IN THE MATTER OF AN INVESTIGATION BY THE INFORMATION AND PRIVACY COMMISSIONER OF PRINCE EDWARD ISLAND UNDER PART III OF THE *HEALTH INFORMATION ACT*, 1988, R.S.P.E.I., Cap H-1.41

INVESTIGATION SUMMARY
Case File Number BRH-22-040
January 19, 2023

PURPOSE

The purpose of this Investigation Summary is to give individuals affected by the breach an overview of the information Health PEI provided to the Office of the Information and Privacy Commissioner ("OIPC") about their privacy breach investigation involving a stolen laptop. We encourage affected individuals to tell us if they have any other questions, concerns or information they believe is relevant for us to consider in our own investigation.

FACTUAL BACKGROUND

[1] On or about April 5, 2022, Health PEI, a custodian under the *Health Information Act* and a public body under the *Freedom of Information and Protection of Privacy Act* 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 with them after work and left it in their parked vehicle overnight, located 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") contained in the paper notebook, but the files they had saved to the hard drive of the laptop likely contained both PI and PHI. A preliminary investigation found both PI and PHI were most likely saved to the laptop.

HEALTH PEI'S INITIAL RESPONSE

[4] 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. 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.

[5] Health PEI notified the Office of the Information and Privacy Commissioner ("OIPC") of the breach on April 6, 2022, and advised of the potential breach of both PHI and PI. Under the *Health Information Act*, except for limited exceptions, it is mandatory for a custodian to report a breach of privacy involving PHI to the OIPC. Under the *Freedom of Information and Protection of Privacy Act*, there is no similar mandatory reporting requirement for public bodies to report a breach involving PI. However, Health PEI voluntarily reported the breach of PI to the OIPC and included it in their investigation.

INVESTIGATION

[6] Both a police investigation and an internal Health PEI investigation were conducted as a result of the theft of the laptop. Both investigations have now been completed.

[7] Police took a statement from the Employee and advised Health PEI that the Employee was cooperative with the 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 shared the laptop's serial number internally, in case it was recovered during the course of other police activities.

[8] 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 has requested physical access to the damaged laptop to allow

further inspection and is continuing to explore whether it is possible to identify if the recovered laptop is the one that was stolen.

[9] 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 the OIPC on January 12, 2023.

[10] 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 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 on April 7, 2022, with a follow up report received from ITSS on April 29, 2022.

[11] As part of its investigation, Health PEI interviewed the Employee. Health PEI also reported the Employee was cooperative throughout the investigation, and presented as very remorseful and greatly concerned about the incident. The 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.

[12] 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 contained on 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.

[13] 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 only Provincial Health Numbers with no other direct identifiers

linking 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 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;
- 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, units, and lengths of stay in hospital; and
- 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 (eg. hours worked, overtime worked, sick time taken, vacation time taken, etc.), and total earnings per employee in each report period.

[14] No foundational identifiers which could be used to establish someone's identity, such as social insurance numbers or passport numbers were saved on the laptop, nor was there any banking information saved on the laptop.

[15] 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.

[16] Health PEI found that the employee's access to and use of the PHI and PI was legitimately required for their work, but that the policy of accessing and using the minimum amount of PHI required to serve the purpose of the access was not followed in all instances. Some factors they found that had contributed to this included: gaps in the orientation of new employees around explanations of privacy and Health PEI's privacy policies; general information practices within some areas of Health PEI were not in line with privacy expectations; 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. The Employee found that the VPN access was slow and did not have good functionality so saved raw data to the laptop. The Employee did not report the VPN issues to ITSS.

[17] Health PEI found 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. The Employee was issued a new laptop and permitted to complete their contract, with changes to their information handling practices in place, 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.

[18] Health PEI continued to assess the risk of harm to the affected individuals. Health PEI did not find evidence about whether the information contained on the laptop was accessed by any third party.

NOTIFICATION OF AFFECTED INDIVIDUALS

[19] Section 36 of the *Health Information Act* requires a custodian to 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.

[20] 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. 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.

[21] Although there was no evidence to suggest anyone had accessed the PHI/PI on the laptop, Health PEI assessed there being 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 assessed the risk of identity theft from the lost or stolen PHI and PI to be very low as the information contained on the laptop could not be used for the purposes of proving identity.

[22] However, 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 *Health Information Act* to notify both the affected individuals whose PHI was involved in the breach and the Commissioner.

[23] The *Freedom of Information and Protection of Privacy Act* does not have a similar provision requiring notification for lost or stolen PI. However, because Health PEI considered the PI to be sensitive information and assessed the potential for unauthorized access to and potential for adverse impacts to be the same as for the PHI, Health PEI decided to voluntarily notify individuals whose PI was involved in the breach, and voluntarily notified the Commissioner as well.

[24] Health PEI notified the OIPC of the breach on April 6, 2022 and provided periodic updates as the investigation progressed. In late May 2022, Health PEI sent written notices of the privacy breach to 3,660 individuals whose PHI was involved in the breach incident and to 1,245 individuals whose PI was involved in the breach incident. A total of 118 individuals whose PHI or PI was involved in the breach 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.

[25] Because 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, and 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.

[26] 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.

[27] Health PEI activated 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.

[28] 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.

REMEDIATION

[29] As a result of this breach investigation, Health PEI identified the following factors had contributed to the privacy breach:

- (potentially) laptop was not encrypted
- Employee left the laptop in a vehicle overnight
- 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 laptop
- Employee had access to/used more PHI than necessary
- some potential gaps in the orientation of new hires around privacy of PHI/PI, IT security requirements/expectations
- some information handling practices within the Employee's division did not meet the expected standards

[30] Health PEI has taken or is in the process of taking the following steps to address the factors that contributed to the privacy breach incident:

- Employee and all staff in Employee's division received re-education on adequate protection of PHI and information handling practices
- All Health PEI staff were given privacy and security reminders
- All Health PEI staff are receiving cyber security training, in partnership with ITSS
- Health PEI is reviewing and enhancing 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
- Health PEI is implementing a data de-identification policy, with reviews being conducted to ensure compliance
- Health PEI is reviewing and updating their Remote Work Policy, and will include specific references to ITSS security guidance regarding appropriate safeguards for technology in transit
- 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

- Health PEI will request a review by ITSS of device security, including encryption, for all mobile devices issued to Health PEI staff
- Health PEI will recommend to ITSS that they consider the use of remote tracking technology and/or remote wiping functionality for Government-issued mobile devices, including mobile devices issued to Health PEI staff

FEEDBACK

This summarizes the information provided to the OIPC by Health PEI about the investigation Health PEI conducted into the privacy breach incident, causes, steps taken by Health PEI to contain the breach and mitigate against similar incidents in future. Before the OIPC concludes its investigation and makes findings, affected individuals have an opportunity to review the information, ask the OIPC any further questions arising from the information presented, comment on any concerns they have about the circumstances of the incident or investigation, or give us any further information they believe may be relevant for us to consider as part of our investigation.

Affected individuals who have questions, comments, or further information they wish to provide to the OIPC, may do so in writing by either sending an email to InfoPrivacy@assembly.pe.ca or by regular mail to:

Office of the Information and Privacy Commissioner
P.O. Box 2000
149 Kent Street, Suite 301
Charlottetown, PE C1A 7N8

We ask that any affected individuals wishing to provide feedback to the OIPC please do so by March 10, 2023.