Department of Health and Social Services

PRIVACY BREACH (Stolen Laptop)

PUBLIC QUESTIONS AND ANSWERS

QUESTION: When was the laptop reported stolen?

RESPONSE: The laptop was stolen from a locked vehicle in the Ottawa area May 9, 2018. The theft was reported to the Ottawa police, the employees supervisor and the Department of Health and Social Services (HSS) Chief Health Privacy Officer the same day.

QUESTION: What type of information did the laptop contain?

RESPONSE: The laptop contains separate datasets for the purposes of doing statistical analysis to generate population-level findings. These datasets include the following types of personal health information: patient information including name, date of birth, community of residence, health care card numbers. Depending on the dataset, patient information also could include infectious disease and conditions, immunization status or laboratory test results.

QUESTION: What was the information on the laptop used for?

RESPONSE: The data on the laptop was collected under the *Public Health Act.* The laptop was used for population health monitoring and reporting. This includes analysis of data used to inform frontline delivery in relation to immunization coverage (influenza and HPV), and management of infectious diseases (including sexually transmitted infections, influenza, TB, invasive diseases, vancomycin resistant enterococcus (VRE), methicillin resistant staphylococcus aureus (MRSA), and *Clostridium difficile*, among others).

QUESTION: Was the laptop protected?

RESPONSE: Yes. The laptop used a strong password for login. The Government of the Northwest Territories' Technology Services Centre (TSC) uses the latest software to encrypt all TSC-supported devices. However, in this case, while the device was capable of encryption, the encryption process either failed or was missed and not detected by the TSC.

QUESTION: Why wasn't the data encrypted?

RESPONSE: As part of the internal investigation, HSS was advised by the Technology Services Centre (TSC) that this laptop was one of a very small number of new devices being piloted (approximately 16). The TSC uses the latest software to encrypt all TSC-supported devices. However in this case the encryption process either failed or was missed and not detected by the TSC.

QUESTION: Are there more pilot laptops used by Health and Social Services that aren't encrypted?

ANSWER: No**.**

QUESTION: Are there other HSS laptops, not part of the pilot group that aren't encrypted?

RESPONSE: The Technology Services Centre has a standard practice of encrypting all supported laptops and tablets before they are issued to staff. The TSC has confirmed that all TSC supported laptops and tablets used by HSS staff are encrypted; any devices that are showing as "inactive" i.e not connected to the network due to vacation, personal leave etc are being followed up by the by the TSC.

QUESTION: Why is the Department reporting the stolen laptop now?

RESPONSE: The Privacy Breach Policy requires a complete investigation to take place before notification can occur. The Chief Health Privacy Officer concluded her initial investigation June 18, 2018. The investigation concluded that a privacy breach

occurred. A privacy breach occurs when data is no longer in control by the custodian (employee).

QUESTION: What type of information did the laptop contain? Is there a risk of identity theft to NWT residents?

RESPONSE: The device contained health information, including names, dates of birth, health card numbers and communities of residence. Depending on the dataset, patient information also could include infectious disease and conditions, immunization status or laboratory test results. The health information was in datasets for the purposes of performing statistical analyses and did not contain any other personal information. NWT health care card is not a foundation document and is not used to confirm identity (e.g. for such documents and/or programs as Driver's License, General Identification Card (GIC), Passport, etc.). In the NWT, when an individual presents a health care card to receive insured services the registration/administration staff are required to confirm identity with additional questions and/or proof of identity. However, in some cases identity theft can occur with as little information as a name and date of birth, so there is a risk that information could be used for illegal purposes.

QUESTION: Do I need to replace my health care card?

RESPONSE: No. An NWT health care card is not a foundation document and is not used to confirm identity (e.g. for such documents and/or programs as Driver's License, GIC, Passport). In NWT, when an individual presents a health care card to receive insured services the registration/administration staff are required to confirm identity with additional questions and/or proof of identity.

QUESTION: What steps has the Department taken to prevent this from happening again?

RESPONSE: It is difficult to prevent theft from locked vehicles; however the Department has reminded staff to not leave laptops in vehicles, ensure strong passwords are always

used in portable devices. Work continues with the GNWTs Technology Services Centre to ensure all devices are encrypted.

QUESTION: Have the patients been informed?

RESPONSE: As a precaution we are notifying all NWT residents of the breach as the total number of client is unknown.

QUESTION: Has the Information and Privacy Commissioner been informed?

RESPONSE: Yes, the Information and Privacy Commissioner was informed June 26 2018. This notification occurred as soon as the investigation was completed.

QUESTION: Is the Department legally obligated to report this breach and advise affected patients?

RESPONSE: Department of Health and Social Services Privacy Breach Policy requires notification to affected individuals where possible. Additionally, real or suspected breaches of personal health information are subject to the *Health Information Act.*

QUESTION: Has the Police been informed?

RESPONSE: Yes. The Ottawa Police were informed on the same date the theft occurred.

QUESTION: Who can residents contact at the Department if they have additional questions or concerns?

RESPONSE: Residents can contact the HSS System Navigator at 1-855-846-9601 or by emailing hss_navigator@gov.nt.ca

QUESTION: What are the current policies for having personal data on portable devices?

RESPONSE: The Health Information Act and the *Electronically Stored and Transferred Information Policy* govern the handling of personal information by HSS employees. This Policy speaks to requirements including storage of portable devices, protection of stored information, the transfer of information and security of portable devices.

QUESTION: How are the policies enforced? Are there regular training opportunities or spot checks?

RESPONSE: With the enactment of the Health Information Act (HIA), comprehensive training has been provided to both health information custodians across the GNWT, including physicians, pharmacists and HSS employees. All HSS staff are required to have privacy training. Additional training courses are provided throughout the year.

QUESTION: What is the Department doing to ensure that policies and procedures are in place across the NWT?

RESPONSE: The Deputy Minister has sent a note to department staff and the Northwest Territories Health and Social Services Authority confirming expectations regarding the safe storage and handling of information on portable devices. Targeted training by the Chief Privacy Officer continues to be delivered for all staff who handle personal information.

QUESTION: Who is the employee and what if any disciplinary actions will they face?

RESPONSE: The Department won't speak to internal employee matters.