pdf (oipc.ab.ca) that recognize how email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

[129] Commissioner's Delegate Finding: I find that there is a risk of adverse impact upon the mental, physical, economical, or social well-being to impacted individuals that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the individual's credit record within the meaning of section 15(7) of *PHIA*.

[130] Commissioner's Delegate Finding: I find that the personal information and personal health information accessed and taken in the attack is highly sensitive information. It is the kind of information that is associated with a high risk of misuse by bad actors and the consequences of such misuse are significant for victims.

ii. Cause and Extent of the Breach

[131] The privacy breach occurred due to the malicious actions of the HIVE ransomware group, a group that is known to attempt to extort payment with threats of publishing stolen data. Over 200 gigabytes of data was taken in this cyber attack and there can be no certainty that the information will not be misused at some point in the future and therefore the breach will never be contained. The data was not encrypted and contained the personal information and personal health information of hundreds of thousands of individuals.

[132] Commissioner's Delegate Finding: I find there is an increased risk to impacted individuals associated with the cause and extent of the breach.

iii. Foreseeable Harm from the Breach

[133] The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a Threat Actor (deliberate intrusion, deployment of ransomware). The Threat Actors in this matter are known to threaten exposure of stolen data by publishing it to websites that expose this information to additional malicious actors. Lack of evidence of misuse of the data does not mitigate against future harm. The harm in this matter is foreseeable as information obtained from a privacy breach can be published or used months or years after an incident[66].

[66] See paras. 81 to 83 in Report 009-2020, 053-2020, 224-2020 (oipc.sk.ca) which describes an incident where information was taken in 2012 and used by the malicious actor four years thereafter with the Commissioner concluding this "shows that malicious actors have patience and stolen data can end up on the dark web at any time, even years later."

[134] Commissioner's Delegate Finding: I find that there is foreseeable harm to individuals impacted by the privacy breach from theft of their personal information and/or personal health information.

[135] The foreseeable harm from a privacy breach is not limited to the impacted individuals. There exists a risk of harm to public trust, which in turn creates a risk to public health and safety. As stated in Report 19-HIA14[67]:

> *Whether or not this information could be used for identity theft or fraud (which is a real possibility with even limited data points) the more significant risk, and the more significant impact of the breach…is the risk that the people of the Northwest Territories will lose confidence in the ability of the Department of Health and Social Services to adequately protect their most sensitive personal health information. This, in turn, negatively impacts on the effectiveness of the health system and the health of residents of the Northwest Territories as a whole.*

[136] The cyber attack privacy breach contributed to an erosion of public trust in our province's Government and the Provincial Health Authority's (Centre and the impacted Regional Health Authorities) ability to safeguard sensitive personal information. The factors which contribute to this foreseeable harm include the following:

- The magnitude of this breach was extensive;
- The categories of impacted persons are lengthy and potentially difficult for everyone who was impacted to understand;
- Direct notification was not possible for all persons impacted by the breach creating a significant "unknown" element to who may have been impacted;
- Key questions asked about the nature of the attack went unanswered by officials until March 2023.

[137] Commissioner's Delegate Finding: I find that the impact of the cyber attack has contributed to an erosion of public trust in Government and the Provincial Health Authority and that this was a foreseeable harm from such an event.

[67] See 2019 NTIPC 10 (CanLII) | Department of Health and Social Services (Re) | CanLII; Also see para 34 together with Commissioner's Message in 2019 NSOIPC 2 (CanLII) | Department of Internal Services (Re) | CanLII which states in part "A failure to protect the privacy rights of Nova Scotians contributes to the erosion of citizens' trust in the government." para. 26 in 2019 NTIPC 10 (CanLII) | Department of Health and Social Services (Re) | CanLII.

iv. Evidence Demonstrating Risk Evaluation

[138] Many steps taken in this matter demonstrate that risks identified above were considered and acted upon by the Department, Centre and the impacted Regional Health Authorities.

[139] Steps were taken to provide a wide variety of notification measures in an attempt to inform the public of the privacy breach, including posting information online, holding public advisory briefings (recorded sit-down briefings where officials described to the public certain details about what occurred and what information was taken), issuing news releases, sending letters to affected community stakeholders, etc.

[140] Where possible, direct notification was primarily provided to individuals who had SIN information or financial information taken in the attack. Credit monitoring services were provided to affected individuals ranging from two to five years with the latter duration being offered to those whose SIN and financial-related information had been accessed and taken in the attack.

[141] As part of public notification measures, impacted individuals were given a list of resources providing other steps that can be taken to protect an individual's information and protect against identity theft. For example, the Department's website on the cyber attack provided the following information:

> *There are other steps you can take to protect your information, or if you suspect you've been the victim of identify theft:*
>
> - *Call Equifax or TransUnion Canada to get a copy of Credit Report.*
> - *If you suspect that your social insurance number is being used fraudulently, Service Canada advises filing a complaint with the police.*
> - *Contact the Canadian Anti-Fraud Centre at 1-888-495-8501.*
> - *Inform your bank and creditors by phone and in writing about any irregularities.*
> - *Report any irregularities in your mail delivery to Canada Post, for example, opened envelopes, missing financial statements or documents.*
> - *Visit a Service Canada office and bring all the necessary documents with you proving fraud or misuse of your SIN.*

- *Fraud Alert: You may want to discuss with Equifax and TransUnion Canada whether you should have a fraud alert placed on your credit report by contacting them using the contact information above.*
- *Alert the Canada Revenue Agency (CRA): You can report suspected fraud or identify theft with the CRA by calling them at 1-800-959-8281.*
- *Additional Information: For additional information about steps you can take to protect your information, please see Digital Government and Service NL's guidance on "Reducing the Risk of Identity Theft".*

[142] Commissioner's Delegate Finding: With the exception of some matters related to notification, I find that the steps taken in response to the cyber attack largely demonstrate that the entities evaluated risk appropriately.

v. Summary of Commissioner's Delegate Findings

[143] The following findings are made regarding risk assessment:

- I find that there is a risk of significant harm that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the credit record within the meaning of section 64(8) of *ATIPPA, 2015*.

- I find that there is a risk of adverse impact upon the mental, physical, economic, or social well-being to impacted individuals that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the individual's credit record within the meaning of section 15(7) of *PHIA*.

- I find that the personal information and personal health information accessed and taken in the attack is highly sensitive information. It is the kind of information that is associated with a high risk of misuse by bad actors and the consequences of such misuse are significant for victims.

- I find there is an increased risk to impacted individuals associated with the cause and extent of the breach.

- I find that there is foreseeable harm to individuals impacted by the privacy breach from theft of their personal information and/or personal health information.

- I find that the impact of the cyber attack has contributed to an erosion of public trust in Government and the Provincial Health Authority and that this was a foreseeable harm from such an event.

- With the exception of some matters related to notification, I find that the steps taken in response to the cyber attack largely demonstrate that the entities evaluated risk appropriately.

c. NOTIFICATION

[144] Pursuant to section 64(3) of *ATIPPA, 2015, o*ur Office is required to be notified of a breach of personal information in the custody or control of a public body. We also required to be notified of a material breach of personal health information in the custody or control of a custodian pursuant to sections 15(4) of *PHIA* and section 5 of the *Personal Health Information Regulations*. Depending on the nature of the privacy breach, it may also be appropriate for public bodies and custodians to contact law enforcement and other professional or regulatory bodies. While notification requirements to such other entities are not specifically outlined in *ATIPPA, 2015* or *PHIA*, we do consider such notifications when assessing whether reasonable steps were taken in responding to a privacy breach.

[145] Public bodies and custodians are required to notify individuals impacted by a privacy breach in the following circumstances: sections 64(3) and 64(7) of *ATIPPA, 2015* require notification to individuals whose personal information is breached if there is a "risk of significant harm"; sections 15(3) and 15(7) of *PHIA* require notification to individuals whose personal health information is breached, unless the breach will not have an "adverse impact" on the individual.

[146] Mitigation of harm is a key consideration when a public body and/or custodian is making decisions about notification, and it is a key consideration in our assessment of what reasonable notification requires. Mitigation of harm impacts decisions about whether to notify, who to notify, how to notify, and what information to include in the notification.

[147] Once a decision is made that notifications are required, individuals are to be notified at the "first reasonable opportunity". What that "first reasonable opportunity" is, might not be the same in every case, and will depend on the particular circumstances of the privacy breach. While it could be the same day in some instances, or several days in others, public bodies and custodians are accountable for their notification decisions, including their interpretation of when they deemed "the first reasonable opportunity" to be.

[148] While notification must occur at the first reasonable opportunity, neither *Act* specifies "how" notification should occur. This means that the method of notification must be assessed based upon the particular circumstances of the privacy breach.

[149] When a public body or custodian determines notification is necessary under the *Acts*, in most circumstances, reasonable notification will require *direct* notification to affected individuals. *Direct notification* is when an individual is notified of the privacy breach in person, by telephone, mail, email, virtual meeting, or other such forms of communication. However, there may be circumstances where direct notification is not possible (for example, contact information is unavailable) and a public body or custodian must rely on indirect notification to reach affected individuals. *Indirect notification* is when an individual is notified of the privacy breach by a form of public communication. Indirect notification can include public announcements such as public advisory briefings, news releases, website notifications, social media postings, newspaper advertisements, and other such similar measures. Indirect notification must be given by a form of public communication that could reasonably be expected to reach the affected individuals. In some cases, using multiple methods of notification may be the most effective approach, for example using indirect public notification to reach as many people as quickly as possible, and then following this up with direct notification letters.

[150] Ultimately, decisions about *how* to notify individuals impacted by a privacy breach require an assessment of the particular circumstances of each case, with mitigation of harm being a key consideration. Where *direct* notification is possible, (for example, there *is* contact information) but an organization makes a decision to provide *indirect* notification instead, our Office requires public bodies and custodians to explain *why* they believe such decisions were reasonable in the circumstances. In making determinations as to whether reasonable notification steps were taken where direct notification does not occur, our Office will take into consideration many factors, including whether direct notification would cause undue hardship to the organization, and whether there are substantial and compounding issues associated with practicality, reliability/accuracy of older contact information, risks of further privacy breaches, etc.

[151] When notification is required under the *Acts,* individuals have a right and a need to receive information about the privacy breach. The notification must include enough information to allow the individual to understand the significance of the privacy breach, and include information that could assist the individual in reducing or preventing harm that could be caused by the privacy breach. Notifications should include the following information:

- Date of the breach (if the date is not known, the period during which the breach occurred, and if that is unknown, the approximate period);
- General description of the circumstances of the breach;
- Description of the information;
- Steps taken so far to control or reduce the harm;
- Future steps planned to prevent further privacy breaches;
- Steps the individual can take (a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm);
- Organization contact information that the affected individual can use to obtain further information about the breach;
- Our Office's contact information and notification of an individual's right to make a complaint.

[152] In addition to the above list, depending on the circumstances, affected individuals may have an enhanced need to know the identity of a malicious actor to make decisions and take steps to mitigate potential malicious intentions[68].

[153] What follows includes a summary of notification efforts as outlined in the Government Report and submissions received by our Office, together with our analysis and findings relating to notification.

[68]Examples found in snooping cases, and may be applicable in other "malicious actor" circumstances, such as a ransomware cyber attack: See para. 72 of Report 2018 CanLII 130517 (PE IPC) | Prince Edward Island (Health) (Re) | CanLII where the Commissioner confirms "In the case of a snooper, citizens have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions."; See paras 140-142 in Report IR23-01 2023 02 08 NSH Investigation Report.pdf (novascotia.ca) where the Commissioner found the Notification letter "possibly obscured the nature and severity of the breaches because it did not name the employee."

i. Notification Efforts – The Government Report

[154] Government's Report[69] released to the public in March 2023 includes the following public (indirect) and direct notification efforts as well as notice to other entities:

- *On **October 30, 2021**, NLCHI issued a public announcement regarding the IT systems outage, and thereafter coordinated with the province to provide regular public updates.*
- *On **October 31, 2021**, NLCHI notified the CCCS, the RNC, and the RCMP.*
- *On **November 1, 2021**, NLCHI notified the OIPC, and a public announcement was made regarding the outage.*
- *On **November 3, 2021**, a public announcement of an attack was made.*
- *On **November 8, 2021**, NLCHI notified the OIPC of the privacy breach and subsequently submitted breach reporting forms. Exfiltrated data was determined to have been taken from the Meditech data repositories and a network drive for Eastern Health.[70]*
- *On **November 9, 2021**, the RHAs were notified of the potential scope of the privacy breach and an initial public announcement was made that a privacy breach had occurred. This was followed up in the latter part of November with public announcements and notifications about resources and information for affected individuals and how they could access free credit monitoring, in addition to direct notifications to certain affected current and former employees and patients.*
- *Between **December 8 and 20, 2021**, on-going communications and updates were provided to the OIPC, by the province, NLCHI, and the RHAs. Further public announcements regarding the privacy breach were made on **December 14, 2021**.*
- *The province and RHAs provided public updates and notifications as information was confirmed regarding the personal information and personal health information involved. Identity theft and credit monitoring services were also offered and continue to be available for impacted individuals. It was also determined that certain patient health and employee information on an Eastern Health network drive was taken during the cyberattack. Eastern Health has concluded its review and notified the affected individuals as per their public statement.*
- *The appropriate authorities were notified, including the Canadian Centre for Cyber Security (CCCS), the Royal Newfoundland Constabulary (RNC), the Royal Canadian*

[69] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)*; listed notification efforts were taken from various parts within the report and do not appear as "one list".

[70] At this time, our Office was provided with the same information being presented to the public. This information did not include any mention of data exfiltration. On November 9, 2021, our Office was provided with the *technical briefing slide deck* (presented to media prior to the Public Advisory Briefing on November 9, 2021) which will be discussed further below within subsection titled "Exfiltration Notification Concerns". The Centre filed its breach reporting forms with our Office on November 15, 2021 *after* the public was advised of data exfiltration confirming that employee information (November 12, 2021) and patient information (November 15, 2021) had been taken in the attack.

Mounted Police (RCMP), and the Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC).

[155] Through release of Government's Report, the public was notified of the nature of the cyber attack and the organization behind the cyber attack.

[156] Commissioner's Delegate Finding: I find the length of time that elapsed prior to the public being notified of this being a ransomware cyber attack concerning, and the rationale provided for such a delay to be insufficient to justify it.

ii. Notification Efforts - The Public Advisory Briefings

[157] Like many other provinces throughout Canada, the Government of Newfoundland and Labrador held media briefings throughout the COVID-19 pandemic to reach and notify as many people as possible. Government officials used such briefings to speak to the population of Newfoundland and Labrador, allowing important information and updates to be provided to the people of our province in a quick and efficient manner. During briefings, once Government officials were done speaking to the public, journalists were able to ask questions, creating an opportunity for officials to provide additional details. Briefings were streamed/recorded, with the ability to watch them live online. They were often simultaneously shown on television or heard on radio. Thereafter recordings remained online allowing people to watch them later. For the purpose of this Report, this specific method of notification is referred to as a "***Public Advisory Briefing***" or the "***Public Advisory Briefings***".

[158] Public Advisory Briefings, previously used and relied upon throughout the pandemic, were used to notify the public of important information about the cyber attack, including notifications that specifically related to the privacy breach. This method allowed Government officials to get information out to as many people as possible, as quickly as possible, and was a familiar communication method to the people of our province. The majority of people impacted by this breach were *not* sent direct notification and therefore public communication measures, such as these, were the only source of notification for most of the people impacted by the cyber attack privacy breach. The following Public Advisory Briefings were held as it relates to the cyber attack:

- On **November 1, 2021,** there was an update on the IT Outage.
- On **November 3, 2021,** additional updates largely related to IT/health services.
- On **November 5, 2021,** it was confirmed our province was the victim of a cyber attack.
- On **November 9, 2021,** personal health information and personal information had been accessed the cyber attack (Eastern Health and Labrador-Grenfell Health patient and employee information).
- On **November 10, 2021,** information was accessed in the cyber attack and investigations into what, if any, data was taken confirmed as ongoing; (breach also including Central Health patient and employee information).
- On **December 14, 2021,** updates on type of information and the time ranges; information being primarily referred to as being "breached" during updates.
- On **March 30, 2022,** confirming Eastern Health Network Drive taken in the cyber attack with general description of some information impacted; review of Network Drive occurring with letters (direct notification) being sent out to those impacted thereafter; do not anticipate further updates on information in cyber attack.

[159] Officials at the briefings read from the scripts developed and prepared for them by the Department and the Minister of Health and Community Services was present at every briefing save one[71]. At times the Public Advisory Briefings were attended by a variety of other officials:

- other Government officials such as the Premier, and the Minister of Justice and Public Safety;
- the Vice President of Solutions and Infrastructure at the Centre;
- the Chief Executive Officers (CEO) of the Regional Health Authorities.

[160] Commissioner's Delegate Finding: I find the use of Public Advisory Briefings was a reasonable approach to take in providing notification to affected individuals in the circumstances of the large-scale breach caused by the cyber attack.

iii. Notification Efforts – Statements to Media

[161] The public was informed of patient and employee information being *taken* in the cyber attack by the Minister of Justice and Public Safety as indicated by the following news articles:

[71] While the Minister of Health and Community Services was not present at the December 14, 2021 Public Advisory Briefing, the Minister of Justice and Public Safety was present at this Briefing.

- on ***November 12, 2021,*** the Minister confirmed, to a news outlet on a Friday evening, that employee information was taken; and

- on ***November 15, 2021,*** the Minister confirmed *patient information was taken* in answering media questions outside of the House of Assembly.

[162] Among the many statements and interviews provided to the news media or through other public channels subsequent to the cyber attack, for the purpose of this Report, the above two are noteworthy as these were the first meaningful notifications from officials about the information being *taken* and not just accessed in the cyber attack.

[163] Commissioner's Delegate Finding: I find the timing and manner in which the public was notified of information being "taken" in the cyber attack concerning.

iv. Notification Efforts - Regional Health Authorities

[164] The CEOs of Regional Health Authorities attended various Public Advisory Briefings and in doing so assisted in providing indirect public notification by reading from the scripts prepared by the Department.

[165] The Regional Health Authorities provided a mixture of direct notification and indirect notification measures. Direct notifications included measures such as emails, meetings with staff, and letters. Indirect notification included measures like website landing pages, news releases, social media engagement, etc. This public notification campaign also included sending letters to various community stakeholders, for example, Labrador-Grenfell Health sent such correspondence to Indigenous Government leaders.

[166] Commissioner's Delegate Finding: I find the Regional Health Authorities' use of multiple methods of notification was a reasonable approach in providing notification in the circumstances of the large-scale breach caused by the cyber attack.

Not Everyone Received Direct Notification

[167] As described in detail within the earlier section titled "SCOPE OF IMPACT", the majority of people who had their information accessed and taken in the cyber attack did *not* receive direct notification; in other words, they did not receive letters or emails confirming that they were impacted. When discussing who received direct notification and who did not, it is helpful to

remember that there were two main parts of this breach: the Meditech Data Repositories and the Eastern Health Network Drive. It is also important to note that the persons impacted by the Meditech Data Repositories could be *categorized* (employees over certain time periods, and patients over certain time periods) and the "type of information" was largely similar within each of these groups (Basic Employee Information with SIN, and Patient Medical Registration Information[72]). On the other hand, due to the vast variety and volume of information of many different types, it was not feasible to organize the information on the Eastern Health Network Drive into useful categories for notification purposes. All of this resulted in the Regional Health Authorities needing to make decisions, which they did in consultation with the Department, about who would get direct notification (such as letters) and who would need to be reached through indirect public notification (briefings, websites, social media, etc.).

[168] In the Meditech Data Repositories Privacy Breach, which impacted *hundreds of thousands* of people, including the majority of the residents of our province:

- All *current* employees of the Regional Health Authorities were sent direct notification(s). This was readily and easily possible as the Regional Health Authorities had existing means of communicating with its employees in the ordinary course.

- Some, but not all, *past* employees of the Regional Health Authorities were sent direct notification. This was done by the respective Regional Health Authorities sending a letter in the mail to some, but not all, past employees based upon the last contact information on file. This means a portion of past employees who had their SIN number taken in the cyber attack were only notified through public notification measures. The impacted Regional Health Authorities had serious concerns about accuracy of employee contact information spanning ~14-28 years into the past and determined this contact information to be unreliable with letters being unlikely to reach these past employees[73].

- *All patients* impacted by the privacy breach were *not* sent direct notification (except for one very small group). This means that all such patients who had their personal health information taken in the cyber attack were only notified through public notification measures.

[72] As will be discussed in this section, while the patient medical registration information was largely similar there was an exception in that a very small number of patients had also had their SIN information collected with registration. This small group of patients were sent direct notification letters.

[73] Direct notification letters were sent to *all* past employees of Labrador-Grenfell Health as the breach of past employee information only went back 8 years. Central Health and Eastern Health had employee records going back 28 years into the past. While both entities sent out initial notification letters, no direct notification letters were sent out for the expanded portion of the employee breach. Central did not send letters to past employees from 14-28 years ago and Eastern did not send letters to employees from more than 14 years ago.

- A *very small group of (living) patients* who had a *SIN number collected* within their Medical Registration were sent direct notifications letters.

[169] In the Eastern Health Network Drive Privacy Breach which impacted approximately 66,691 individuals:

> All (living) persons who had their personal information and personal health information taken and accessed from this part of the privacy breach were sent direct notifications. Determination of who was impacted and what type of information was taken, took considerable investigation efforts for purposes of direct notifications[74].

[170] The Regional Health Authorities were faced with a large scale, unprecedented privacy breach. The patients impacted by the Meditech Data Repositories (the Patient Registration Information) included the majority of people in our province. Providing direct notification letters to each and every person who had registered for health care services during that time would have put considerable strain on the resources of the provincial health system. The living patients whose SIN information was taken were sent direct notification letters, demonstrating a useful tailored approach that took into account the harm associated with this type of information. The past employees whose contact information was considered to be accurate and reliable were also sent direct notification letters.

[171] The past employees from 14-28 years ago received indirect notification only, as contact information records were determined to be unreliable/not accurate. While ordinarily an organization may be able to dedicate resources and efforts in a smaller scale breach to locate persons impacted to obtain reliable contact information and send direct notification, this was not reasonably feasible in the circumstances due to the sheer magnitude and inherent

[74] It was confirmed that over 200,000 files were taken in the cyber attack from the Eastern Health Network Drive. Subsequently, extensive investigation efforts were required to first identify files potentially containing personal information and personal health information, and then a subsequent manual review was required to investigate the over 200,000 files to identify privacy breaches. Such extensive efforts meant individual notification letters were being sent out well after the cyber attack took place. This resulted in a series of different letters going out in batches with the last of these letters being released in 2023. Eastern Health explained that in April 2022 a first batch of letters were sent out to living patients who had attended the St. John's Breast Screening Centre (36,909), between December 2022 to ~ February 2023; additional batches were sent out at different times to other patients (31,277) and employees, including locums and physicians (281). In total 68,467 letters were sent out (although Eastern Health does note that 1,495 people had received more than one letter for this breach, making the number of letters sent to ***unique*** living individuals who impacted by this breach to be 66,691).

challenges of such an undertaking in light of the available resources to carry it out. The inherent unreliability and inaccuracy associated with the records from 14-28 years in the past, the significant magnitude of the breach, and resource limitations created substantial and compounding problems, and in the face of such problems, reasonable notification steps were taken. While it is concerning that SIN information for such past employees was breached, there were numerous indirect public notification measures taken by the Regional Health Authorities and also through the Department's organization of Public Advisory Briefings, and this portion of the breach was able to be meaningfully categorized.

[172] The patients and employees whose information was taken in the Eastern Health Network Drive Breach did receive letters but those letters came *well after* the cyber attack took place. The cyber attack happened in October 2021 and some people impacted by this portion of the breach were still receiving their letters this year. This resulted in frustration for some, and confusion for others. Indirect public notification was provided on this portion of the breach through the March 30, 2022 Public Advisory Briefing, and other means (such as website postings) to provide warning as to this portion of the breach which had no easy or meaningful category. After investigation efforts, which did take substantial time, direct notification letters were sent out.

[173] Commissioner's Delegate Finding: I find that reasonable notification measures were taken by the Regional Health Authorities to notify individuals impacted by the cyber attack.

[174] Recommendations for the Provincial Health Authority involving notification are discussed below.

v. The Department's Role in Notifications and Centre's Role in Investigating

[175] Prior to addressing issues about exfiltration and ransomware notifications, it is important to understand the Department's role in cyber attack notifications and the Centre's role in cyber attack investigations.

[176] As noted in the "BACKGROUND" section above, the Department is tasked with providing leadership, coordination, and support to the Regional Health Authorities and the Centre. The

Minister has the authority to direct the Regional Health Authorities[75] and the Centre[76] and those entities are required to comply. During the cyber attack, the Department did take on a leadership role, largely as it relates to cyber attack notifications, to support the Centre and the Regional Health Authorities. Through Shared Services, the Centre's mandate was expanded to include responsibility for information technology and information security[77] for the Regional Health Authorities. Following the cyber attack, the Centre was largely responsible for pursuing the investigations into the cyber attack, including engaging with third party experts.

[177] The Department's submissions speak to a coordinated approach to public notifications amongst the Centre, the Regional Health Authorities, and itself, noting that the "Provincial Government coordinated public notifications, updates and advisories with the [Regional Health Authorities] and [Centre] on the cyber attack due to its province-wide impacts." The Department describes how "[the Centre] communicated with [the Department] with information and updates regarding the investigation and response to the cyber attack to inform the Public Briefings and coordinated with [the Department] regarding the information included in the Public Briefings." The Centre's submissions largely align with the Department's, stating it (the Centre), "consulted, coordinated and collaborated closely with [the Department] regarding updates and notifications regarding the cyber attack."

[178] The Regional Health Authorities provided our Office with detailed submissions and timeline records. While the Regional Health Authorities do describe extensive collaborative communication efforts, especially as it relates to rebuilding and restoring the health care IT

[75] At the time of the attack, the Department (the Minister) had the power to exercise this authority under sections 3 to 5 in the *Regional Health Authorities Act*, SNL 2006, c R-7 and section 4 of the Department's Regulation *NLR 98/19*. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which includes all Regional Health Authorities) per sections 3 to 5 of the new *Provincial Health Authority Act*.

[76] At the time of the attack, the Department (the Minister) had the power to exercise this authority under section 5 of the *Centre for Health Information Act*, SNL 2018, c. C-5.2. Today the Minister continues to have the authority to direct, control, and approve funding for this singular Provincial Health Authority (which now includes the Centre) per sections 3 to 5 of the new *Provincial Health Authority Act*.

[77] The wording used within the Minister's directive letter to the Centre described this as "information technology and telecommunications (e-Health)". Under the Centre's Act, it refers to this as "information systems", and the Act's terms when read together, confirming that the Centre is responsible for the management, operations and security of the "information systems" of the Regional Health Authorities.

systems, the roles attributed to the Department and the Centre as it relates to notifications concerning the privacy breach are described somewhat differently, with Regional Health Authorities' submissions stating:

- *The "sole source of information" for the privacy breaches was the Centre and "at times the information received was slow, inaccurate, and changed over time."*
- *"The Department scheduled several media briefings in the period following the cyberattack. These media briefings were attended primarily by one or more Government representatives (the Premier, the Minister of Health and Community Services, the Minister of Justice and Public Safety) and representatives from [the Centre]". At times, one or more RHA CEOs would attend. The communications at the media briefings were prepared by the [the Department]."*
- *"As part of its response to the Cyber-Incident, [the Department] controlled the messaging (including the timing and wording of notifications) that were to be communicated from [the Regional Health Authority] to the public and its staff. [The Regional Health Authority] required approval from [the Department] prior to releasing notifications. [The Regional Health Authority] did not have direct access to information regarding the breach and its impacts, nor did it have ultimate control over its outward communications."*
- *While the Regional Health Authority "was the face of the communications efforts with the public and employees relating to privacy breaches, the truth was that [the Centre] was controlling the investigation and the [Department] was controlling the messaging."*

[179] Given the legislated mandates of the entities, it is understandable how the Department's role included overseeing the cyber attack related notifications, while the Centre worked on cyber attack related investigations. In the circumstances of such a large-scale cyber attack where there were several different public bodies/custodians and several different aspects being addressed (a privacy breach, a security breach, and the overall continuation of health care services) it is reasonable for different organizations to focus on different aspects. Given the entirety of these circumstances, although the Regional Health Authorities were frustrated in having to rely upon the Centre for information about the breach and the Department for notifications, overall this was a reasonable approach to managing this challenging set of circumstances.

[180] Commissioner's Delegate Finding: I find the Regional Health Authorities' reliance on the information provided to it by the Centre for Health Information to be reasonable in the circumstances.

[181] Commissioner's Delegate Finding: I find the Department's role in overseeing and managing notifications and the Centre for Health Information's role in investigating the cyber attack and resulting privacy breach reasonable in the circumstances.

vi. Exfiltration Notification Concerns

[182] While we take no issue with decisions made on the primary roles and functions taken on by each entity, the same cannot be said for how some information was released to the public.

[183] The Department and Centre both had intimate knowledge of, and were involved in, the response to the cyber attack. The Department confirmed in its submissions that updates during November 2021, including updates on evidence of exfiltration, "were provided daily, and sometimes more frequently, to officials of the [the Department] by [the Centre's] officials. Specifically, information was received by the Deputy Minister of the Department of Health and Community Services from [the Centre's] officials."

[184] Officials received evidence of data exfiltration between November 5, 2021, and November 9, 2021. The Centre explained the general process of how this evidence was used to draw conclusions about exfiltration scope and this approach was reasonable in the circumstances. By November 8, 2021, the Centre had made the determination that data, containing patient and employee information, was taken in the cyber attack. The Department was made aware of this through its frequent communications with the Centre[78].

[185] The Department and the Centre *knew* that the highly sensitive information being described at the initial privacy breach Public Advisory Briefings had been *taken* by the Threat Actor, but failed to provide this warning to the public. Instead of being discussed at the far-reaching Public Advisory Briefings, the fact that patient and employee information had been *taken* in

[78] The Centre states that it had confirmed the data exfiltration to the Regional Health Authorities. However, the Regional Health Authorities, whose records were detailed and consistent, confirm the Centre initially advised of there being a "privacy breach" of patient and employee information on November 7, 2021 and that this information was taken occurring later (November 11, 2021, or later).

the attack was released later and in a limited manner. The relevant timeline during this period is as follows:

- **November 5 to November 9, 2021,** Evidence of Data Exfiltration;
- **November 8, 2021,** Determination of Data Exfiltration (patient and employee information *known* to be taken in the cyber attack);
- **November 9, 2021**, Public Advisory Briefing stating information had been accessed in the cyber attack (Eastern and Labrador-Grenfell Health);
- **November 10, 2021,** Public Advisory Briefing stating information had been accessed in the cyber attack (Central Health) and investigations into what, if any, data was *taken* confirmed as ongoing;
- On ***November 12, 2021,*** the Minister confirmed employee information was taken to a media news outlet on Friday evening; and
- On ***November 15, 2021,*** the Minister confirmed patient information was taken in answering media questions outside of the House of Assembly as discussed news media articles.

[186] Our questions to the Department and the Centre *pointed* to the evidence of data exfiltration, *pointed* to the Centre's determination of data exfiltration, *pointed* to this information only being released to the public later through news articles, and *asked* them to explain the reason why this information was not released earlier. The Department's and the Centre's answers to our questions demonstrate a lack of transparency and accountability. The answers we received consisted of the following:

- there was ***no delay***; and
- the public ***was told*** that personal information and personal health information was taken on November 9, 2021

[187] The Department's and the Centre's positions are not supported by the video evidence, and are not supported by the detailed records and submissions of all of the Regional Health Authorities[79]. The evidence relied upon by the Department and the Centre, to show that the

[79] The detailed records and submissions of the Regional Health Authorities show that they were informed of information being *accessed* and were to use this wording throughout all of its notifications; the Regional Health Authorities both confirm receiving confirmation from the Centre that data had been taken on or after November 11, 2021.

public *was* told of information being taken as of November 9, 2021 is overly selective and ultimately fails to support their positions:

- both entities point to the *Department's website* as being one of the "primary" notification methods;
- the Centre points to a *technical briefing slide deck* released to media prior to the on November 9, 2021, Public Advisory Briefing[80]; and
- the Centre points to a news article from November 9, 2021[81].

[188] The Department and Centre are now relying upon the Department's website and the technical briefing slide deck because both sources did state that personal information and personal health information was "obtained" in the cyber attack. However, the Department and Centre failed to acknowledge many flaws in this position: the *actual content* of the November 9, 2021, and November 10, 2021, briefings, reliance on a singular "primary" source within a multi-source approach, and the fact that the use of the word "obtained" (appearing on the website and within the technical slide deck), was specifically walked back by officials at the November 10, 2021, briefing. While the Department and the Centre are *now* maintaining that the public *was* notified of information being taken (stolen) in the attack as of November 9, 2021, the following statements by Government officials at the November 10, 2021, Public Advisory Briefing clearly tell a different story:

> *Please know that* ***the information and language we use is deliberate and intentional****. As previously said, based on investigations to date, we* ***currently understand that certain data was accessed. The investigation is also focusing on the impact of that of that access to determine what, if any, data was taken. Access is different than exfiltration.*** *To reiterate we have no evidence at this time that the information accessed has been misused.*
>
> - Minister of Justice and Public Safety

[80] This technical briefing slide deck was developed and distributed by the Department and given to media prior to the November 9, 2021 Public Advisory Briefing.

[81] This is an article from November 9, 2021 that references information being stolen and obtained, and has a media interviewer who asks questions using language of "stolen" and "obtained"; Answers provided by the Premier stated we do not know that information right now, there's an ongoing investigation, and confirms there was "unauthorized access", the extent of which is not known; the Premier does not state that information was stolen in this interview; it also references an answer Eastern Health CEO had provided at the briefing. At the actual briefing the CEO had been asked "…if somebody's been to say Eastern Health in the last 14 years as a patient should they just assume that their information has been taken?" His answer was "I think the answer to that is yes." While this may have been sound advice (to Eastern Health Patients) it was certainly not sufficient notification that this data had been taken; nor does the article serve that purpose, especially given comments made by the Minister of Justice and Public Safety and the Minister of Health and Community Services at the November 10, 2021 Public Advisory Briefing.

> ***…****[D]o we have evidence that the data was accessed? And what I've been saying to people who've asked me this question is sort of to think about it in terms of maybe your own workplace and for example in my department, the department of justice and public safety, I have access to all kinds of information. It doesn't- certainly doesn't mean that I've taken it, and it certainly doesn't mean that I've stolen it. So there is- that is the reason for the distinction****. In the cyber world and specifically access to that data, this bad actor has access and had access to data at some point in time, does not mean that it was copied, it does not mean that it was taken****. The ongoing investigation will lead us to a conclusion about whether that has happened but at this time we have no evidence that any of the accessed data has been misused.*
>
> - Minister of Justice and Public Safety

> **Media Question:** I have a question for, I guess this is probably for [the Minister of Health and Community Services]. In our Technical briefing yesterday we received a package of documents. I'll read you a line – it says "we understand that some personal information and some personal health information was obtained from our system." How we do reconcile that with the message that we're getting today that information was just accessed?
>
> *I think that may be a difference in uses of words. We have, certainly [the Minister of Justice and Public Safety] and I, have* ***discussed really tightening our use of words to reflect more accurately what we understand the situation to be. You know, accessed and obtained are different verbs, they're different words and mean different things. Our understanding as of today, is that that information was accessed. Whether it was further altered, or taken away, or copied, that is not clear****. What we can say at the moment is from our experts involved in the field, we have no evidence of it being misused.*
>
> -Minister of Health and Community Services

[189] Even if officials were simply relying on expert advice not to release this information during an active situation as it could lead to harm, we note the following:

- This is not the actual position that either the Centre or the Department put forth to our Office;
- There is a heightened risk of harm that exists when a malicious actor successfully *take*s data (containing personal information/personal health information). The above language of "access" being used at this conference and the emphasis on the distinctions between "accessed" and "taken", were an inaccurate account of what was known by officials at that time, and ultimately minimized the risk of harm;

- The Department and the Centre were provided with ample opportunity to provide our Office with submissions to explain why this information was not released earlier to the public; and
- Both entities failed to provide us with any evidence to support the decisions they made as it relates to privacy breach notifications.

[190] With a large scale breach, where notifications are being released in a variety of formats to get the information out to as many people as possible, as quickly as possible, reliance on accurate information being contained within one "primary" source is unreasonable. Accuracy of information, especially key information, is required throughout all methods of notification. When information is released in such a broad and quick manner, it is understandable that information initially released may change over time as more detailed investigations continue[82]. However, the circumstances here are different: key information was already *known* by both the Centre and the Department and withheld from the public. Rather than provide our Office with a clear explanation for *why* this information was initially withheld from the public, both entities chose to ignore the issues we raised.[83]

[191] An additional concern is that a Public Advisory Briefing was never actually held with its key message being that information had been *taken* in the attack. Instead, this information was, for all intents and purposes, dumped into the news cycle on a Friday evening and followed up somewhat on Monday in a question period. Even at the December 14, 2021 Public Advisory Briefing, the key messages given by officials to the public no longer used "accessed", but that messaging did not use the word "taken" either. Rather, officials largely referred to the updated information being "breached" when reading their messaging. This was the first Public Advisory Briefing held where a key message of information being *taken* could have been given. This opportunity was missed.

[82] Such as what occurred in this matter: Initial information type and date ranges were provided at the November 9, 2021 and November 10, 201 Public Advisory Briefings, and thereafter adjusted at the December 14, 2021 Public Advisory Briefing.

[83] While there *could* have been a reasonable explanation for this delay, and while our Office *did* ask what those reasons for the delay were, what our Office received (after waiting over four months for the Department and the Centre to answer the questions put to them in January 2023) failed to include *any* explanation for the delay whatsoever; instead denial that a delay had even occurred.

[192] We note that while officials at the November 10, 2021 briefing repeatedly emphasized information was "*accessed*" and had repeatedly emphasized that "*accessed is different from taken*", there was never any equal emphasis (or emphasis whatsoever) provided to the public on the information being "*taken*". We would have expected officials to highlight the fact that the information was *stolen* by a malicious actor, in the same manner or greater than when describing it as being accessed and this simply was not done. However, regarding the December 14, 2021 briefing, we do acknowledge that, while the key messaging to the public used the language of information being "breached", the language of "taken" was eventually being used at this briefing later on. In addition to this, we also note that the other various forms of notifications did adopt the language of "taken" as well.

[193] While it is concerning that the public was not informed at an earlier stage that information was taken in the cyber attack, nor was it a key message within a Public Advisory Briefing in 2021, the fact that this information was taken by a Threat Actor in the cyber attack did become known through the various methods of notifications used by the Department and the Regional Health Authorities.

[194] Commissioner's Delegate Finding: I find the initial delay in confirming the existence of the cyber attack privacy breach (the delay between November 1, 2021 up to when the public was first informed of the privacy breach on November 9, 2021) reasonable in the circumstances.

[195] Commissioner's Delegate Finding: I find, that as of November 8, 2021, the Department and Centre knew that personal information and personal health information was both accessed and taken (exfiltrated) by the Threat Actor in the cyber attack.

[196] Commissioner's Delegate Finding: I find, that at the Public Advisory Briefings held on November 9, 2021 and November 10, 2021, the Department was in a position to notify the public that the information being described as accessed, was in fact taken (exfiltrated) by the Threat Actor in the cyber attack and failed to do so.

[197] Commissioner's Delegate Finding: I find that the impacted public was not informed at the first reasonable opportunity of personal information and personal health information being

taken in the cyber attack, as required by section 15(3) of *PHIA* and section 64(3) of *ATIPPA, 2015*.

vii. Ransomware Notification Concerns

[198] As stated above, when notification is required under the *Acts*, the content of that notification must include enough information to allow the individual to understand the significance of the privacy breach, and include information that could assist the individual in reducing or preventing harm that could be caused by the privacy breach. It is important to note that the likelihood of harm resulting from a privacy breach is increased where the personal information and/or personal health information is compromised due to the malicious actions of a Threat Actor. This includes breach of information due to a *ransomware cyber attack,* where there is deliberate intrusion, deployment of ransomware, exfiltration of the information, and/or threats of disclosure[84]. Impacted individuals should be informed, at the earliest reasonable opportunity, of the nature of the attack and be provided with an explanation of the implications, including if there are threats to release their information.[85] Knowing this type of information may assist an individual in making decisions about protecting themselves, including decisions about engaging in mitigation measures (for example credit monitoring) at all, or decisions about how quickly to engage in such measures.

[199] On January 9, 2023, we put questions to the Department asking why this type of information (the fact this was ransomware cyber attack perpetrated by HIVE ransomware group) had not yet been released to the public. Our questions[86] on this topic stated the following:

---

[84] See Notification Decisions involving privacy breaches due to ransomware from the OIPC Alberta Examples: P2022-ND-065.pdf (oipc.ab.ca) and P2022-ND-063.pdf (oipc.ab.ca) While these are decisions about notification, confirming that notifications are required due to the real risk of harm, these decisions are also specifically and consistently positing the nature of the cyber attacks as being *ransomware* cyber attacks.

[85] Examples found in snooping cases, and maybe applicable in other "malicious actor" circumstances, such as a ransomware cyber attack: see paragraph 72 of Report 2018 CanLII 130517 (PE IPC) | Prince Edward Island (Health) (Re) | CanLII where the Commissioner confirms "In the case of a snooper, citizens have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions." See paras 140-142 in Report IR23-01 2023 02 08 NSH Investigation Report.pdf (novascotia.ca) where the Commissioner found the Notification letter "possibly obscured the nature and severity of the breaches because it did not name the employee."

[86] During our investigation, in an effort to respect the Department and Centre's decisions (at the time) to limit the knowledge of this being a ransomware cyber attack, we drafted questions about this particular topic in a neutral and general manner (without this information being within the questions). This was done so that our

> *Our Office is aware of the exact nature of the Cyber Attack. We understand that at the time of the cyber attack there was also an awareness of the exact nature of the Cyber Attack within [the Department]. However this information has not been confirmed to the public.*
>
> *It was identified to the public early on via Public Advisory Briefings that answering questions, including those regarding this specific topic could not be released as this was an "active" situation and is what the retained experts were advising. It appears that active dealings stopped by the end of 2021. Further a written advisory from the [the Department] issued on 30 MAR 2022 stated:*
>
> > *At this late stage of the investigation, it is believed that the full extent of the incident is understood, and further updates regarding the breach of information as a result of this incident are not anticipated.*
>
> *The Commissioner will need to consider from an accountability perspective whether the likelihood of significant harm resulting from this incident was increased as a result of the exact nature of the cyber attack. The Commissioner will also need to consider whether knowing the exact nature of the cyber attack may have impacted the decision making of those who could have had their information breached (e.g. the exact nature of the cyber attack may be the determining factor for someone to register for the credit monitoring, or it might have caused a person to register for credit monitoring sooner). Given these type of considerations, I am trying to understand why this information (the exact nature of the cyber attack) was not and is not being released to the public as part of compliance with the notification obligations under the Acts.*
>
> *Given that the [the Department] maintained/maintains control over notifications, messaging and public briefings concerning the cyber attack, why has this information, ie the exact nature of this cyber attack, not been released to the public and individuals specifically impacted by the cyber attack? If applicable, please provide a detailed explanation on why [the Department] believes that this information should not be released. (If applicable) If the [the Department] is relying upon the expert opinions or advice of others please provide confirmation of what such opinions or advice entailed and the evidence upon which this opinion or advice is based.*

[200] On January 4, 2023, we also put similar questions to the Centre. We did not receive any responses from the Department or the Centre until mid-April 2023. In the interim period, on March 14, 2023, the nature of this attack was unexpectedly confirmed through release of

"questions document" could be more easily circulated within each entity to gather information and answers. Notably, our questions document sent to the Department was subsequently released into the public domain when the Provincial Government filed them with its court application the day after telling the public about ransomware/HIVE ransomware group through release of its report.

Government's Report[87], informing the public that the 2021 cyber attack had been a ransomware cyber attack that was perpetrated by the HIVE Ransomware Group. While our Office was pleased to see this information finally released, we nevertheless continued to wait upon the Department's and the Centre's answers and evidence as to why this information had not been previously released to the public and affected individuals.

[201] When the responses to our questions were received in mid-April 2023, no meaningful answers were provided as to why this information could not have been released previously[88]. The Department and the Centre did answer the question, but chose to answer by merely stating, "A report was released to the public in March 2023" providing the link to Government's Report[89].

[202] Neither the Department nor the Centre provided our Office with any answers as to why it took almost 500 days for this information to be released to the public, nor did either entity provide any evidence that would support such an excessive delay. As stated above, once a decision is made that notification is required, individuals are to be notified at the "**first reasonable opportunity**". No **evidence** or submissions were provided to our Office that would justify any delay[90], let alone a delay of almost 500 days.

---

[87] See *Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023)*; listed notification efforts were taken from various parts within the report and do not appear as "one list";

[88] Our questions were sent in early January 2023 and both entities sought extensions for a variety of reasons. Eventually, we confirmed an expectation for partial answers to be provided by March 15, 2023 with full answers to follow on March 31, 2023. On March 15, 2023, no partial answers were provided and instead we received the Provincial Government's court application, which outlined that the Department fully intended to cooperate with our investigation if Commissioner Harvey no longer had carriage of the matter. Later that evening, the Centre followed suit stating that "*Given the subject matter of the application and its direct implications for the OIPC's investigation, NLCHI will not be sending responses to the OIPC's questions and recent requests for additional information pending the outcome of the application*". Fortunately, these delays were avoided as the Commissioner promptly appointed a delegate to take responsibility for the matter and we immediately confirmed that full answers were to be provided by April 10, 2023. After four months of waiting for answers, a portion of responses received (which includes the one being discussed in this paragraph) were overly vague, failed to answer the question entirely, or failed to address the specific concerns we had raised.

[89] The Centre's answer was similar in content, differing slightly in wording stating "This information has been released in a March 2023 report "Cyberattack on the Newfoundland and Labrador Health Care System", which was announced on the Cyber Incident Site described above, and which is available for download at the following link: https://www.gov.nl.ca/hcs/files/OVERVIEW-NL-Health-Cyber-Incident-March-2023.pdf."

[90] For example a small purposeful delay in notifying an individual ***may*** be reasonable in circumstances where law enforcement authorities are engaged (as part of the containment strategy of the breach in question) so as to not impede a criminal investigation; However, there must be actual evidence supporting this position – evidence showing that law enforcement have specifically requested notification not occur with reasons set out why notification would impede the criminal investigation. See paragraph 112-115 2019 NSOIPC 2 (CanLII) | Department of Internal Services (Re) | CanLII.

[203] While responses to our investigation were lacking on this point, media articles[91] do, however, reference the Minister of Justice and Public Safety's statements made with the release of Government's Report:

> *U.S. law enforcement officials announced in January that they had dismantled the Hive ransomware network.*
>
> *[The Minister of Justice and Public Safety] said that disclosure cleared the way for officials in Newfoundland and Labrador to finally say who was responsible for the attack that targeted their systems 18 months ago.*
>
> *"One[92] of the reasons again, I want to stress, that we're able to reveal who the entity is, is because of the work that was done in the States by the Department of Justice there," [the Minister] said.*
>
> *"**We now know that the threat has been extinguished. So now that that doesn't exist any more, we feel we're safe to disclose it to the public. Doing so any earlier would have still, we felt, put systems at risk**."*

[204] The statements made by the Minister of Justice and Public Safety do not provide the necessary evidence that would support any delay in notification, let alone an excessive delay.

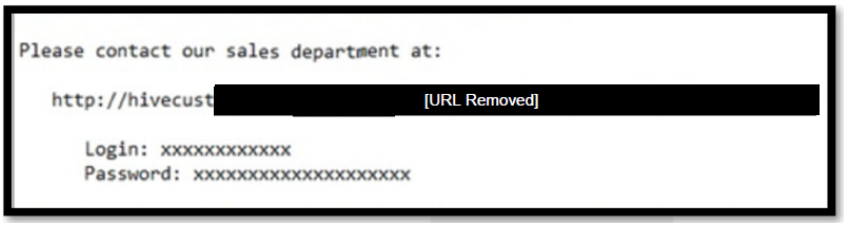
Minister Statement: "*the threat has been extinguished*"

[205] In our view, this is not an accurate representation of what occurred on January 26, 2023 with the United States Department of Justice announcement.[93] While the HIVE ransomware group's *infrastructure* was dismantled (described as a *disruption of HIVE's computer networks)*, the malicious actors themselves who ran and operated HIVE ransomware group, ***and*** the other malicious actors who used HIVE's "services" are still very much out there and, to the best of our knowledge, have not been arrested. While HIVE ransomware group was disrupted, its members may very well remain active. We also note that there are other ransomware groups.

---

[91] N.L. says Hive ransomware group was behind 2021 cyberattack on health systems | CBC News.
[92] Regarding the comment of this being "one of the reasons": Our function in investigating a privacy breach is not to scour news articles to come up with reasons to support the positions being taken by entities under investigation. Rather, an entity must provide our Office with its submissions and evidence it is relying upon. We raise this point in the event that other reasons are later found within other news articles, or in the event that subsequent reasons are later stated to the public after the publication of this Report. The Department noted in its court application that it intended to fully cooperate with our investigation, and part of that full cooperation entails providing our Office with complete responses and evidence to support the positions taken in this matter.
[93] *Announcement* on Disruption of Hive Ransomware dated January 26, 2023.

[206] Calling out HIVE by its name, even *prior to* its infrastructure being dismantled, would not have made HIVE ransomware group any "*more*" of a threat than it already was (in the general sense); HIVE (as an organization) did not want to remain "anonymous" - quite the opposite – HIVE (like other ransomware-as-a-service groups) *wanted* to be known as a "legitimate business." This can easily be seen in the ***example*** ransom note[94] which refers its example victim to "hive" in the website location, and asks the victim to contact its "sales department":



[207] Even if we considered this to be a reasonable position to take (which we do not), this does not explain the delay between when the HIVE ransomware group's infrastructure was announced as being dismantled on January 26, 2023, up to the release of the Government's Report on March 14, 2023. Officials cannot claim a lack of awareness, as our Office sent correspondence to both the Department and the Centre the next day (January 27, 2023) asking to be advised if any of the information taken in the 2021 cyber attack was seized by USA officials.[95]

[208] In addition, even if officials believed that HIVE *itself* could not be named, this does not explain why officials did not confirm this was a ***ransomware*** cyber attack much earlier. Ransomware cyber attacks are readily and actively disclosed by other organizations that have

[94] See Cybersecurity & Infrastructure Security Agency's Website (USA) for full example note; See also cbc news article interview with a security expert "At the end of the day, there will be no retaliation if you were to say what happened. In fact, these gangs kind of want you to talk about it."

[95] Our January 27, 2023 letters to the Department's and Centre's lawyers (through which investigation communications were conducted) stated: "*Further to recent news reports [linked in a footnote], it is our understanding that HIVE infrastructure was recently dismantled and seized by law enforcement. Given this development, we ask that you please keep us informed should relevant information pertaining to the October 2021 cyber attack be released to you/your client. For example, we ask that you please advise our Office should law enforcement find continued existence of personal information and/or personal health information that was taken in October 2021 cyber attack…*" We did not receive any acknowledgment or response to this inquiry from either the Department or the Centre.

fallen victim[96]. No evidence or answers were provided explaining why authorities in this province believed they could not identify ransomware as being the sources of the cyber attack.

> Minister Statements: *"we feel we're safe to disclose it to the public. Doing so any earlier would have still, we felt, put systems at risk."*

[209] It is unclear how systems would be put at risk as no actual evidence was provided to our Office supporting this statement. Feelings and beliefs must be reasonably held, *and* supported by actual evidence, when being used to justify withholding important notification information from the public and from the affected individuals.

[210] Again, while we are pleased that officials decided to release this information, after being faced with our questions raising concerns over why this information was not yet released, we continue to have serious concerns over the lack of transparency and evidence to justify past actions taken with respect to notification.

[211] Commissioner's Delegate Finding: I find the public was not informed of this being a ransomware cyber attack, nor of this attack being perpetrated by the HIVE ransomware group at the first reasonable opportunity.

[212] Commissioner's Delegate Finding: I find the content of notifications made about the privacy breach should have included more details about the nature of the attack, namely that it was a ransomware cyber attack together with other general details, such as confirmation that a Threat Actor exfiltrated/stole data containing personal information and/or personal health information for malicious purposes.

viii. Summary of Commissioner's Delegate Findings

[213] The following findings are made regarding notification:

- I find the length of time that elapsed prior to the public being notified of this being a ransomware cyber attack concerning, and the rationale provided for such a delay to be insufficient to justify it.

[96] See February 27, 2023 News Article where US Marshals stated *within one week "it had* discovered a ransomware and data exfiltration event affecting a stand-alone USMS system"; See Notification Decisions involving privacy breaches due to ransomware from OIPC Alberta Examples: P2022-ND-065.pdf (oipc.ab.ca) and P2022-ND-063.pdf (oipc.ab.ca) specifically and consistently positing the nature of the cyber attacks as being *ransomware* cyber attacks.

- I find the use of Public Advisory Briefings was a reasonable approach to take in providing notification to affected individuals in the circumstances of the large-scale breach caused by the cyber attack.
- I find the timing and manner in which the public was notified of information being "taken" in the cyber attack concerning.
- I find the Regional Health Authorities' use of multiple methods of notification was a reasonable approach in providing notification in the circumstances of the large-scale breach caused by the cyber attack.
- I find that reasonable notification measures were taken by the Regional Health Authorities to notify individuals impacted by the cyber attack.
- I find the Regional Health Authorities' reliance on the information provided to it by the Centre for Health Information to be reasonable in the circumstances.
- I find the Department's role in overseeing and managing notifications and the Centre for Health Information's role in investigating the cyber attack and resulting privacy breach reasonable in the circumstances.
- I find the initial delay in confirming the existence of the cyber attack privacy breach (the delay between November 1, 2021 up to when the public was first informed of the privacy breach on November 9, 2021) reasonable in the circumstances.
- I find, that as of November 8, 2021, the Department and Centre knew that personal information and personal health information was both accessed and taken (exfiltrated) by the Threat Actor in the cyber attack.
- I find, that at the Public Advisory Briefings held on November 9, 2021 and November 10, 2021, the Department was in a position to notify the public that the information being described as accessed, was in fact taken (exfiltrated) by the Threat Actor in the cyber attack and failed to do so.
- I find that the impacted public was not informed at the first reasonable opportunity of personal information and personal health information being taken in the cyber attack, as required by section 15(3) of *PHIA* and section 64(3) of *ATIPPA, 2015*.
- I find the public was not informed of this being a ransomware cyber attack, nor of this attack being perpetrated by the HIVE ransomware group at the first reasonable opportunity.
- I find the content of notifications made about the privacy breach should have included more details about the nature of the attack, namely that it was a ransomware cyber attack together with other general details, such as confirmation that a Threat Actor exfiltrated/stole data containing personal information and/or personal health information for malicious purposes.

ix. Commissioner's Delegate Recommendations on Notification

[214] The following recommendations are made regarding notification:

> I recommend the Provincial Health Authority provide an update within its communications (such as each region's website landing pages for the 2021 cyber attack) confirming this was a ransomware cyber attack and providing a link to Government's Report which outlines more details about the attack and prevention steps being taken.

> I recommend that the Provincial Health Authority update notification policies to reflect that where there is a breach of personal information or personal health information (where notification is required under an Act), that in the case of a ransomware cyber attack, notification should include information about those circumstances at the earliest reasonable opportunity, and furthermore that the factors considered in making such decisions about notification must be documented.

d. Prevention of Future Breaches

[215] An important step in managing a privacy breach is prevention. It is essential for a public body or custodian to conduct the investigations required to fully understand what happened, to be able to identify the root causes, and to evaluate the factors that contributed to it occurring. This is key in mitigating the risk of a future breach and the end result should be that the risks identified during the entity's investigation are addressed to the fullest extent possible. As discussed in the Privacy Breach Protocol there are many steps and plans that may be required: Investigations in the form of security audits into physical and technical security, development or improvement of long-term safeguards, reviewing and updating policies to reflect lessons learned from the investigation, additional training of staff, and conducting an audit at the end of the process to ensure that a prevention plan has been fully implemented.[97]

i. Cyber Security

[216] Large organizations that have become victim of an extensive ransomware cyber attack will often retain the assistance of third party cyber security experts who have the experience and expertise to effectively assist with the cyber incident response. Investigations are conducted to determine if the attackers are still active in the system, if they left anything behind (that

[97] See Privacy Breach Protocol.

would let them back in later), and uncover where they went within the systems to determine if data was accessed and taken.

[217] Through the Centre's legal counsel, a company called CrowdStrike was engaged to assist in its incident response efforts. CrowdStrike produced a post-incident Forensic Report titled "Investigation Summary" prepared for the Centre dated June 30, 2022. CrowdStrike conducted "*a forensic analysis of systems and logs to determine evidence of Threat Actor or exfiltration data, earliest and most recent dates of Threat Actor activity, determining how the Threat Actor gained access to the systems, [and] what systems if any, the Threat Actor moved laterally to within the NLCHI-managed environment*." The detailed evidence within the CrowdStrike Report provides the foundation for the overview of facts found within Government's Report explaining, at a high level, the movement of the Threat Actor within the health information systems.

[218] The Centre also sought the assistance of the Canadian Centre for Cyber Security who provided a post-report titled "CCCS Report Pertaining to: NL Health Authority Reviews and Recommendations" dated May 25, 2022. The purpose of this document was stated to be "*to provide advice and guidance to [the Centre] as provided from the combined efforts of the CCCS teams on the ground and the teams who have been working in Ottawa to assist in recovery and providing guidance moving forward. This document will also serve as a reference for [the Centre] as they move forward in rebuilding their systems*."

[219] Commissioner's Delegate Finding: I find that the necessary investigations were conducted to determine, to the extent possible, the root causes of the privacy breach and the cyber attack as a whole.

[220] While we cannot provide the details contained within the post-incident reports, it is clear that there were a number of factors that contributed to the cyber security breach. There were security gaps where the necessary controls were not in place at the time of the cyber attack, or were not consistently applied across the health system. The security gaps identified within the post-incident reports also revealed the weaknesses and deficiencies of our province's health care information system's overall cyber security posture. While substantial progress

has been made in addressing these vulnerabilities across the entire health care environment, it would be premature and would risk further harm to the security of personal information and personal health information for us to disclose specific details about those vulnerabilities in this Report. In an effort to assist the Provincial Health Authority, we are attaching a **confidential annex** to this Report which highlights the specific cyber security vulnerabilities that contributed to this privacy breach and identifies the missing controls that correspond with the Threat Actor's actions and movement within the health care information systems.

[221] In an effort to improve the health care information system's cyber security posture, the Centre put forth a funding request to pursue a security assessment to identify vulnerabilities (subsequent to the cyber attack) and provide it with recommendations as to how to move forward in addressing those vulnerabilities. On March 31, 2022, the Centre received funding approval "to enter into a contract with a company called Gartner to conduct a security assessment and develop a security strategy" (the "**Gartner Assessment**"). The Centre stated within its submissions that:

> *Gartner reviewed [the Centre's] current-state security, taking into account changes made by [the Centre] since the Deloitte Assessment, and made a set of recommendations which have been incorporated into Project Breakwater (along with input from [the Canadian Centre for Cyber Security], Public Safety and CrowdStrike). Accordingly, under Breakwater, [the Centre] is addressing the most current and relevant set of recommendations it has received*.

[222] As stated in Government's Report,[98] Breakwater (the plan containing a series of security-related projects developed after the cyber attack), is described as "a *coordinated and multi-disciplinary effort led by [the Centre] and the [Regional Health Authorities] to counter the risks of cyber threats and to create resiliency against future attacks. Active priority work in Breakwater continues to this day as part of a roadmap to enhancement of cybersecurity for the provincial health systems."* That Report provided a high-level summary of some of the mitigation measures being implemented through Breakwater:

- *Continued operationalization of the use of a leading cybersecurity industry endpoint security, monitoring and remediation tool and services.*
- *Continued scanning of external access points.*

[98] See Cyberattack on the Newfoundland and Labrador Health Care System Overview (March 2023) prepared by the Department of Health and Community Services and Department of Justice and Public Safety.

- *Continued steps toward the implementation of a centralized gateway and firewall to further enhance cybersecurity detection and control capabilities.*
- *Continued steps toward the implementation of a Provincial Security Information and Event Management (SIEM) system Roll out of a new mandatory cybersecurity training program to NLCHI and RHA staff.*
- *Ongoing Active Directory review and further enhancement.*
- *Continued work to enhance IT asset management.*
- *Implementation of centralized email/URL filtering technology to enhance centralized event protection, detection, and investigation capabilities.*
- *Data quality and safety through continued review of backfilling of patient data into systems affected by the disruption caused by the attack.*
- *Enhancement and maintenance of awareness and understanding of cyber-risk across the entire health workforce.*
- *Enhancement of a culture that enables and encourages vigilance to protect patients and employees from future cyber-attacks.*

[223] On March 3, 2023, the Vice President of Solutions and Infrastructure with the Centre met with our investigation team to provide an overview of the Breakwater projects, their status, and future plans. The overview also demonstrated how the projects aligned with the recommendations provided in the Gartner Assessment. Subsequent to this meeting, the Centre provided us with the slide deck that included the Gartner recommendations.

[224] On January 9, 2023, prior to meeting with the Centre's Vice President, we requested a copy of the Gartner Assessment. That request was eventually refused in the Centre's response to our Office received on April 11, 2023. The Centre's position outlined that the "*Gartner assessment, which has been completed, is privileged and confidential. The engagement and assessment was performed by Gartner for the purpose of assisting [the Centre's] legal counsel to provide legal advice to [the Centre]*". With respect, we disagree. As a reminder, the funding approval letter states that such funds were provided to allow the Centre "to enter into a contract with Gartner to conduct a security assessment and develop a security strategy." It is clear from the wording of the funding approval letter that the Assessment's *primary purpose* was to protect the security of our province's health care information systems, not protect the Centre from civil liability associated with the cyber attack privacy breach. It is unfortunate and concerning that the Centre would take this position in refusing to disclose the contents of the Gartner Assessment to this Office. In light of the broader circumstances, including the time

that has elapsed since the cyber attack and the other information available to us through this investigation, we have decided not to challenge this claim of privilege in court. Having received a presentation on key elements of the Gartner Assessment, pursuing a copy of the assessment report through litigation, while within our ability, would not justify the excessive delay in providing our findings to the public that would result.

[225] We were not able to review the specific vulnerabilities that would have been identified in the Gartner Assessment. However, as stated above, we did review the recommendations meant to address those vulnerabilities. While we cannot comment upon any additional vulnerabilities that may have been uncovered through that assessment, we can confirm that reasonable steps are being taken to address the specific vulnerabilities that contributed to the cyber attack. The security projects roadmap presented by the Centre looks balanced, aims to reduce cyber risk, and will increase the maturity of our province's cyber security posture. We do have a few points regarding priority of certain projects and resourcing that, as we do not wish to highlight these matters to malicious actors, we have outlined to the Provincial Health Authority in the **confidential annex** referenced earlier.

[226] Commissioner's Delegate Finding: I find that reasonable cyber security steps have been and are being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack.

ii. Patient SIN Information

[227] It was identified at the December 14, 2021 Public Advisory Briefing that a number of patients had had their SIN information collected at patient registration.

[228] During our investigation, the Regional Health Authorities confirmed that the collection of patient SIN information at registration was unnecessary. It was determined that the collection of patient SIN information at registration had occurred for no other reason than there was a place for it to be entered on the screen in the Meditech Admissions Module.

[229] Pursuant to section 5(1)(d) of *PHIA*, the definition of "personal health information" includes "registration information", which therefore includes SIN information taken at the time of patient registration. *PHIA* includes provisions requiring that custodians only collect what is

necessary, and it has been determined, subsequent to the cyber attack, that the routine collection of SIN numbers by the Regional Health Authorities at registration was an unnecessary collection. The sections that are particularly relevant to the issue of SIN collection state that a custodian "*shall not collect personal health information if other information will serve the purpose of the collection*" (section 29(3)) and a custodian "*shall not collect more personal health information than is reasonably necessary to meet the purpose of the collection*" (section 32(1)).

[230] Commissioner's Delegate Finding: I find that the collection of SIN information at patient registration was in contravention of section 29(3) and section 32(1) of *PHIA*.

[231] The Regional Health Authorities and the Centre have since taken the necessary steps to delete the previously collected SIN information. Further investigation efforts into this matter confirmed that the SIN field in the Meditech Admissions Module could not be "removed" from the Admissions Module but the SIN field could be suppressed. At the Regional Health Authorities' request, the Centre engaged with the company Meditech to suppress the SIN field within the Meditech Admissions Module[99]. Meditech (the company) subsequently activated a software solution to prevent the collection of SIN, by making the field unavailable for collection of SIN numbers. Although the SIN field (the box to enter this information) is still present, nothing can be entered into it.

[232] Commissioner's Delegate Finding: I find that reasonable steps have now been taken to delete and prevent the unnecessary collection of patient SIN at registration.

iii. Records Management

[233] It was identified at the December 14, 2021 Public Advisory Briefing that the "past employee" portion of the Meditech Data Repository breach was larger in magnitude than originally thought, with officials revealing that past employee information extended 28 years

[99] Central Health explained that the Centre was required to engage with Meditech (the company) to address this issue stating that "*[the Centre] holds responsibility for the Meditech and Meditech Data Repository environment since the implementation of IT Shared Services. Meditech (the company) must implement restrictions or changes to the fields within the Meditech software. If restrictions or changes to Meditech's input fields are needed, this constitutes an enhancement or customization, both of which must be carried out by Meditech itself (because Meditech is a proprietary piece of software)*".

into the past for both Eastern Health and Central Health. It was also apparent that deceased patient information was also being maintained for longer than necessary.

[234] Nothing in *ATIPPA, 2015* or *PHIA* sets out how long records are to be retained. However, part of protecting personal information and personal health information is ensuring that there are policies and procedures in place that minimize the risks associated with a privacy breach[100]. This includes implementing and maintaining policies and procedures that manage the information through its lifecycle, including ensuring that there is a retention and destruction schedule for all holdings of personal information and personal health information.

[235] During our investigation, inquiries were made to the Regional Health Authorities about records retention and destruction policies and/or plans. The Regional Health Authorities provided submissions confirming that these are at various stages of development and implementation. Central Health developed a Records Retention Schedule which was approved on May 31, 2022 and outlined a series of steps it is taking in pursuit of implementation. Labrador-Grenfell Health has identified that it was awaiting approval from the Government Records Committee for its records retention and disposal schedules, noting that these plans may change with the transition to the Provincial Health Authority. Eastern Health confirms that a standardized provincial retention schedule for health records has been submitted through the Centre to Government for approval, noting as well that plans may change with transition to the Provincial Health Authority.

[236] Commissioner's Delegate Finding: I find that the Regional Health Authorities failed to implement appropriate records management policies and procedures relating to retention and destruction of personal information and personal health information prior to the cyber attack, which unnecessarily left this information vulnerable to a breach of privacy.

[100] Pursuant to section 13 of *PHIA,* custodians are required to have in place policies and procedures that address records retention and disposal. The stated purpose for this is "to minimize the risk of unauthorized access to or disclosure of personal health information." Under the *Management of Information Act*, ("MOIA") public bodies are required to develop and maintain a records management system that addresses records retention and disposal. Sections 63 and 64 of *ATIPPA, 2015* require that public bodies take reasonable steps to ensure that information is accurate and complete, and that it is secure against theft, loss and unauthorized collection, use or disclosure. These provisions, among many others in *ATIPPA*, imply a suitable records management system, and retention and destruction/disposal are necessary parts of any such system.

[237] Commissioner's Delegate Finding: I find that reasonable steps are being taken towards the development and implementation of a records retention and destruction schedule.

iv. Summary of Commissioner's Delegate Findings

[238] The following findings are made regarding prevention of future breaches:

- I find that the necessary investigations were conducted to determine, to the extent possible, the root causes of the privacy breach and the cyber attack as a whole.
- I find that reasonable cyber security steps have been and are being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack.
- I find that the collection of SIN information at patient registration was in contravention of section 29(3) and section 32(1) of *PHIA*.
- I find that reasonable steps have now been taken to delete and prevent the unnecessary collection of patient SIN at registration.
- I find that the Regional Health Authorities failed to implement appropriate records management policies and procedures relating to retention and destruction of personal information and personal health information prior to the cyber attack, which unnecessarily left this information vulnerable to a breach of privacy.
- I find that reasonable steps are being taken towards the development and implementation of a records retention and destruction schedule.

v. Commissioner's Delegate Recommendations on Prevention

[239] The following recommendation is made regarding prevention of future breaches:

> I recommend that the Provincial Health Authority continue to take diligent steps to ensure that information management policies and procedures addressing retention and destruction of personal information and personal health information are developed and implemented to minimize the breadth and impact of any future privacy breach.

IX. SECURITY AND INFORMATION PRACTICES

Issue #2: Did the Centre and Regional Health Authorities have reasonable security and information practices in place at the time of the cyber attack for its electronic information systems as required by PHIA?

[240] While *ATIPPA, 2015* requires public bodies to protect personal information, and *PHIA* requires custodians to protect personal health information, the statutory requirement for protection of this information is the same. A public body/custodian is required to take steps that are reasonable in the circumstances to ensure that the personal information/personal health information in its custody or control is protected against "theft, loss and unauthorized collection, access, use or disclosure."

[241] An assessment of whether a public body or custodian has "taken steps that are reasonable in the circumstances" involves looking at whether a public body or custodian has "reasonable security arrangements" in place. Our counterpart, the Nova Scotia Information and Privacy Commissioner, has outlined a list of factors commonly considered when evaluating the reasonableness of an entity's security. While the following factors[101] are discussed within the context of custodians, in general, these factors are applicable to both custodians and public bodies when assessing if there are reasonable security arrangements in place:

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.*
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*

[101] Please note the footnote links cited within this section were removed for simplicity of our Report; for full NS OIPC decision with links, please see para. 158 in 2023 NSOIPC 2 (CanLII) | Health (Nova Scotia) (Re) | CanLII; Also see 2019 NSOIPC 2 (CanLII) | Department of Internal Services (Re) | CanLII.

technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

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.*
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.*
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.*
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.*

a. Sensitivity of Information and Trust Consideration

[242] It is important to note the special place personal health information has within our society and how important it is for this information to be protected. As stated in *Investigation Report F10-02*[102]:

> *[1] Personal health information has a special status in that it is the most sensitive type of personal information and is collected as part of a unique relationship between health care providers and individuals. In general, personal health information is only disclosed by a patient to a health care provider because the patient requires health care that the patient believes the provider is qualified to deliver. Were it not for this need and the*

[102] 2010 BCIPC 13 (CanLII) | Electronic Health Information System (Re) | CanLII.

> *expectation that the provider can assist, the sensitive personal health information would never be disclosed. The only purpose for the disclosure of personal health information by a patient is to seek and obtain health care.*
>
> *[2] One of the ethical obligations of every health professional is to protect the confidentiality of patient information. The assurance of privacy is essential for patients to be willing to engage in the frank communication with their health care providers that providers rely on to deliver quality care. Patients assume that their personal health information is kept confidential because it is such a well understood hallmark of the provider/patient relationship.*
>
> *[3] In an era where technology permits health care providers to utilize a common electronic health record, rather than their own separate paper files, it becomes more difficult to assure privacy protection. An electronic health record system is large and complex, more providers and administrative support staff access the system, and more information about more patients is available faster and easier.*
>
> *[4] We are well aware of the value of electronic health record systems in facilitating the delivery of efficient, timely, and cost-effective health care services. At the same time, however, privacy is a system design imperative––not only to carry forward the ethical obligations of providers but also to comply with legal obligations with constitutional dimensions. The protection of privacy is a fundamental value in modern democracies and is enshrined in ss. 7 and 8 of the Canadian Charter of Rights and Freedoms.*

[243] There is a clear expectation that personal health information will be protected to the highest degree of privacy and security against the risk of a privacy breach[103]. As British Columbia's Information and Privacy Commissioner Michael McEvoy stated in a recent report about British Columbia's public health database:

> *The System is indispensable when it is used for its intended purposes, which are the delivery of healthcare and managing threats like communicable disease outbreaks. However, the System is subject to abuse if wrongly accessed by any bad actor, ranging from cyber criminals to a jilted lover looking for information about an ex to someone simply curious about their neighbour.* ***Given its high level of sensitivity and the risk of its unauthorized access, one would expect the highest degree of privacy and security would be in place to protect our personal information from such intrusions.***

[244] As Canadians, the same expectations for privacy and security of personal health information apply in British Columbia as they do in Newfoundland and Labrador. Our residents need to trust that their most sensitive information will be given the highest degree of privacy

[103] See Investigation Report 22-02 titled "*Left untreated: Security gaps in BC's public health database.*"

and security that can reasonably be implemented to protect their personal health information from being taken.

[245] Commissioner's Delegate Finding: I find that the personal health information and personal information taken in the cyber attack was highly sensitive information that deserved the highest degree of protection.

b. What Security Measures were Required to Defend against this Cyber Attack?

[246] The HIVE ransomware group and the tactics and tools that they used in this cyber attack were not "unstoppable". In fact, many of the techniques used in this cyber attack were basic techniques commonly used in cyber attacks and were well known within the cyber security community. An adequate cyber security defense system can identify such techniques in its system and provide incident response measures to prevent further movement within a system and/or prevent or reduce the removal of data.

[247] The mitigation measures recommended in the FBI's *Flash Alert*[104] from August 25, 2021 listed to assist organizations in defending against HIVE:

- *Back-up critical data offline.*
- *Ensure copies of critical data are in the cloud or on an external hard drive or storage device.*
- *Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.*
- *Use two-factor authentication with strong passwords, including for remote access services.*
- *Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable.*
- *Keep computers, devices, and applications patched and up-to-date.*
- *Install and regularly update anti-virus or anti-malware software on all hosts.*

[248] While this Flash Alert was issued mere months before the cyber attack took place, the mitigation measures being recommended were not 'new' and were standard within the cyber security industry.

[104] See Federal Bureau of Investigation (FBI) *Flash Alert* dated August 25, 2021.

[249] The *Analyst Note* from the Department of Health and Human Services (USA)[105] also listed standard practices that should be followed in defending against HIVE:

> - *Use two-factor authentication with strong passwords – this is especially applicable for remote access services such as RDP and VPNs.*
> - *Sufficiently backing up data, especially the most critical, sensitive and operationally necessary data is very important. We recommend the 3-2-1 Rule for the most important data: Back this data up in three different locations, on at least two different forms of media, with one of them stored offline.*
> - *Continuous monitoring is critical, and should be supported by a constant input of threat data (open source and possibly proprietary as well)*
> - *An active vulnerability management program must be comprehensive in scope and timely in implementation of the latest software updates. It should apply to traditional information technology infrastructure as well as any medical devices or equipment that is network-connected.*
> - *Endpoint security should be comprehensive in scope and updated with the latest signatures/updates aggressively.*

[250] Although this Analyst Note is dated April 18, 2022, after the cyber attack, the above list of mitigation measures were hardly new or unheard of. During the time period leading up to the cyber attack these were standard practices. The Flash Alert and Analyst Note highlighted a new ransomware group that was taking advantage of those organizations which did not have such standard practices in place throughout their information systems.

c. What Security Measures were in Place at the Time of the Cyber Attack?

[251] The Department filed our list of questions with its court application, thereby making our questions a public document. While this Report will not name the specific vulnerabilities taken advantage of by the Threat Actor, we will highlight the cyber security concerns raised in our questions, as the Department, in choosing to file it in a public court document, made a determination that it was suitable to release to the public.

[252] Our questions to the Department noted that there was a privacy and security posture assessment obtained by the Centre prior to the move to Shared Services, wherein the Centre

[105] Analyst Note dated April 18, 2022.

became responsible for the Regional Health Authorities' information technology and information security. In providing some context for our questions we stated:

> *Approximately three (3) months prior to the implementation of shared services, [the Centre] received a privacy and security posture assessment (the "**Deloitte Assessment**") that identified a number of cyber security weakness and gaps, and which also confirmed that neither [the Centre] nor the regional health authorities were fully compliant against the international cyber security standards they were measured against[106]. The shared services model became effective on October 2, 2019, with the Centre becoming solely responsible for the information technology ("**IT**"), which includes cyber security, of our province's four regional health authorities.*

[253] Our questions thereafter noted that during the pandemic (~11 months after the Centre took over responsibility for the Regional Health Authorities' cyber security, and ~14 months after the Deloitte Assessment) the Centre's Information Note[107] titled *Ransomware: Threat and Mitigation Plans* from September 2020 (~one year before the cyber attack took place) stated as follows:

> *…[the Centre's] Information Note[108]…rated the likelihood of a ransomware attack as being high, [and in it the Centre] references continuing cyber security weaknesses requiring priority stating in part:*
>
> > *Significant IT vulnerabilities exist, with new vulnerabilities identified daily such as outdated OS, unpatched systems, software flaws.*
> >
> > *…*
> >
> > *Critical ransomware mitigations require additional focus during times of elevated risk, such as the current health emergency. **[the Centre], under the existing mandate, will require significant effort to elevate all eHealth IT environments to an acceptable level of security.** This will include consolidating and, in some cases, upgrading legacy applications and infrastructure to*

[106] *Deloitte Privacy & Security Posture Assessment dated 02 July 2019 provides a high-level assessment of the security practices of NLCHI and the RHAs against certain ISO27001[106] security controls and Deloitte's Cyber Security Framework. ISO/IEC 27001 is an international standard to manage information security. The standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005, revised in 2013, and again most recently in 2022. It outlines a set of technical, operational and governance controls. The report highlighted a number of gaps from a technical and operational point of view*.

[107] The Department's Submissions explain that "*information notes are intended to brief a Minister on particular issues, not to seek or approve direction. In this case, [the Centre] provided its mitigation strategy to these threats to fulfil their statutory obligations.*"

[108] NLCHI Information Note titled *Ransomware: Threat and Mitigation Plans* from September 2020.

> *reduce overall vulnerability. The controls required to prevent ransomware attacks, and prepare the organizations to recover and respond, warrant additional priority, and include:*
>
> *Prevention Priorities:*
>
> 1. ***Security training and awareness*** *for all health related staff;*
> 2. ***Patch and vulnerability Management*** *for all eHealth IT equipment: Attackers concentrate on the easiest way to break in, meaning all systems and solutions need to be at an acceptable security level;*
> 3. ***Backup and Restore*** *of vital and critical systems and data: Backups have to be enabled with appropriate access controls, so they do not fall victim to encryption or destruction by an attacker;*
> 4. ***Enhanced monitoring and alerting***:
>   i. *Internet gateway controls (Email filtering, Web filtering, host based security controls, application whitelisting);*
>   ii. *Security Information and Event Management operations;*
>   iii. *Enhanced threat intelligence gathering to remain current with attack methods, campaigns and defence techniques; and*
> 5. ***Credential Hygiene:*** *users must be limited to privileges they need for their role, and restrict using privileged accounts for routine activities.*

[254] Our questions also reference the Canadian Centre for Cyber Security Report, obtained by the Centre after the cyber attack took place, stated:

> *The recommendation from the team on the ground was to implement a syslog-NG type centralized logging service to begin collecting all logs in a single repository. In parallel with this the procurement of a SIEM tool would be required to process all the events being collected. Alternatively, the [Centre] have been discussing contracting out MSP functionality. MSP functionality has not been fully explored so what's going to be included is still up in the air however one thing for consideration is that the internal staff is not in a position to keep up with what needs to be done and expertise across the board is limited as well.*
>
> ...
>
> *They are considering a hand-over of monitoring capabilities to a 3rd party (MSP) since they recognize that they do not possess the expertise or the staff to maintain these solutions.*
>
> ...

> *RHA's and NLCHI are severely understaffed from a technical resource perspective. There are currently **three IT security staff** for the province as a whole.*
>
> [Emphasis Added]

[255] Our questions also reference a funding request note the Centre sent to the Department in January 2022 after the cyber attack which stated:

> *In October 2019, [the Centre] assumed the mandate to provide IT services, including security, from the [Regional Health Authorities] under an eHealth shared service model. Among the objectives of implementing this model were merging and standardizing networks and infrastructure, finding efficiencies through economies of scale and eliminating duplication, and simplifying the overall environment to improve manageability and reduce risk. Early plans identified multiple opportunities to strengthen IT security across the [Regional Health Authorities] through consistent adoption of security best practices and through leveraging new and existing tools for threat defense and IT operations management. Due to demands stemming from the pandemic response and other competing priorities, as well as financial constraints, progress toward meeting these objectives has been limited.*

d. The Pandemic, Competing Priorities and Costs

[256] The pandemic resulted in a shift to more remote work and an increased reliance on having virtual access to health care services. The Centre stated in its submissions:

> *In terms of how ongoing cybersecurity work was impacted by the pandemic response, this naturally became the top priority of all workstreams at [the Centre] as of March 2020. Due to the urgent demands of the pandemic situation, resources were reallocated to complete work required for pandemic management to ensure the effective ongoing delivery of healthcare services.*
>
> *Although this naturally limited [the Centre's] ability to focus on other workstreams such as with respect to cybersecurity, [the Centre] remained committed at all times to maintaining the security of the information and systems in the [Centre]-managed environment, and no cybersecurity work was formally paused or stopped. [The Centre's] existing cybersecurity measures continued to be used during the pandemic, and departmental and individual accountabilities for cybersecurity … generally did not change during this time.*

[257] The Centre identified many competing priorities during this time period noting that it reallocated its resources to:

1. *Clinic Support:*
    a. *Setting up COVID testing and vaccination sites for each RHA, including logistics related to devices, networking, and project management/ coordination.*
2. *Work-From-Home (WFH) Support:*
    a. *Deploying a solution to support the volume of WHF needs for RHA and NLCHI personnel.*
    b. *Configuring devices (e.g., laptops, phones, etc.) to support WFH arrangements.*
    c. *Developing return-to-work processes and supports.*
3. *Reporting and Decision Support:*
    a. Various COVID-19-related reporting to the RHAs and DHCS.
4. *Application Development:*
    a. *Development of various COVID-19-related applications and websites to support the various pandemic needs of the RHAs and DHCS.*
5. *Virtual Care & Virtual Care Clinics:*
    a. *Support for the RHAs to develop their delivery of virtual care services.*
    b. *Support for certain physicians to develop their delivery of virtual care services.*
    c. *General expansion of telehealth services .*
    d. *ER virtual clinic support for each RHA.*
6. *IT Inventory Logistics:*
    a. *Procurement, inventory, and delivery, etc.*
    b. *Providing online self-scheduling support for vaccination clinics.*
    c. *Establishing and managing a third party call centre to provide communications support for various new online tools.*
    d. *Development and support of a contact tracing system ("COVID Tracker").*
    e. *Partial development of a provincial COVID-19 exposure notification app (ultimately superseded by the COVID Alert app).*
    f. *Procurement, launch, and support of the NLVaxPass COVID-19 vaccination record storage app.*

Additional competing priorities can be found in the eHealth Projects Update…

[258] We asked the Centre about whether it had asked for funds to address the cyber security weaknesses and gaps previously identified in the Deloitte Assessment, and also raised in the Information Note. The Centre explained:

> *Following the formal transition to Shared Services in October 2019, the consolidated information technology budget relating to the [Regional Health Authorities] had an annual deficit of $3-million, which financially limited [the Centre's] ability to comprehensively address cybersecurity. [The Centre] made reductions in this deficit by achieving efficiencies in certain areas, but these efforts were also affected by the need to prioritize the pandemic response. Further, [the Centre] was subject to government direction to make no new operational budget requests for fiscal years 2020-22….*
>
> *Between the date of the Deloitte Assessment and the cyber attack, there were no specific operational funding requests to the [Department] related to [the Regional Health Authority] cyber security weakness for fiscal years 2020-22 given government direction in those years to make no new operational budget requests.*

[259] The Department received the Centre's Information Note on September 22, 2020[109] which not only rated the threat of a ransomware cyber attack as being high, but also specifically listed a variety of concerns and vulnerabilities directly related to ransomware, as well as proposed mitigations. The Information Note made it clear that the health care information systems were not at an acceptable level of security. It is concerning that there would be a Government direction to the Centre, tasked with the protection of the health care information systems, not to make any new operational budget requests for the 2020-22 fiscal years, particularly in light of the known high risk of a ransom attack.

[109] In a recent news interview the Minister stated that he did not read the five page information note and was instead provided with a summary by the Centre. We received submissions from the Department stating the history of the information note as follows: "The Executive of the [the Department] received the note on September 22, 2020. Shortly thereafter, it was shared with the Chief Executive Officers of the Regional Health Authorities. The note highlighted risks and mitigation actions to be taken. As this was about mitigation measures, this matter was added to the agenda for Deputy Minister/CEO monthly meeting in October [2020]. The minutes from the October meeting reflect that the draft briefing note was presented and that the CEO of the [Centre] would work with the Office of the Chief Information Officer and the Regional Health Authorities to develop a policy and return to committee for review. There is no written summary document. The Executive of the [Department] provided a verbal briefing to the Minister in May 2022." Additional context was added later on stating, "the information note was not in final form, and was meant for Executive discussion at the time. The briefing for the Minister in 2022 was part of a larger briefing related to an ATIPP request."

e. WAS THE CYBER ATTACK FORESEEABLE?

[260] On June 19, 2019, Eastern Health CEO sent an email to other Regional Health Authorities, the Centre's CEO and a senior executive of the Department containing two articles about the City of Baltimore, Maryland where all City systems were held for ransom. The CEO specifically stated in the email "*The various stories mention vulnerability of hospital with respect to lack of investment in Cyber.*"

[261] In a Strategic Proposal[110] prepared for Eastern Health with input from the Centre, it proposed the development of a centre of excellence in health care cyber security, and a core component of this would be development of a Security Operation Center[111] that would be responsible for network monitoring. Not only did this proposal identify a number of existing vulnerabilities and security concerns within part of the health care Information system[112], this document **dated September 2020** highlighted the need to address the cyber security of our health care information systems, stating:

> *In Canada and globally, there is growing realization that cybersecurity in healthcare is a serious and growing concern. There is an urgent need to address these threats in a manner commensurate with the significance of the consequences. Evidence mounts, almost daily, of attacks in healthcare facilities around the world and, almost certainly, this evidence understates the true size and severity of the problem as many attacks remain either undetected or unreported. The COVID-19 pandemic has only made matters worse as it makes society more reliant on digital connectedness thus exposing all sectors even more than before. It has also made Canadians realize that having a safe, resilient and innovative healthcare sector is critical to both managing pandemic response as well as preparing for post pandemic economic recovery. In the future, the current and growing state of vulnerability will no longer be acceptable.*

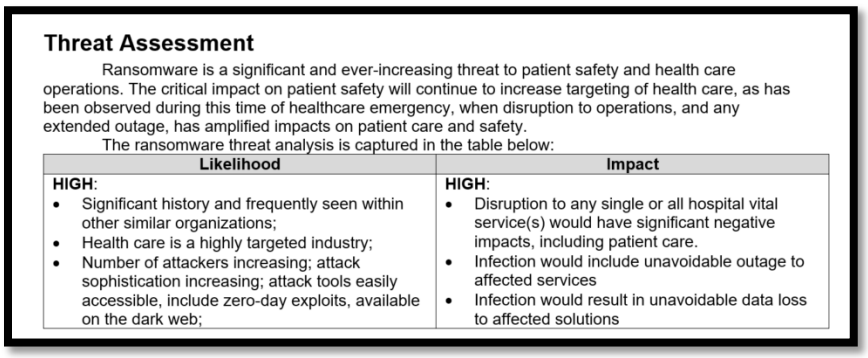
---

[110] Eastern Health Centre of Excellence in Healthcare Cybersecurity Business Plan Strategic Proposal" prepared by Canada Israel Technology Solutions Inc. dated in September 2020.

[111] A Security Operation Center (SOC) is a physical or virtual facility that centralizes an organization's security operations, including security monitoring, incident response, and threat intelligence. It is responsible for identifying, assessing, and responding to cybersecurity threats in a timely manner to protect the organization's assets and maintain business continuity.

[112] Long before N.L. cyberattack, report flagged flaws in system | CBC News.

[262] As stated above, on September 22, 2020, the Centre provided a five page Information Note[113] to the Department which rated the likelihood of a ransomware attack against health care organizations as being high and also confirmed that its impact would be high:



Threat Assessment

Ransomware is a significant and ever-increasing threat to patient safety and health care operations. The critical impact on patient safety will continue to increase targeting of health care, as has been observed during this time of healthcare emergency, when disruption to operations, and any extended outage, has amplified impacts on patient care and safety.

The ransomware threat analysis is captured in the table below:

Likelihood	Impact
HIGH: • Significant history and frequently seen within other similar organizations; • Health care is a highly targeted industry; • Number of attackers increasing; attack sophistication increasing; attack tools easily accessible, include zero-day exploits, available on the dark web;	**HIGH**: • Disruption to any single or all hospital vital service(s) would have significant negative impacts, including patient care. • Infection would include unavoidable outage to affected services • Infection would result in unavoidable data loss to affected solutions

[263] On October 30, 2020, one year prior to the cyber attack, the Canadian Centre for Cyber Security issued an alert called "*Renewed Cyber Threats to Canadian Health Organizations*[114]" which highlighted the "imminent and increased threat" to Canadian health care providers, confirming that the COVID-19 pandemic presented an "elevated level of risk to the cyber security of Canadian health organizations", and recommended that "*organizations take extra precautions in identifying, as early as possible, potential vulnerabilities and inadequate security controls that may lead to an infection resulting in ransomware being deployed.*"

[264] On November 2, 2020 the insurance provider HIROC[115] circulated a "*Subscriber Alert: Ransomware incidents in Healthcare on the rise*" to its subscribers, highlighting in this email "HIROC has learned that a new wave of ransomware attacks have been compromising health care organizations across Canada and US" and highlighting/linking to the Canadian Centre for Cyber Security's Alert noted above. Eastern Health's CEO forwarded this Alert to the Centre's CEO. The Centre's CEO replied, indicating he had already received it.

[265] January 8, 2021, email was sent by Eastern Health's CEO to the Department (Deputy Minister) sharing an article on the ransomware cyber attack on eHealth in Saskatchewan, in which the article states "*Saskatchewan's information and privacy commissioner is calling last*

[113] NLCHI Information Note titled *Ransomware: Threat and Mitigation Plans* from September 2020.
[114] Renewed Cyber Threats to Canadian Health Organizations - Canadian Centre for Cyber Security.
[115] Healthcare Insurance Reciprocal of Canada.

year's ransomware cyberattack on eHealth one of the province's largest privacy breaches ever…In total about 40 gigabytes of encrypted data was extracted. On Jan 21, 2020, eHealth discovered the files were sent to IP addresses in Germany and the Netherlands…"New and better and bigger cyberattacks continue to occur*," he said, adding training in cybersecurity is a constant and ongoing process.* "I think it's fair for us to accept that we should insist upon the highest standard of security when it comes to protecting the most sensitive information we have*."*

[266] On May 17, 2021 Eastern Health's CEO sent an email to the Deputy Minister of the Department providing updates since the cyber security project presentation which Eastern Health had given to the Department the week prior, confirming that Eastern Health's VP "*has met again with [the Information and Privacy Commissioner] to ensure he is still supportive and has no concerns [with the project]. He has been engaged previously and is indicating he is very supportive of the need to develop this capability, given that it is only a matter of time before an attack is successful here*." Eastern Health provided additional emails showing it was continuing to pursue a Centre of Excellence in Cyber Security project thereafter, including a letter dated October 15, 2021 sent to the Premier on October 18, 2021, shortly after the Threat Actor entered the health care information system.

[267] Commissioner's Delegate Finding: I find that a high impact ransomware attack against our province's health care information systems was foreseeable.

f. WHAT STEPS WERE BEING TAKEN?

[268] In an effort to understand what, if any, steps the Centre had taken in addressing the identified weaknesses and gaps within the Deloitte Assessment and the Information Note, we asked the Centre what it had done to address these vulnerabilities. The Centre provided the following response:

> *As a preliminary point, it is important to note that the Deloitte Assessment was commissioned prior to [the Centre] assuming the Shared Services mandate in October 2019, when [the Centre] and the [Regional Health Authorities] operated as separate entities. Deloitte began its work in 2018 and finalized the assessment prior to October 2019, which reflects circumstances at the point in time that Deloitte undertook its work. While [the Centre] took a number of steps to address key items flagged by the Deloitte Assessment (as described*

> *below), the Deloitte Assessment has been superseded by subsequent changes and by current analysis and recommendations regarding [the Centre's] current-state security. In particular, Gartner reviewed [the Centre's] current-state security, taking into account changes made by [the Centre] since the Deloitte Assessment, and made a set of recommendations which have been incorporated into Project Breakwater (along with input from [the Canadian Centre for Cyber Security], Public Safety and CrowdStrike). Accordingly, under Breakwater, [the Centre] is addressing the most current and relevant set of recommendations it has received.*
> *…*
> *Deloitte's work was undertaken in 2018 and the assessment finalized in 2019 prior to Shared Services based on the then-current circumstances. Under Project Breakwater, [the Centre] is addressing the most current and relevant set of recommendations it has received. Nonetheless, with respect to the Deloitte Assessment, [the Centre] had implemented the a [sic] number of enhancements up to the point of the cyber attack…*

[269] The Deloitte Assessment provided a high-level assessment of the security practices of [the Centre] and the [Regional Health Authorities] against certain ISO27001[116] security controls. While this Assessment was conducted prior to the Centre becoming responsible for the health care information systems, it is important to note that this Assessment was conducted for the very purpose of moving to Shared Services. As stated therein:

> *The Privacy & Security Posture Assessment measured process and policy alignment with industry standards across the provincial eHealth landscape. The objective of the Privacy & Security Posture Assessment included:*
>
> - *Establishing an understanding of the established privacy and security practices within the Newfoundland and Labrador Centre for Health Information (NLCHI) and the four regional health authorities (Central Health, Eastern Health, Labrador-Grenfell Health and Western Health); and*
> - *Leveraging the combined experiences of NLCHI and the regional health authorities (RHAs) to reach a standardized level of compliance with privacy and security best practices.*

[270] The Deloitte Assessment provided recommendations in a roadmap to assist with the Centre's attempts to reach a standardized level of compliance with privacy and security best practices. We agree with the Centre that the Deloitte Assessment represents a "point in time"

[116] ISO/IEC 27001 is an international standard to manage information security. The standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005, revised in 2013, and again most recently in 2022. It outlines a set of technical, operational and governance controls.

assessment and we acknowledge that this assessment has subsequently been replaced by a more recent analysis and assessment done in response to the cyber attack. However, the "point in time" Deloitte Assessment is still relevant to our consideration of what, if any, steps were taken by the Centre in addressing the known weaknesses and gaps identified therein during the time leading up to the cyber attack. The Deloitte Assessment was intended to assist the Centre in its task of taking over responsibility for the health care information systems in moving to Shared Services and as the only comprehensive assessment of its kind at that time, it remained relevant after it took over this role.

[271] In its submission, the Centre listed a number of projects that were intended to address gaps and vulnerabilities identified in the Deloitte Assessment. In our review of the security projects listed, we can confirm that these were important security projects that would have addressed some of the weaknesses that the Threat Actor was able to take advantage of. However, these projects had a low completion rate or were otherwise too limited in scope to be effective. It was also not clear how the list of projects was specifically tied back to the Deloitte Assessment roadmap, why the existing cyber security framework provided by Deloitte was not followed, nor was there an explanation as to how these projects were prioritized, or worked together to minimize risk.

[272] Implementation of security measures for larger organizations require more than a list of cyber security projects. As stated within Report F06-01[117]:

> *Information security measures are properly established through a methodical assessment of risk that assesses both the foreseeability of a privacy breach (intentional or accidental) occurring in the context of current threats to or weaknesses in existing information-security measures and the severity and extent of the foreseeable harm that could result from a privacy breach. This assessment is then used to identify and implement a hierarchy of security measures according to the degree of risk involved.*

[273] As stated elsewhere in this Report, we have reviewed the Breakwater security projects roadmap presented by the Centre that was developed in response to and as a result of the

[117] See para. 54 2006 CanLII 13536 (BC IPC) | Sale of Provincial Government Computer Tapes Containing Personal Information, Re | CanLII; While this is not a decision on cyber security, this statement is nevertheless still accurate in describing the need for careful implementation of mitigation measures.

cyber attack. The Breakwater security projects were developed within a framework that was recommended to the Centre by a Gartner Assessment. These security projects are balanced, aim to reduce cyber risk, and will increase cyber maturity as they progress. While it is true that the Gartner Assessment supersedes its Deloitte predecessor, many of these new projects address the same control gaps previously identified in the Deloitte Assessment, including the control gaps the Threat Actor was able to use in the cyber attack. While we are pleased that these efforts are being put forth now, it is clear that these measures should have been taken at an earlier point in time, certainly before the cyber attack and arguably much earlier.

[274] Commissioner's Delegate Finding: I find that, in the circumstances, in light of the sensitivity of the information and the foreseeability and likelihood of significant harm to privacy that could result from a cyber attack, the Centre, Eastern Health, Central Health, and Labrador-Grenfell Health did not have reasonable security arrangements in place to protect personal health information and personal information at the time of the cyber attack, contrary to section 15(1)(a) of *PHIA* and 64(1)(a) of *ATIPPA, 2015*.

g. Shared Services Impact on Mitigation Measures

[275] Shared Services came into effect on October 2, 2019, when the Regional Health Authorities and the Centre were all considered to be individual and separate legal entities. On April 1, 2023, the Centre and Regional Health Authorities were integrated into the Provincial Health Authority. The below section discusses issues that arose due to the nature of Shared Services, where separate entities try to work together with different roles and responsibilities and in the within matter, it was the Centre which was tasked with responsibility for managing and securing the Regional Health Authorities' information systems. We acknowledge that with all of these entities becoming one, the following issues have been resolved. However, it is important to reflect on the arrangement that existed prior to the cyber attack, to understand, for the sake of transparency and accountability, how the relationship among the different entities and their respective roles helps us to assess the reasonableness of the security arrangements that were in place at the time.

[276] After announcing intentions to proceed with Shared Services, the Minister provided written directives with his letter sent on October 5, 2017, wherein the Centre was assigned

responsibility for leading and managing a province-wide service for information technology and telecommunications, also referred to as eHealth services. This letter confirmed that agreements would need to be in place ***prior to*** the full implementation of Shared Services, stating:

> *It is acknowledged that there are a number of issues to be addressed prior to full implementation of the new models, including but not limited to governance, roles and responsibilities, scope of service, performance expectations, financial terms, privacy considerations, liability and indemnity and dispute resolution. These issues will be addressed by way of agreement(s) that will be put in place to support these province wide services.*

[277] In 2018, the Centre's legislation was amended to expand its mandate to include it having responsibility for the health care information systems[118].

[278] While the Minister's directive letter states that agreements would be put in place prior to the full implementation of Shared Services, that is not what transpired between the entities. The Centre explained:

> *The integration of eHealth services was organized into four phases, with phases one and two focusing on the recruitment, hire, and transition of the executive team and the management team respectively. These two phases were complete by January 2020.*
>
> *Phase 3 formally began in January 2020 with a focus on the integration and transition of targeted staff for NLCHI and the RHAs, with an eHealth Memorandum of Understanding ("MOU") as a target deliverable. The first part of this deliverable, an MOU focused on "Finance and Assets", was completed as of June 4, 2020 (the "Finance MOU"). The Finance MOU was approved by NLCHI for signature and was signed by the RHAs by July 8, 2020. As described in the Finance MOU:*
>
> > *In January 2020, a working group started developing an eHealth MOU [work on individual sections of the MOU had begun prior to October 2019, and were consolidated through the working group], however due to the COVID-19 outbreak that hit our province early March 2020, the members and resources involved in this deliverable were redirected to work on COVID-19 initiatives to prepare and respond to the imminent COVID-19 outbreak. As a result of this, the eHEALTH MOU is delayed by*

[118] See section 2(f) and 4 under the Centre for Health Information Act, SNL 2018, c. C-5.2

> *several months. Due to the difficulties, and constraints created by the COVID-19 outbreak in the province, a multi-staged approach for the completion of this eHealth MOU is the most suitable option at this point. Given this, the first section for this multi-staged approach of the eHealth MOU would be, Finance and Assets.*
>
> *The next stage of the MOU process, addressing the "Provision of eHealth Services" (the "draft eHealth Services MOU"), was prepared in draft by February 4, 2021 … While the parties continued work towards its completion, this phase of the MOU process was ultimately not finalized.*

[279] It is not clear why the "draft eHealth Services MOU" was not signed. The Centre states it was because the "*parties have known for some time now that the MOU would be moot given the forthcoming move to a single Provincial Health Authority as of April 1, 2023."* Central Health and Labrador-Grenfell Health both state they are *"unable to provide a reason why the remainder of the MOU was not signed*". Eastern Health confirmed it had provided extensive feedback on the Draft MOU to the Centre, stating, "*Eastern Health legal services, privacy, records retention, health technology and data management, and human resources departments all reviewed the draft MOU and made the revisions noted in the April 21, 2021, draft. No attempts were made by [the Centre] to address the changes to the MOU made by Eastern Health, and nothing happened with the MOU after that date*".

[280] However, notwithstanding this document went unsigned, the Centre and the Regional Health Authorities do agree that the terms in the draft MOU were generally followed. The Centre stated in its submissions:

> *While there were some limited instances where [a Regional Health Authority] took some steps relating to cybersecurity without involvement from [the Centre], [the Centre] considers that [the Centre] and the [Regional Health Authorities] generally had a clear understanding of the…accountabilities and execution of responsibilities regarding cyber security under Shared Services.*

[281] The Centre explained its understanding of the general terms of the accountabilities for cyber security under Shared Services stating:

> *(a) [the Centre] was accountable for and executed responsibilities regarding cybersecurity for the personal information of [The Centre] staff and others pursuant to ATIPPA; and*

> *(b) the [Regional Health Authorities] were accountable for and [the Centre] executed responsibilities regarding cybersecurity for:*
>
> *(i) the personal information of [Regional Health Authority] staff and others pursuant to ATIPPA; and*
>
> *(ii) all personal health information in the [the Centre]-managed environment.*

[282] Central Health and Labrador-Grenfell Health confirmed their understanding was that "responsibility for all matters relating to information technology (IT), including cyber security, transitioned to [the Centre]" explaining, in practical terms, that responsibility for IT infrastructure and related services was transferred out of the Regional Health Authority and into the Centre. Eastern Health submissions explain this as well and provide more context stating:

> *[The Centre] made it clear to Eastern Health that it had jurisdiction over matters relating to [information technology and information management] and the majority of Eastern Health's IT employees were transitioned over…All accountabilities and execution of responsibilities regarding cyber security (and all other IT functions) transferred to [the Centre]. As of October 2nd, 2019, Eastern Health had no capacity, resources, or budget to conduct IT operations.*

[283] Eastern Health's submissions state that prior to Shared Services:

> *Eastern Health's Board of Trustees had identified cybersecurity as a risk to the organization. Work had commenced within Eastern Health to implement more cyber training, draft a cyber policy and to participate in cyberworm exercises. The cyberworm tabletop exercises were organized by the Healthcare Emergency Management team at Eastern Health and were done to broaden Eastern Health's knowledge of cyber-attacks and its impacts.*
> *…*
>
> *…[* the first tabletop exercise went back] *as far as 2018 when the manager for security at Eastern Health (…prior to shared services) led the first tabletop exercise for the executive team. Eastern Health leadership believed at the time that cyber security was a threat to the organization and continued where possible to try and raise awareness…*

[284] Eastern Health confirmed it stopped its own cyber security review and monitoring, leaving it for the Centre to action. Eastern Health explains the reasoning for this stating that:

> *Eastern Health had no operational resources to conduct the work post shared services. [The Centre] further enforced these IT boundaries through budgeting*

> *and contracting decisions as they mandated a requirement that all IT budgets and contracts be signed over to them for centralized execution and management going forward.*

[285] Notwithstanding Eastern Health's efforts and interest in improving cyber security, from the time of the implementation of Shared Services it was essentially barred from making substantial efforts to comply with its security obligations under *ATIPPA, 2015* and *PHIA* as it relates to cyber security. No amendments to *PHIA* or *ATIPPA, 2015* were made to remove accountability for those obligations, however, and amendments to the *Centre for Health Information Act* do not over-ride either statute, both of which have paramountcy clauses at sections 11 and 7 respectively. The Ministerial Directive and amendments to the *Centre for Health Information Act* that form the basis in law for Shared Services, essentially restricted Eastern Health (and the other health authorities for that matter), from complying with their statutory obligations under *PHIA* and *ATIPPA, 2015* for cyber security, placing it entirely in the hands of the Centre. There is a strong argument to be made that a province-wide approach to cyber security is a valid policy, however the particular model of implementation that was selected (Shared Services) did not remove or otherwise appropriately account for the statutory obligations of the Regional Health Authorities that existed in *PHIA* and *ATIPPA, 2015* at the time of and in the period leading up to the cyber attack. All of that being said, it can only be a matter for speculation at this point whether Eastern Health, or the other Regional Health Authorities for that matter, would have been better off or worse off from a cyber security standpoint had Shared Services not been implemented.

[286] We noted that within the Centre's Information Note[119] it had listed a variety of ongoing mitigation measures, some of which would necessarily require some level of engagement with the Regional Health Authorities. In the Centre's Information Note it stated that:

> *NLCHI mitigates Phishing attacks with the following activities:*
> ***Information Protection Training and Awareness*** *– NLCHI has an established privacy and security training and awareness program, with a multi-year plans that include yearly training, notifications, bulletins, "Lunch n' Learns", and posters;*

[119] NLCHI Information Note titled *Ransomware: Threat and Mitigation Plans* created in September 2020.

> ***Testing*** *– NLCHI periodically executes simulated Phishing campaigns for all staff, to help train staff to recognize and respond appropriately to Phishing attempts.*

[287] We asked the Regional Health Authorities if these mitigation measures were taking place and how the Regional Health Authorities worked with the Centre in implementation of these measures. The following responses we received provide evidence that the Centre had overstated some of its mitigation measures contained within the Information Note:

> *[Labrador Grenfell-Health] is not aware of any formal Information Protection Training and Awareness programs arranged by [the Centre] prior to the cyber attack beyond a general information/educational presentation given to the [Labrador Grenfell-Health] Board of Trustees and senior executive on September 25, 2021. [Labrador Grenfell-Health]is not aware of phishing campaigns arranged by [the Centre] prior to the cyberattack.*
>
> *Central Health is not aware of any formal information protection training and awareness programs conducted by NLCHI prior to the cyber attack. Central Health attempted to initiate some awareness raising campaigns out of necessity following at least one phishing incident discovered within Central Health (and reported to OIPC…).*
>
> In response to our inquiry asking Eastern Health if these measures were taking place Eastern Health stated *"No, while these plans are most likely drafted, they would have been internal to [the Centre and the Centre's Staff].*

[288] Eastern Health did identify a cyber security training course (~20 minutes in length with educational material) that was developed by the Centre together with Eastern Health's Protection Services Department[120]. Once completed, this course was placed on the LMS (Learning Management System) with continuous availability to staff, which was launched in May 2021 as an onboarding for new hires[121]. While this 20 minute training course is beneficial, the mitigation measures the Centre put forth in its Information Note were overstated when it comes to demonstrable measures put in place across the health system prior to the cyber attack.

[120] Eastern Health submissions confirm its Department of Protection Services has a mandate to provide personal security for Eastern Health. Through this larger mandate, Protection Services functions to provide "very general" cybersecurity awareness.

[121] After the cyber attack in or about the fall of 2022 additional efforts were put in place to engage existing staff in taking this cyber security training course within the Regional Health Authorities.

[289] As noted, neither *PHIA* nor *ATIPPA, 2015* were amended to account for the idea of shared or joint custodianship under a Shared Services arrangement. Under Shared Services, the Regional Health Authorities were left with *accountability* to protect personal health information and personal information, but stripped of all the resources and authority (in light of the Minister's Directive) to put the required protection in place. The Regional Health Authorities were required to rely upon the Centre for this protection. No matter what level of warnings Eastern Health provided, the Centre was the only entity that had the ability to prioritize cyber security and seek the necessary budgetary allocations from the Department to deliver it. To be fair to the Centre, however, there is objective evidence from the Deloitte Assessment that cyber security standards were significantly lacking across the entire provincial health information system, and those were the conditions it inherited with Shared Services.

[290] Commissioner's Delegate Finding: I find that, in the circumstances, in light of the sensitivity of the information and the foreseeability and likelihood of significant harm to privacy that could result from a cyber attack, the Centre, Eastern Health, Central Health, and Labrador-Grenfell Health did not have reasonable security arrangements in place to protect personal health information and personal information at the time of the cyber attack, contrary to section 15(1)(a) of *PHIA* and 64(1)(a) of *ATIPPA, 2015*.

h. Summary of Commissioner's Delegate Findings

[291] The following findings are in relation to security of personal health information and personal information:

- I find that the personal health information and personal information taken in the cyber attack was highly sensitive information that deserved the highest degree of protection.
- I find that a high impact ransomware attack against our province's health care information systems was foreseeable.
- I find that, in the circumstances, in light of the sensitivity of the information and the foreseeability and likelihood of significant harm to privacy that could result from a cyber attack, the Centre, Eastern Health, Central Health, and Labrador-Grenfell Health did not have reasonable security arrangements in place to protect personal health information and personal information at the time of the cyber attack, contrary to section 15(1)(a) of *PHIA* and 64(1)(a) of *ATIPPA, 2015*.

i. COMMISSIONER'S DELEGATE RECOMMENDATIONS ON SECURITY

[292] The following are recommendations regarding security of personal health information and personal information:

> I recommend that the projects outlined in Breakwater be appropriately resourced and implemented within the time frame outlined in the plan, informed and adjusted as required by the Gartner Assessment and any other subsequent assessments or analyses, with the goal of ensuring that cyber security across the provincial health information system meets internationally accepted cyber security standards.

> I recommend that the Provincial Health Authority undertake periodic external reviews, assessments, or audits at reasonable intervals going forward, to assess the status of cyber security across the provincial health information system and to determine whether the cyber security standards found to be in place are appropriate for the size of organization and the nature and sensitivity of the information to be protected, in accordance with internationally accepted cyber security standards, and furthermore to communicate the results of such assessments to the Minister.

X. CONCLUSIONS

[293] In closing, I would like to acknowledge the efforts of the parties in responding to this investigation. In particular, the Centre was mostly forthright and provided the necessary level of detail, although there were exceptions where that level of detail was lacking. The Regional Health Authorities' submissions and responses were generally satisfactory, but in particular, Eastern Health's submissions and responses were the most detailed and forthcoming, and we thank them for providing important information which greatly assisted our analysis of this complex event.

[294] It may not escape notice that while this Report has many findings, it has relatively few recommendations. That is due entirely to the fact that, subsequent to the immediate aftermath of the cyber attack, a great deal of work was launched, led primarily by the Centre, but also with the cooperation of the Regional Health Authorities, to address the vulnerabilities and the shortcomings which the attack had laid bare. In the time that has passed, great strides

have been made to prevent a future cyber attack, and even if one were to occur, to reduce its impact. We encourage this progress to continue.

[295] When it comes to cyber security practices and standards, it must be stated that the threat landscape is vast and it knows no borders. This is part of what makes it such a daunting area for any organization to address. The nature of the threat of cyber attack is constantly changing and evolving, which leads to the conclusion that any defense against such attacks cannot be carried out in isolation. To those who work in cyber security, this goes without saying. Prior to and following the cyber attack, the Centre engaged consultants who can draw on broad networks and extensive experience nationally and internationally. Our health sector, and our province, need to continue to draw on these resources from time to time, and this includes engagement at the Federal-Provincial-Territorial (FPT) level. In 2022, the Federal Government announced a National Cyber Security Strategy. Among its commitments were:

> *The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.*
>
> *...*
>
> *The federal government will lead, in partnership with provinces, territories, and the private sector, the development of a national plan to prevent, mitigate and respond to cyber incidents, one that ensures efficient coordination and effective action.*

[296] One of the purposes of the Strategy is to protect critical infrastructure, which includes: "Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government." Our health information system clearly falls into this category of critical infrastructure. I trust that our Government will fully engage with our FPT partners to ensure that the strategy is developed in such a way that it supports and augments efforts in this province to prevent cyber attacks in the future.

[297] While cyber security has an international, borderless element, the decisions that impact how it is carried out are primarily local, within our own jurisdiction, so this Report will close with some reflections and a recommendation on that front. Although the implementation of

Shared Services meant that the Regional Health Authorities were no longer in a position to, of their own accord and on their own efforts, make improvements to their cyber security, they could certainly communicate those concerns, if they had them, to the Centre, and we do have evidence that at least Eastern Health did so. It must be noted, however, that the Deloitte Assessment, which was conducted in order to assess the state of cyber security across the Regional Health Authorities prior to Shared Services, certainly found a lot of significant vulnerabilities. So, despite having their hands largely tied regarding cyber security from the point of implementation of Shared Services, Central Health, Labrador-Grenfell Health, and Eastern Health must share accountability with the Centre for the state of cyber security prior to the cyber attack.

[298] Even though the Centre failed to take sufficient measures to raise the bar for cyber security for the Regional Health Authorities to appropriate levels following the implementation of Shared Services, we do know through the September 2020 Information Note that some effort was made to inform the Department of the seriousness of the issue. The Information Note itself should have rung alarm bells when it was received by the Department, and one would think the Department would have been asking the Centre what resources it needed to address this matter of substantial significance and urgency. Once again, we have no evidence that any such communication occurred between the Department and the Centre, or whether the Department fully absorbed the implications of the Information Note. The Centre, as noted above, was able to confirm that there was no increase in the budget allocation for the Centre for the purpose of cyber security in the period between the Deloitte Assessment, which identified vulnerabilities that needed to be addressed, and the time of the cyber attack. The Department pointed out that substantial spending has been allocated for cyber security subsequent to the cyber attack.

[299] It must be noted that where budgetary matters are concerned, the Department has indicated that budget submissions are cabinet records and thus cannot be disclosed. Section 102(3) of *ATIPPA, 2015* requires that I take "reasonable precautions to avoid disclosing and shall not disclose … any information or other material if the nature of the information or material could justify a refusal by the head of a public body to give access to a record or part of a record." I have considered all of the information that has been disclosed in this Report,

and it is my view that none of that information would be contrary to my obligation under section 102(3). While this statutory provision serves an important purpose, in this case it limits my ability to establish one particular aspect of accountability. I acknowledge that it is not typically necessary for a privacy breach investigation to even consider such matters, however in this case the interconnected, conflicting, and overlapping accountabilities of the parties has led me to consider its potential relevance.

[300] For the purposes of establishing a key locus of accountability for decisions that contributed to the failure to bring cyber security standards up to an acceptable level prior to the cyber attack, it would be helpful to be able to say whether one of two events occurred: whether the Centre, despite Government direction not to make a request for an increased *operational* budget, might have made a budget request for cyber security purposes for a *capital* budget allocation OR, alternatively, whether it did not make any such requests. If the Centre made such a request but was denied, one could conclude that it attempted to fulfil its mandate to some extent by ensuring that pressing cyber security improvements were resourced. If such a request was made but denied by the Minister or Cabinet, we could place a certain amount of accountability there. If no such requests were made by the Centre, then clearly the Centre's leadership would have to be accountable for that. Unfortunately that is one aspect of accountability associated with the cyber attack that I believe I am barred by statute from addressing in this Report, and if that information is ever to be disclosed it must be through another process or proceeding other than this investigation. I note, however, that I have made this assessment in light of the particular language in section 102(3), and my decision in that regard does not bind the Commissioner should the matter come before him in the future in making findings or recommendations resulting from a complaint about an access to information request.

[301] As stated in the previous section of this Report, with the pursuit of Breakwater, there are reasonable cyber security steps now being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack. The Department's move to combine the Centre and the Regional Health Authorities into the Provincial Health Authority will assist in these efforts, as it will eliminate any uncertainty or friction around roles and accountabilities that were inherent in Shared Services.

[302] However, notwithstanding the integration into one legal entity, there remains the practical reality of ensuring that cyber security for the entire health care information system, across the province, is raised to and maintained at an appropriate standard. While much progress has been made already in that regard, there is more to be done, and it will be an ongoing task, involving not just technical measures, but appropriate policies and employee training, and crucially, leadership.

[303] Establishing a consistent culture of privacy starts with creating clear roles and accountabilities within senior management and executive. In an organization as large and complex as the new Provincial Health Authority, privacy protection should not just be part of the role of a senior official who has other responsibilities.

[304] Commissioner's Delegate Recommendation:

> I recommend the creation of a Chief Privacy Officer position, within the Provincial Health Authority, at or reporting directly to the executive level, whose role it is to ensure that privacy best practices are embedded within all of the Authority's activities, and to help ensure the Authority's compliance with privacy laws. The person to fill that role should have qualifications and experience in privacy, with an appropriately resourced staff to carry out that mandate, from the largest hospital to the smallest clinic to virtual care, encompassing all parts of the Authority's activities, including primary care, secondary uses of information for research and evaluation, and employee personal information.

XI. FINDINGS

[305] The following constitute the findings of this Report:

1. I find that reasonable steps were taken to investigate and attempt to contain the privacy breach.
2. I find that reasonable steps were taken to investigate the credential compromise.
3. I find that prior alerts were not properly investigated and/or responded to. Had this been done it may have prevented or reduced the extent of the malicious extraction of data that followed.
4. I find that the breach of personal information and personal health information stolen in this matter was not contained.
5. I find that the credit monitoring service being provided to those impacted by the cyber attack is a reasonable containment step.

6. I find that there is a risk of significant harm that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the credit record within the meaning of section 64(8) of *ATIPPA, 2015*.

7. I find that there is a risk of adverse impact upon the mental, physical, economic, or social well-being to impacted individuals that includes humiliation, damage to reputation or relationships, financial loss, identity theft, and negative effects on the individual's credit record within the meaning of section 15(7) of *PHIA*.

8. I find that the personal information and personal health information accessed and taken in the attack is highly sensitive information. It is the kind of information that is associated with a high risk of misuse by bad actors and the consequences of such misuse are significant for victims.

9. I find there is an increased risk to impacted individuals associated with the cause and extent of the breach.

10. I find that there is foreseeable harm to individuals impacted by the privacy breach from theft of their personal information and/or personal health information.

11. I find that the impact of the cyber attack has contributed to an erosion of public trust in Government and the Provincial Health Authority and that this was a foreseeable harm from such an event.

12. With the exception of some matters related to notification, I find that the steps taken in response to the cyber attack largely demonstrate that the entities evaluated risk appropriately.

13. I find the length of time that elapsed prior to the public being notified of this being a ransomware cyber attack concerning, and the rationale provided for such a delay to be insufficient to justify it.

14. I find the use of Public Advisory Briefings was a reasonable approach to take in providing notification to affected individuals in the circumstances of the large-scale breach caused by the cyber attack.

15. I find the timing and manner in which the public was notified of information being "taken" in the cyber attack concerning.

16. I find the Regional Health Authorities' use of multiple methods of notification was a reasonable approach in providing notification in the circumstances of the large-scale breach caused by the cyber attack.

17. I find that reasonable notification measures were taken by the Regional Health Authorities to notify individuals impacted by the cyber attack.

18. I find the Regional Health Authorities' reliance on the information provided to it by the Centre for Health Information to be reasonable in the circumstances.

19. I find the Department's role in overseeing and managing notifications and the Centre for Health Information's role in investigating the cyber attack and resulting privacy breach reasonable in the circumstances.

20. I find the initial delay in confirming the existence of the cyber attack privacy breach (the delay between November 1, 2021 up to when the public was first informed of the privacy breach on November 9, 2021) reasonable in the circumstances.

21. I find, that as of November 8, 2021, the Department and Centre knew that personal information and personal health information was both accessed and taken (exfiltrated) by the Threat Actor in the cyber attack.

22. I find, that at the Public Advisory Briefings held on November 9, 2021 and November 10, 2021, the Department was in a position to notify the public that the information being described as accessed, was in fact taken (exfiltrated) by the Threat Actor in the cyber attack and failed to do so.

23. I find that the impacted public was not informed at the first reasonable opportunity of personal information and personal health information being taken in the cyber attack, as required by section 15(3) of *PHIA* and section 64(3) of *ATIPPA, 2015*.

24. I find the public was not informed of this being a ransomware cyber attack, nor of this attack being perpetrated by the HIVE ransomware group at the first reasonable opportunity.

25. I find the content of notifications made about the privacy breach should have included more details about the nature of the attack, namely that it was a ransomware cyber attack together with other general details, such as confirmation that a Threat Actor exfiltrated/stole data containing personal information and/or personal health information for malicious purposes.

26. I find that the necessary investigations were conducted to determine, to the extent possible, the root causes of the privacy breach and the cyber attack as a whole.

27. I find that reasonable cyber security steps have been and are being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack.

28. I find that the collection of SIN information at patient registration was in contravention of section 29(3) and section 32(1) of *PHIA*.

29. I find that reasonable steps have now been taken to delete and prevent the unnecessary collection of patient SIN at registration.

30. I find that the Regional Health Authorities failed to implement appropriate records management policies and procedures relating to retention and destruction of personal information and personal health information prior to the cyber attack, which unnecessarily left this information vulnerable to a breach of privacy.

31. I find that reasonable steps are being taken towards the development and implementation of a records retention and destruction schedule.

32. I find that the personal health information and personal information taken in the cyber attack was highly sensitive information that deserved the highest degree of protection.

33. I find that a high impact ransomware attack against our province's health care information systems was foreseeable.

34. I find that, in the circumstances, in light of the sensitivity of the information and the foreseeability and likelihood of significant harm to privacy that could result from a cyber attack, the Centre, Eastern Health, Central Health, and Labrador-Grenfell Health did not have reasonable security arrangements in place to protect personal health information and personal information at the time of the cyber attack, contrary to section 15(1)(a) of *PHIA* and 64(1)(a) of *ATIPPA, 2015*.

XII. RECOMMENDATIONS

[306] The following recommendations are directed to the Provincial Health Authority. I make these recommendations in accordance with section 72(2)(c)(iv) of *PHIA* and section 76(2)(a) of *ATIPPA, 2015*:

1. I recommend the Provincial Health Authority provide an update within its communications (such as each Region's website landing pages for the 2021 cyber attack) confirming this was a ransomware cyber attack and providing a link to Government's Report which outlines more details about the attack and prevention steps being taken.
2. I recommend that the Provincial Health Authority update notification policies to reflect that where there is a breach of personal information or personal health information (where notification is required under an Act), that in the case of a ransomware cyber attack, notification should include information about those circumstances at the earliest reasonable opportunity, and furthermore that the factors considered in making such decisions about notification must be documented.
3. I recommend that the Provincial Health Authority continue to take diligent steps to ensure that information management policies and procedures addressing retention and destruction of personal information and personal health information are developed and implemented to minimize the breadth and impact of any future privacy breach.
4. I recommend that the projects outlined in Breakwater be appropriately resourced and implemented within the time frame outlined in the plan, informed and adjusted as required by the Gartner Assessment and any other subsequent assessments or analyses, with the goal of ensuring that cyber security across the provincial health information system meets internationally accepted cyber security standards.
5. I recommend that the Provincial Health Authority undertake periodic external reviews, assessments, or audits at reasonable intervals going forward, to assess the status of cyber security across the provincial health information system and to determine whether the cyber security standards found to be in place are appropriate for the size of organization and the nature and sensitivity of the information to be protected, in accordance with internationally accepted cyber security standards, and furthermore to communicate the results of such assessments to the Minister.

6. I recommend the creation of a Chief Privacy Officer position, within the Provincial Health Authority, at or reporting directly to the executive level, whose role it is to ensure that privacy best practices are embedded within all of the Authority's activities, and to help ensure the Authority's compliance with privacy laws. The person to fill that role should have qualifications and experience in privacy, with an appropriately resourced staff to carry out that mandate, from the largest hospital to the smallest clinic to virtual care, encompassing all parts of the Authority's activities, including primary care, secondary uses of information for research and evaluation, and employee personal information.

[307] Section 74 of the *Personal Health Information Act* requires the head of the Provincial Health Authority to give written notice of his decision with respect to these recommendations to the Commissioner's Delegate and any person who was sent a copy of this Report within 15 (calendar) days after receiving this Report. Section 78 of the *Access to Information and Protection of Privacy Act, 2015*, requires the head of the Provincial Health Authority to give written notice of his decision with respect to these recommendations to the Commissioner's Delegate within 10 business days following receipt. Accordingly, given that the 10 business day deadline under *ATIPPA, 2015* is one day earlier than 15 calendar days and both are statutory deadlines, the head of the Provincial Health Authority must provide written notice of his decision on each recommendation by the earlier of the two deadlines, which is 10 business days following receipt of this Report.

[308] Dated at St. John's, in the Province of Newfoundland and Labrador, this 23rd day of May 2023.

Sean Murray
Commissioner's Delegate
Office of the Information and Privacy Commissioner
Province of Newfoundland and Labrador

XIII. CONFIDENTIAL ANNEX

Purpose: To provide the Provincial Health Authority with the benefit of some observations and analysis drawn from the work of our consultants which cannot be disclosed in a public report due to the risk to cyber security from releasing such details. The head of the Provincial Health Authority may choose to distribute this Annex to those deemed appropriate within the organization in full or in redacted form.