SAFEGUARD

A quarterly newsletter published by the
Office of the Information and Privacy Commissioner

Volume 7, Issue 3 August 2023

Contact Information

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:
commissioner@oipc.nl.ca

Website:
www.oipc.nl.ca

Follow us on social media!

Twitter:
@oipcnl

New!
LinkedIn:
https://Linkedin.com/company/oipc-nl

This Issue:

OIPC Report on the 2021 Cyber Attack

Brief Background

In October 2021, the HIVE ransomware group entered our province's health care information systems. Its presence went unnoticed for a two-week period, after which time it brought the majority of health care services to a grinding halt through a ransomware cyber attack. Although it was not immediately known at the time, most everyone in our province had some amount of personal health information or personal information accessed and taken in this ransomware cyber attack.

> *"…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…"*
>
> -Report P-2023-001/PH-2023-002 pages 26-27

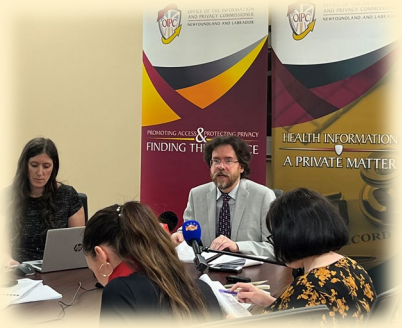
In the months that followed, considerable efforts took place to bring the health care system back to functioning capacity. In conjunction with restoration of services, the impacted entities took steps to investigate the breach, attempt containment, provide notification, and implement measures to prevent future breaches.

In the aftermath of the cyber attack, on December 8, 2021, our Office confirmed we would be launching an investigation into this province's largest privacy breach. The official investigation began on April 8, 2022, and was conducted over the course of 13 and a half months. We examined the response to the breach of our province's Regional Health Authorities, the Newfoundland and Labrador Centre for Health Information and the Department of Health and Community Services. We also assessed the security and information practices that were in place at the time of the attack, and examined the steps being taken after the cyber attack to strengthen our health information systems.

On May 23, 2023, our Office issued Report P-2023-001/PH-2023-002 outlining the results of our largest and most complex investigation to date. In total, this Report contains 34 findings and six recommendations, the latter of which we outline below.

We encourage you to read this Report as it provides an overview of the law and acts as a cautionary tale to those who do not place sufficient priority on ensuring there are reasonable cyber security arrangements in place to protect the personal information and personal health information that is collected and stored.

While there are many takeaways that can be found within our Report, which spans more than 100 pages, for purposes of this Newsletter, we are focusing on the breach of the personal health information and some takeaways that may be helpful to custodians.



-May 24, 2023 Sean Murray, Director of Research and Quality Assurance, and Commissioner's Delegate who concluded the investigation, providing a briefing to media on Report P-2023-001/PH-2023-002. To Sean's right is lead investigator Meagan Cottreau.

TAKEAWAYS

Collection of More Information than was Necessary

Many people in our province had their personal health information taken. A large part of the privacy breach involved information that was collected by the health authorities at registration. This included information such as names, contact information, MCP numbers, reason for the visit, birth dates, email addresses, etc.[1] After the cyber attack, it came to light that a relatively small group of patients also had their social insurance number (SIN) collected during registration for medical services. Pursuant to section 5(1)(d) of *PHIA*, this registration information constituted "personal health information".

> *"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…"*
>
> -Report P-2023-001/PH-2023-002 page 81

Section 32(1) of *PHIA* specifically limits the scope of information a custodian is able to collect. The provision states in full:

> *32.(1) A custodian shall not collect more personal health information than is reasonably necessary to meet the purpose of the collection.*
>
> *(2) Subsection (1) does not apply to personal health information that a custodian is required by law to collect.*

Our Report found the collection of patient SIN information at registration was not reasonably necessary to meet the purpose of the collection. In fact, it had occurred due to staff entry error whereby SIN information was collected because there was an input field on the registration screen where it *could* be entered. This collection was in clear contravention of section 32(1). Measures were subsequently taken by the Regional Health Authorities to rectify this issue on a prospective

[1] For a complete breakdown of what information was taken in the attack see pages 19 through 24 of the Report.

basis, but the patient SIN information that did not need to be collected at all, was nevertheless part of what was taken in the cyber attack.

Takeaway: When collecting personal health information, it is important to ensure that the information being collected is "reasonably necessary to meet the purpose of collection" to comply with *PHIA* requirements. In doing so, this will not only comply with the law, but will also minimize the impact or scope of a potential breach.

Tip: Periodically review policies, procedures, and forms (electronic or paper) used in the collection of personal health information and take action as appropriate to ensure the risk of over collection is minimized or eliminated.

Failure to Manage Information Throughout its Lifecycle

PHIA does not provide a timeline for how long records must be kept or when they must be destroyed. However, section 13 of *PHIA* does require a custodian to, among other things, put in place policies and procedures that address record retention and disposal. Part of protecting personal health information is ensuring such policies and procedures are in place and, in doing so, this will likely minimize risk associated with a future breach.

> *"…[the custodians] failed to implement appropriate records management policies and procedures…which unnecessarily left this information vulnerable to a breach of privacy."*
>
> -Report P-2023-001/PH-2023-002 page 83

The cyber attack revealed the health care custodians did not have a record retention and destruction schedule in place. This meant some records that might have otherwise been appropriately destroyed, if there had been records management policies and procedures in place, were still present and subject to being taken in the attack. Our Report found that this failure unnecessarily left this information vulnerable to a breach.

Takeaways: When collecting personal health information, it is important to ensure there are policies and procedures in place to manage this information throughout its lifecycle in compliance with section 13 of *PHIA*. Part of information management includes having policies and procedures that address the retention and destruction of records.

Direct Notification versus Indirect Notification

Pursuant to sections 15(3) and 15(7) of *PHIA*, custodians are required to notify individuals whose personal health information is breached, unless the breach will not have an "adverse impact" on the individual. While *PHIA* requires notification to occur, it does not state "how" this notification should occur. Custodians must assess what method(s) of notification to use and determinations of "how" notification occurs will largely depend upon the particular circumstances of each privacy breach.

In the 2021 cyber attack, the majority of people who had their personal health information taken did ***not*** receive direct notification, in other words, they did not receive a phone call, an email or a letter in the mail confirming their information was taken. Rather, the majority of people who had their personal health information taken received notification by indirect means through a mixture of public notification efforts. As described in our Report, in most circumstances, reasonable notification of a breach will require direct notification to affected individuals. However, there are circumstances where providing only indirect notification (e.g. public advisory briefings, news releases, website notifications, social media postings, newspaper advertisements, etc.) may nevertheless serve as a reasonable method of notification to impacted individuals. 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.

> *"When a…custodian determines notification is necessary…in most circumstances, reasonable notification will require direct notification to affected individuals."*
>
> -Report P-2023-001/PH-2023-002 page 54

In the cyber attack, a portion of affected individuals did receive *direct* notification, but, as stated above, a large number of impacted individuals did not receive direct notification at all, with the custodians relying exclusively upon *indirect* notification measures to reach a significant portion of those impacted. Exclusive reliance upon indirect notification measures occurred due to many compounding factors (e.g. breach magnitude, resource limitations, accuracy concerns for dated contact information, etc.). Our Report found that the Regional Health Authorities did take reasonable notification measures to notify individuals impacted by the cyber attack and this includes exclusive reliance upon indirect notification measures for a portion of the breach.

The circumstances of the cyber attack were very fact specific and custodians should continue to remain cautious of using indirect notification as the only notification measure. 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 or accuracy of older contact information, risks of further privacy breaches, etc.

Takeaways: If a custodian is struggling with determinations as to whether or not to provide direct notification to individuals affected by a breach, be mindful that in most circumstances reasonable notice will require direct notification. However, this is an assessment that a custodian must determine on a case-by-case basis.

Tips: Document reasons for *why* a particular method or methods of notification are being chosen, especially when a decision is made to rely exclusively upon indirect notification measures. Maintaining such a record will allow the custodian to reflect upon its past decisions, which may result in making adjustments to improve upon existing policies or procedures associated with responding to a breach in the future. In addition, this will allow a custodian to be in a better position should they need to respond to our Office's investigation of a privacy complaint about the breach.

Notification Issues

Once a decision is made that notifications are required, section 15(3) of *PHIA* requires that individuals affected by the breach 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, custodians are accountable for their notification decisions, including their interpretation of when they deemed "the first reasonable opportunity" to be.

In the case of the cyber attack, our Report contains findings confirming the public could have been informed that information had been *taken* at earlier public advisory briefings, and that the public could have been informed earlier of the fact that this was a ransomware cyber attack (whereby a malicious actor is threatening release of information). It took almost 500 days for the public to be informed this was a ransomware cyber attack and no evidence or submissions were provided to our Office to justify this delay. Our Report found that, in contravention of section 15(3) of *PHIA*, the impacted public was not informed at the first reasonable opportunity that information had been *taken* in the attack, nor that this was a ransomware cyber attack.

> *"…key information was already known by both the Centre and the Department and withheld from the public…"*
>
> -Report P-2023-001/PH-2023-002 page 68

When notification is required, 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.

As stated in the Report, notifications to individuals impacted by a breach should include:

- 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; and
- our Office's contact information and notification of an individual's right to make a complaint.

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.

The likelihood of harm resulting from a privacy breach is increased where personal health information is compromised due to actions of a malicious nature. In the case of a ransomware cyber attack, malicious actions can include deliberate intrusion, deployment of ransomware, exfiltration of the information, or threats of disclosure. 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), or decisions about how quickly to engage in such measures.

Our Report found that 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 malicious actor exfiltrated or stole data containing personal information or personal health information for malicious purposes.

Takeaways: Impacted individuals should be notified, at the earliest reasonable opportunity, and notification details 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.

Tips: As noted above, these decisions should be documented as well.

Failure to have Reasonable Cyber Security Measures in Place

The Report confirms that the security of our province's health information system was lacking at the time of the cyber attack, with industry standard cyber security measures either not in place or not fully implemented, which left the personal health information of our province's citizens vulnerable to a cyber attack, something which was almost an inevitability. Vulnerabilities were known within the health care system and there was a failure to take sufficient and timely steps to remedy them. As stated in the executive summary of the Report:

> *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.*

The personal health information in the cyber attack was highly sensitive information that deserved the highest degree of protection and a high impact ransomware attack against our province's health care information systems was foreseeable. The Report found that the custodians did not have reasonable security arrangements in place to protect this personal health information contrary to section 15(1)(a) of *PHIA*.

While our Report did not specify the exact tools and techniques that were used in the ransomware cyber attack, it nevertheless listed the many mitigation measures that were being recommended to defend against the HIVE ransomware group. These recommended mitigation measures included things like ensuring two-factor authentication with strong passwords, continuous monitoring, an active vulnerability management program, keeping computers, devices, and applications patched and up-to-date[2].

> **"…the tactics and tools that they used in this cyber attack were not "unstoppable". In fact, many…were basic techniques commonly used in cyber attacks and were well known within the cyber security community."**
>
> -Report P-2023-001/PH-2023-002 page 88

[2] For a full list of mitigation measures that were being recommended to defend against this ransomware group see pages 88 and 89 of the Report.

While our Report found that the custodians did not have reasonable security arrangements in place at the time of the cyber attack, it does go on to state that reasonable cyber security steps were being taken to mitigate the risk of a future breach as it relates to the vulnerabilities that contributed to the cyber attack. The Report states at paragraph 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.*

However, the Report goes on to caution within paragraph 302:

> *…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.*

Takeaways: Ransomware cyber attacks are continuing to occur throughout the world and the health sector is one of its prime targets. As custodians who collect and retain personal health information, your systems are specifically being targeted by malicious actors who operate in an organized businesslike fashion. Personal health information is highly sensitive information and it is your responsibility to ensure its protection, including making sure there are reasonable cyber security measures in place.

Tips: Do not be reactive, be proactive in ensuring there are reasonable cyber security arrangements in place. Cyber security is not a one-time fix. It is an ongoing project, and it is essential that sufficient focus and resources continue to be directed to this task. Review your contracts with Information Managers, contractors and agents who have access to the personal health information of your patients and clients. Specifically ask them whether they have taken measures to ensure their cyber security defenses are up to date in light of the increase in cyber attacks on health information systems.

The Report's Recommendations

As of April 1, 2023, the entities involved in the cyber attack were integrated into one Provincial Health Authority known as NL Health Services. While the Report outlines what occurred with respect to individual entities, the recommendations were addressed specifically to NL Health Services as the Provincial Health Authority. The recommendations made in our Report are as follows:

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.

The responding letter to our Report sent on behalf of the Provincial Health Authority ("PHA") includes confirmation that:

> *The PHA appreciates the OIPC's recognition of the tremendous efforts of the PHA to continue to further enhance cybersecurity for the health sector in Newfoundland and Labrador. While the PHA disagrees with a number of the findings in the Report, the PHA will comply with all of the recommendations in the Report*.

Summary Part 2 of *PHIA* Toolkit for Small Custodians – Coming Soon!

This Office released new guidance for small custodians – *PHIA* Toolkit for Small Custodians on March 31, 2023. As this guidance piece is detailed, we have broken it down into two parts.

If you happened to have missed it, be sure to see Summary Part 1 in the previous issue of Safeguard where we covered the definitions of custodian, agent and information manager as well as some custodian obligation.

Stay tuned for Summary Part 2, which will be in the next issue of Safeguard where we will go over security as it relates to personal health information; collection, use and disclosure of personal health information; and access and correction of personal health information. A review of the full guidance piece is still recommended!

Breach Notifications

Between May 1, 2023 and July 31, 2023, OIPC received seven breach notifications from six different custodians. Email and fax breaches remain the most common with the misdirection of personal health information or not using the blind copy (Bcc) function when emailing large groups.

During the last quarter, one custodian had some information stored on a third party contractor's server and that contractor experienced a cyber incident. The custodian is working with the contractor in an ongoing investigation to confirm what information was stored on the server and what if any personal health information was compromised. The interim results indicate that only one record containing personal health information was taken during the cyber incident. The custodian has consulted with OIPC regarding this breach and continues to work with the contractor during the investigation.

We would like to remind custodians that OIPC can offer *PHIA* training that is customized to their needs!

Interested custodians should email OIPC at commissioner@oipc.nl.ca.

There are also a number of *PHIA* resources available on OIPC's website.