**amended at clause [54](c)*

OFFICE OF THE
INFORMATION & PRIVACY COMMISSIONER
for
Prince Edward Island

Investigation Report: IR-24-001
(OIPC File No: BRH-22-040)

Custodian: Health PEI

Prince Edward Island Information and Privacy Commissioner
Denise N. Doiron

January 25, 2024

Summary: Health PEI was advised by a temporary contract employee that a laptop assigned to them had been stolen from their vehicle, along with a paper notebook. The notebook did not contain personal information or personal health information, but the laptop contained both. The laptop was not recovered. Health PEI notified affected individuals, conducted an investigation, and took a number of remedial actions. The Commissioner was satisfied that Health PEI responded appropriately to the breach, but made recommendations around security for laptop computers and other mobile devices.

Statutes Considered: *Freedom of Information and protection of Privacy Act*, R.S.P.E.I. 1988, Cap. F-15.01, section 35

Health Information Act, R.S.P.E.I. 1988, Cap. H-1.41, section 36 and 39

Cases Considered: *Department of Health and Social Services (Re)*, 2019 NTIPC 10 (CanLII)

Nova Scotia Health Authority (Re), 2020 NSOIPC 2 (CanLII)

I. BACKGROUND

[1] On or about April 5, 2022, Health PEI was advised by an employee of Health PEI (the "Employee") that a laptop assigned to the Employee had been stolen from their vehicle in the overnight hours between April 4 and April 5, 2022. The Employee was a temporary contract employee, whose contract was almost up when the incident occurred. The Employee's job duties included working on various analysis projects related to health care services delivery and patient flow between services.

[2] The Employee reported they had taken the laptop home after work and left it in their parked vehicle overnight, in the back seat in a backpack-style bag, along with a paper notebook. The following morning, the Employee discovered the bag containing the laptop and notebook was missing from the vehicle. The Employee stated they believed they had locked the vehicle, but they did not see any signs of forced entry.

[3] The Employee immediately notified police of the theft and reported it to their manager at Health PEI, who then reported the incident to the Executive Director of Performance and Innovation. The Employee indicated there was no personal information ("PI") or personal health information ("PHI") in the paper notebook, but the files they had saved to the hard drive of the laptop likely contained both PI and PHI.

II. JURISDICTION

[4] Health PEI is a health information custodian as defined in the *Health Information Act* ("*HIA*") and a public body under the *Freedom of Information and Protection of Privacy Act* (*"FOIPP Act"*). Therefore, I am satisfied I have jurisdiction in this matter.

III. INFORMATION

[5] I accept Health PEI's assessment that the laptop contained both PHI and PI.

[6] The types of information that had been saved to the hard drive of the laptop can be generally described as:

(a) full patient names;
(b) Provincial Health Numbers;
(c) dates/times of registration, admission and discharge;
(d) reason for patients' visits;
(e) patients' family doctors;
(f) facilities, units, and length of patients' stay in hospital; and
(g) full staff names and employment information.

[7] The types of information described in clauses (a) through (f) above meets the definition of "personal health information" as set out in the *HIA*, and the types of information described in clause (g) above meets the definition of "personal information" as set out in the *FOIPP Act*.

[8] The information was from four months in 2021 and 2022, including information about patients visiting the Emergency Department between September and October 2021, information about patients medically discharged but remaining in hospital in February 2022, and information about employees working in Health PEI-operated long-term care facilities in January and February 2022.

IV. ISSUE

[9] The issue in this investigation is not whether a privacy breach occurred, as Health PEI acknowledged that the technical, physical, and administrative safeguards in place to protect PHI and PI were not followed, and that the incident was a breach of privacy.

[10] The issue in this review is whether Health PEI took appropriate steps to respond to the privacy breach.

V. DISCUSSION

[11] When there is a privacy breach, there are several steps a custodian is expected to take in response:

(a) Containment of the breach;
(b) Notifications to affected individual/s and to the Commissioner;
(c) Investigation of the circumstances of the breach; and
(d) Remediation.

Some of these steps can be, and should be, followed concurrently. For instance, in this matter, Health PEI's investigation commenced immediately upon being notified of the incident and continued throughout the process, while the other steps were also being undertaken. However, for ease of reference, I will address each step separately below.

(a) Containment of the breach

[12] Upon being notified of the theft of the laptop and determining there was a high degree of likelihood that the laptop contained PHI and sensitive PI, Health PEI immediately reported the incident to Information Technology Shared Services ("ITSS") and notified the Health PEI Privacy Officer. Health PEI initiated a breach response plan and commenced an investigation the same day the incident was reported by the Employee. They reported the incident to the police and requested the police to investigate the theft. Health PEI also requested ITSS to conduct a security assessment and take whatever steps it could to restrict access to the information on the laptop.

[13] ITSS did an initial security assessment and immediately took what measures were available to them to reduce the risk of unauthorized access to the PHI/PI on the laptop, such as changing the Employee's login credentials (username and password) and disabling the laptop's ability to access Health PEI and Government networks. ITSS was not able to determine if the laptop was encrypted. ITSS did not have the ability to remotely track the location of the laptop or remotely erase the hard drive of the laptop.

The initial security assessment report was provided to Health PEI two days later, on April 7, 2022, with a follow up report on April 29, 2022.

[14] I am satisfied that Health PEI's initial response to the breach and their efforts at containment were appropriate. They acted immediately upon being notified of the theft of the laptop and took all reasonable steps available to them to contain the breach. While it would have been preferable for the laptop to have been encrypted, or for ITSS to have been able to remotely locate the laptop and/or remotely lock or erase the hard drive, these options were not available.

(b) Notifications

[15] Health PEI is both a custodian under the *HIA* and a public body under the *FOIPP Act*. Both statutes have requirements to protect the PHI/PI in their custody or under their control. Health PEI determined that both PHI and PI were compromised as a result of this incident. Notification requirements are not the same for both Acts.

Health Information Act

[16] Section 36 of the *HIA* requires that a custodian notify an affected individual and the Commissioner if PHI is lost or stolen, unless the custodian reasonably believes that the theft or loss will not have an adverse impact on the provision of health care or other benefits to the affected individual, or on the mental, physical, economic, or social well-being of the individual.

[17] Health PEI utilized the security assessment reports from ITSS to assist in completing a Real Risk of Significant Harm ("RROSH") assessment, to determine the level of risk of adverse impacts to individuals whose PHI/PI may have been able to be accessed, and to determine next steps in notifying individuals potentially affected by the privacy breach.

[18] Because ITSS could not confirm whether the laptop was encrypted, Health PEI worked under the assumption the laptop was not encrypted when assessing the risk of adverse

impact. I am satisfied that this was a prudent assumption, considering the sensitivity of the information involved in the breach incident.

[19] However, I do not endorse the use of the RROSH threshold for assessing whether notification is required under the *HIA*. The benchmark of "real risk of significant harm" is a much higher threshold than is contained in the *HIA*. Utilizing a RROSH threshold could lead to a custodian in PEI not meeting their legislative obligations for notification under the *HIA*.

[20] Section 36 of the *HIA* requires a custodian to notify an individual to whom the PHI relates, and the Commissioner, if the PHI is stolen, lost, disposed of without authority or disclosed to or accessed by an unauthorized person. The only exception is when the custodian "reasonably believes that the theft, loss, disposition or disclosure of, or access to the personal health information will not have an adverse impact on the provision of health care or other benefits to, or the mental, physical, economic or social well-being of, the individual to whom the personal health information relates."

[21] What this means is that the threshold for requiring notification of an individual and the Commissioner is "a reasonable belief of adverse impact" on the provision of health care or other benefits to, or the mental, physical, economic or social well-being of the individual. A reasonable belief of adverse impact is a much lower threshold than a "real risk of significant harm", which is the threshold for the RROSH assessment tool. Therefore, use of the RROSH may result in a custodian deciding not to notify an individual when the legislation would have otherwise required them to do so.

[22] In this instance, Health PEI decided to notify, so their use of the RROSH threshold, although not appropriate, did not result in Health PEI failing to comply with the notification requirements under the *HIA*. I would encourage Health PEI to ensure they have a more appropriate method of assessing whether there is a reasonable belief of adverse impact, to ensure they are meeting their legislative obligations regarding notification in the event of a privacy breach.

[23] Health PEI indicated that although they did not have evidence to suggest anyone had accessed the PHI/PI that was saved to the laptop's hard drive, there was a potential that a third party could access the PHI and PI on the stolen laptop because they assumed the laptop was not encrypted and ITSS was not able to erase or lock the hard drive remotely. Health PEI considered the risk of identity theft from the lost or stolen PHI and PI was very low as they believed information contained on the laptop could not be used for the purposes of proving identity.

[24] I would note that other jurisdictions have assessed the risk of identity theft as higher than "very low" when similar kinds of PHI/PI were compromised, finding that the risk of identity theft or fraud is possible with only a name and date of birth (see: *Department of Health and Social Services (Re)*, 2019 NTIPC 10 (CanLII)). Further, there is a potential risk of health care fraud when PHI is involved (see: *Nova Scotia Health Authority (Re)*, 2020 NSOIPC 2 (CanLII)), which Health PEI has not addressed, and it is unclear whether they assessed this potential risk.

[25] Insurance companies and cybersecurity professionals in North America have been warning about the value of healthcare data for malicious actors for years. The risks associated with PHI are not identical to the risks associated with identity or credit fraud. With financial data, such as credit cards or bank account numbers, the stolen numbers can be cancelled or changed. But, with health information, individuals cannot just cancel or change this information. Health care information associated with an identifiable individual is permanent.

[26] The more PHI in a dataset, the higher the risk that the information could be used fraudulently, whether for identity theft or other malicious purposes, such as health care fraud. There was sufficient PHI associated with full names (such as Provincial Health Number, medical issues, family doctor, dates and locations of services) that could potentially result in health care fraud. In addition, small amounts of PHI/PI obtained through a privacy breach can be put together with other information, which could be publicly available or obtained through other avenues, to further identify individuals to

target for fraudulent purposes, or to enhance the profile known about an individual that could make them more susceptible to fraud. Social engineering techniques used by malicious actors are getting increasingly sophisticated and better able to use smaller sets of information to effect significant malicious acts. Seniors are particularly vulnerable to such targeting, but it makes everyone more vulnerable, raising the potential risk level when particularly sensitive information, such as PHI, is compromised.

[27] For these reasons, I do not agree that the risk was "very low". I would have assessed the risk as being closer to "moderate" in the circumstances. This may not have reached the level of "real risk of significant harm" under the RROSH threshold assessment, but it very well may have met the threshold of adverse impact required for notification under the *HIA*.

[28] Nevertheless, because the information on the laptop included PHI, which is sensitive information, and that information was associated with full patient names, Health PEI assessed there to be a potential risk of adverse impact related to humiliation or damage to reputation or relationships if the information were to be accessed by an unauthorized individual. For these reasons, Health PEI determined that it was required under the *HIA* to notify both the affected individuals whose PHI was involved in the breach and the Commissioner. The decision to notify affected individuals and the Commissioner was the correct decision in these circumstances.

Freedom of Information and Protection of Privacy Act

[29] As mentioned earlier, the *FOIPP Act* does not have the same requirements as the *HIA* when a privacy breach occurs. Section 35 of the *FOIPP Act* requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, disposal or destruction of PI. However, there is no requirement for a public body to notify affected individuals or the Commissioner in the event of a breach of privacy involving PI.

[30] The PI involved in the breach was PI of Health PEI employees. In this instance, Health PEI considered the PI to be sensitive information and assessed the potential for unauthorized access, and potential for adverse impacts, to be the same as for the PHI. For this reason, Health PEI made the decision to voluntarily notify their employees whose PI was involved in the breach, and to voluntarily notify our office of the breach. They included the theft of the PI in their investigation of the theft of the PHI.

No Notification to Estates

[31] I note that there was a total of 118 individuals whose PHI or PI was involved in the breach but who were deceased at the time the breach occurred. Health PEI decided not to send notifications to the estates of these 118 individuals because Health PEI assessed the risk of adverse impact to these individuals or their estates to be low. I agree with this assessment, and Health PEI's decision not to notify the estates of these individuals.

Timing of Notification

[32] Section 36 of the *HIA* requires that notification must be given to the individual to whom the PHI relates and the Commissioner, in writing, at the first reasonable opportunity. The "first reasonable opportunity" is a subjective standard and will depend on the circumstances in each specific breach scenario. The first reasonable opportunity in one set of circumstances may not be the same amount of time in other circumstances. It must be assessed on a case-by-case basis.

[33] Health PEI notified our office of the breach on April 6, 2022, which was the day after they became aware of the theft of the laptop. They also provided periodic updates as the investigation progressed.

[34] In late May, 2022, approximately 8 weeks after they became aware of the theft, Health PEI sent written notices of the privacy breach to more than 4,900 individuals, including 3,660 individuals whose PHI was involved in the breach incident and 1,245 individuals whose PI was involved in the breach incident.

[35] Health PEI set up a toll-free number for affected individuals to call for more information and invited affected individuals to contact them by email if that was preferable. Health PEI also instituted a process where affected individuals could request a copy of their PHI/PI that was on the laptop when it was stolen. Health PEI reports that 36 individuals requested, and received, a copy of their PHI/PI through this process.

[36] On June 1, 2022, Health PEI's CEO circulated a memo to staff regarding the incident, Health PEI issued a news release to the general public, and Health PEI's CEO did interviews with local media. A follow-up memo to staff was circulated, reminding staff of privacy and security expectations relating to handling of PHI, use of laptops, and working remotely.

[37] Health PEI reported that a total of 69 affected individuals called the toll-free number and 16 affected individuals emailed Health PEI in relation to the breach. Three individuals contacted Health PEI to see if their PHI or PI was affected after seeing the media reports. The last contact through the toll-free number was on August 10, 2022, and the number was deactivated on October 13, 2022.

[38] I am satisfied that in the circumstances of this breach, Health PEI adequately met its notification obligations, both to our office and in notifying affected individuals. We did receive some comments early on in the notification process expressing concern about the time between Health PEI learning of the breach and when notification to affected individuals was made. However, I accept that Health PEI required time to conduct their investigation and determine what PHI/PI was on the laptop, consider whether there would be an adverse impact, and determine the identities of, and contact information for, the affected individuals. They also had to prepare and address more than 4,900 individual notification packages to be mailed to the affected individuals, which would have also taken a fair amount of time. I am satisfied that the notification of affected individuals was made at the first reasonable opportunity in the circumstances, and that Health PEI met the requirements of section 36 of the *HIA*.

(c) Health PEI's Investigation

[39] After being informed of the incident, Health PEI initiated an internal investigation and requested a police investigation. Although we are aware the police conducted an investigation, we are not aware of the details of the police investigation or if they attended the scene at the time the theft was discovered.

[40] Health PEI investigated the nature and scope of the privacy breach, factors and circumstances that may have contributed to the occurrence, conducted a review of technology and security requirements, and a review of existing Health PEI policies regarding technology, security and privacy. The investigation was initiated on April 5, 2022 as soon as the incident was reported, and Health PEI provided a written report of their investigation and findings to our office on January 12, 2023.

[41] Health PEI interviewed the Employee as part of its investigation, and reported the Employee was cooperative throughout the investigation and presented as very remorseful and greatly concerned about the incident. Health PEI reported their investigation revealed that the Employee had completed orientation at the time of hire, including basic privacy and confidentiality training, and had signed all standard confidentiality and acceptable-use-of-technology agreements. ITSS confirmed the Employee's password was strong, and the Employee indicated they had not shared their credentials with any other person.

[42] Health PEI reported that they have a reasonably high degree of confidence that they were able to identify all the files that were saved to the Employee's laptop, and the nature of the information contained within these files. The information had been extracted from Health PEI's clinical and administrative information systems and no full employee records or patient charts were saved to the laptop. The source databases were not affected, the records were not originals, and no records were permanently lost as a result of the theft of the laptop.

[43] The investigation revealed that there were 28 files saved to the laptop. Most of the files contained raw data related to analyzing patient flow and system utilization with no personally identifying information. Some files contained Provincial Health Numbers with nothing else to link them to an identifiable individual. Three files contained full names and additional information (PI or PHI) of patients or staff, and covered a limited period of time. The information included:

(a) A data extract from Emergency Department visits that occurred in September and October 2021, containing full patient names, Provincial Health Numbers, registration dates/times, reason for patients' visits, admission dates/times, discharge dates/times, and patients' family doctors;

(b) A data extract from February 2022 hospital admissions involving patients who were medically discharged but remained in hospital, containing full patient names, Provincial Health Numbers, facilities, facility units, and lengths of stay in hospital; and

(c) A data extract from the Health PEI payroll system involving staff who worked in long-term care facilities in January and February of 2022, containing full employee names, positions, locations of work, employment status, time reported (e.g. hours worked, overtime worked, sick time taken, vacation time taken, etc.), and total earnings per employee in each report period.

[44] Health PEI reported that no other identifiers, such as social insurance numbers or passport numbers, were saved on the laptop, nor was there any banking information saved on the laptop.

[45] Health PEI continued to investigate the circumstances surrounding the breach and attempted to identify what factors may have contributed to the breach, both individual to the Employee and systemically within Health PEI. Health PEI also worked to identify improvements that could be made to mitigate against a similar incident occurring again.

[46] Health PEI determined that the Employee's access to and use of the PHI and PI was legitimately required for their work, but the Employee had more PHI/PI than they needed for their job tasks, which was against Health PEI policy. Some factors they found that had contributed to this incident included: gaps in the orientation of new employees around explanations of privacy and Health PEI's privacy policies; some areas of Health PEI, including within the Employee's work unit, were engaging in information-handling practices that fell below expected standards and were not in line with Health PEI's privacy policies; and the Employee was working mostly from home, as was the protocol during the pandemic, and had Virtual Private Network ("VPN") login credentials to access Health PEI's information systems but opted to store identifiable information on the hard drive of their laptop instead of accessing it through VPN. The Employee indicated they had found the VPN access slow and did not have good functionality, so they saved raw data to the laptop. However, the Employee did not report the VPN issues to ITSS.

[47] Health PEI concluded that the Employee had not intentionally jeopardized the privacy of affected individuals and had taken appropriate steps to contain the breach immediately upon its discovery. Health PEI issued a new laptop to the Employee and permitted the Employee to complete their contract, with changes to their information handling practices being required, and supplemental education on adequate protection of PHI/PI. The Employee left Health PEI when their contract was completed. Health PEI reported that the Employee continued to cooperate with the investigation after their employment ended.

[48] I cannot say that I agree with Health PEI's conclusion that the Employee had not intentionally jeopardized the privacy of affected individuals. I accept that the Employee may not have set out with a specific intention to breach the privacy of the affected individuals. However, the Employee was aware of Health PEI's privacy policies and had signed the acceptable-use-of-technology agreements but decided anyway to engage in activities that were not in compliance with those requirements. The Employee acted

intentionally in making their decisions to do what they did, and a foreseeable risk of those intentional actions was jeopardizing the privacy of the affected individuals. Therefore, I would not agree that the Employee had not intentionally jeopardized the privacy of affected individuals.

[49] Health PEI continued to assess the risk of harm to the affected individuals throughout their investigation. Health PEI did not have the means to determine whether the information contained on the laptop was accessed by any third party, so decided to work on the assumption that access by a third party was possible.

[50] Police took a statement from the Employee and advised Health PEI that the Employee was cooperative with their investigation. However, they were not able to recover the laptop. Further, they were unable to identify a suspect and did not make any arrests as a result of their investigation, so closed their file after their investigation was completed. Police reported they had shared the laptop's serial number internally in case it was recovered during the course of other police activities.

[51] In or about mid-August 2022, the RCMP notified Health PEI that they had recovered a badly damaged laptop, and emailed photos to see if it might have been the stolen laptop. Health PEI forwarded the photos to ITSS for their review. However, the laptop was too badly damaged and lacking in specific identifiers to be able to confirm if it was the stolen laptop. ITSS requested physical access to the damaged laptop to allow further inspection and continued to explore whether it was possible to identify if the recovered laptop was the one that was stolen. ITSS reported it tried a number of different methods to attempt to identify if this was the stolen laptop, but as of the date of this report, ITSS had not been able to confirm whether the recovered laptop was the stolen laptop.

[52] I am satisfied that Health PEI conducted a thorough investigation of the circumstances of the breach.

(d) Remediation

[53] As a result of their investigation, Health PEI identified a number of factors that contributed to the privacy breach. The factors Health PEI identified included the following:

(a) the Employee had left the laptop in a vehicle overnight;
(b) the laptop was (potentially) unencrypted;
(c) the Employee saved PHI and PI to the laptop's hard drive rather than viewing it through VPN and saving only de-identified or non-identifying data to the laptop;
(d) the Employee had access to /used more PHI/PI than necessary for their duties;
(e) some potential gaps in the orientation of new hires around privacy, IT security requirements/expectations; and
(f) some information handling practices within the Employee's division that did not comply with Health PEI policies and procedures.

[54] Health PEI took various steps to address the factors they determined had led to the privacy breach, to mitigate against a similar breach happening again. These steps included:

(a) the Employee and all staff in the Employee's division received re-education on adequate protection of PHI and information handling practices;
(b) all Health PEI staff were given privacy and security reminders;
(c) all Health PEI staff ~~were given~~ [<u>are receiving]</u> cyber security training, in partnership with ITSS; [amended]
(d) Health PEI commenced a review and enhancement of its privacy training program, with a focus on more privacy content being included in the orientation package for new hires, and development of a training program for managers and supervisors on best practices for data analysis;
(e) Health PEI commenced implementing a data de-identification policy, with reviews being conducted regularly to ensure compliance;
(f) Health PEI reviewed and updated their Remote Work Policy, with specific references to ITSS security guidance regarding appropriate safeguards for technology in transit;
(g) Health PEI is enhancing their policy on privacy and protection of PHI, and will provide more clarity around expectations for protection of privacy, the "need to know" principle, and using the minimum amount of PHI necessary in all circumstances;

(h) Health PEI has requested or will request a review by ITSS of device security, including encryption, for all laptops and other mobile devices issued to Health PEI staff; and
(i) Health PEI will recommend to ITSS that they consider the use of remote tracking technology and/or remote wiping functionality for Government-issued laptops and other mobile devices issued to Health PEI staff.

[55] I would note that although the Employee was a contract employee whose contract was due to end shortly after this incident occurred, Health PEI provided education and training to the Employee around privacy and appropriate information handling practices before the Employee's contract ended. Health PEI also treated this incident as a systemic issue and took steps to attempt to mitigate against a similar incident throughout their organization, rather than treat it as isolated to the actions of one individual. I am satisfied that Health PEI responded appropriately to this breach and the steps taken to remediate the situation and protect against a similar occurrence in future were adequate.

OIPC Response

[56] The *Health Information Act* requires the Commissioner to notify an affected individual of the breach notification and give them a summary of the review procedures. Due to the significant number of affected individuals, Health PEI offered to include a notification letter from the OIPC with their notification letters sent to affected individuals.

[57] We determined it would be more beneficial for affected individuals to receive one package of information about the breach rather than multiple letters from different authorities. This also meant Health PEI did not have to share a large volume of personal information (contact information) with our office. Therefore, we accepted Health PEI's offer and, when Health PEI sent out their notification letters to affected individuals, their package included a letter from our office and a summary of our review procedures.

[58] We received numerous calls and emails in the first few weeks after the affected individuals were notified, and after Health PEI's media announcement about the breach.

The majority of the callers were asking about what PHI or PI of theirs was involved, and we redirected them to Health PEI as we did not receive a copy of the specific information involved in the breach. Anyone who asked about our response received an explanation of our process, was advised that we intended to post a summary on our website and invite their input before we concluded our investigation, and was encouraged to monitor our website for updates.

[59] We maintained an open dialogue with Health PEI throughout their investigation and response and received periodic updates from them until their investigation was completed and they provided us with their investigation report.

[60] We compiled an Investigation Summary, which we posted on our website in January 2023, summarizing the investigation Health PEI conducted into the privacy breach incident, causes, and steps taken by Health PEI to contain the breach and mitigate against similar incidents in the future. We invited affected individuals to review the report and contact our office with any feedback before we concluded our review. We provided individuals with an opportunity to ask our office any further questions arising from the information presented, comment on any concerns they had about the circumstances of the incident or investigation, or give us any further information they believed may be relevant for us to consider as part of our investigation.

[61] We left the Investigation Summary posted on our website for a period of approximately 8 weeks but did not receive any feedback from any affected individuals. We then proceeded to close our investigation.

VI. CONCLUSION

[62] I find that Health PEI did not meet its obligations under section 39 of the *HIA* and section 35 of the *FOIPP Act* to ensure adequate protection and security of PHI/PI in its custody and control. Although Health PEI did have policies in place to protect the PHI/PI in their custody and control and to guard against unauthorized access to, use or disclosure of

PHI/PH, there were some gaps in policies and practices at the time of the breach incident, and employees within the organization, specifically the Employee and others within the Employee's work unit of Health PEI, were not following Health PEI policies or standard practices for security of information at the time of the breach. While I recognize that Health PEI is a large organization that must rely on supervisory staff to ensure policies and standard practices are being followed, section 39 of the *HIA* requires that custodians ensure their agents, which includes employees, adhere to the safeguards and controls implemented to protect PHI. Therefore, it is the organization's responsibility as a whole to make sure adequate oversight is in place at all levels to protect against any weaknesses in the supervision of the day-to-day practices of its staff.

[63] Despite finding that Health PEI failed to meet its obligations to adequately safeguard PHI/PI in its custody and control, I find that Health PEI took this privacy breach seriously and acted expeditiously to contain the breach. I am satisfied that Health PEI acted appropriately in responding to this serious breach incident, took reasonable steps to contain the breach, and, subject to the recommendations I make below, has taken reasonable steps to mitigate against future breaches of a similar nature.

[64] I would like to thank Health PEI for being forthright with our office about the circumstances of the breach, for voluntarily reporting the PI breach, and for keeping our office updated throughout the progress of their investigation and response.

[65] I would also like to thank the affected individuals who contacted our office, for their patience and understanding as this matter unfolded. It is distressing to be notified of a privacy breach that affects you, and the process to address a breach can seem interminably long when it is your information that is involved. However, it is important for a custodian or public body to take the time required to undertake a thorough investigation to ensure the circumstances of the breach are fully understood, and so that the factors that contributed to the breach can be identified and remediated to mitigate against such a situation occurring in future.

VII. RECOMMENDATIONS

[66] As I am satisfied that Health PEI responded to the breach appropriately, I will make no order in this matter.

[67] However, I recommend that Health PEI ensure they have a more appropriate method of assessing whether there is a reasonable belief of adverse impact, to ensure they are meeting their legislative obligations regarding notification in the event of a privacy breach.

[68] I am also concerned that there appears to be an unknown number of laptops and other mobile devices being used within Health PEI that are not, or may not be, encrypted.

[69] Health PEI indicated it would request a review by ITSS of device security, including encryption, for all laptops and other mobile devices issued to Health PEI staff, and would recommend ITSS consider the use of remote tracking technology and/or remote wiping functionality for laptops and other mobile devices issued to Health PEI staff. However, I would go one step further.

[70] I recommend that Health PEI, in conjunction with ITSS, audit their inventory of laptops and other mobile devices, determine which ones contain encryption capabilities and which do not, and ensure those that have the capability to be encrypted are encrypted, and those that do not have encryption software have it installed and activated forthwith.

[71] I further recommend that Health PEI consult with ITSS and, if possible, disable the ability to save information to the hard drive of all laptops and other mobile devices issued to Health PEI staff.

[72] I also recommend that, if they have not done so already, Health PEI work with ITSS to ensure that all laptops and mobile devices assigned to Health PEI staff are capable of being remotely located and/or wiped by ITSS in the event they are lost, stolen, or

misplaced.

[73] While this investigation and review are specifically about Health PEI, in the current climate of mobile devices and remote work being the new normal, I would strongly encourage all public bodies to ensure that their laptops and other mobile devices are encrypted and have the capability to be remotely located and wiped, in the event of loss or theft, and that the ability to save information to the hard drives is disabled.

Denise N. Doiron
Information and Privacy Commissioner