Ministère de la Santé et des Services sociaux

ATTEINTE À LA VIE PRIVÉE (ordinateur portatif volé)

QUESTIONS ET RÉPONSES

QUESTION À quel moment l'ordinateur portatif a-t-il été déclaré volé?

RÉPONSE L'ordinateur portatif a été volé dans un véhicule verrouillé, dans la région d'Ottawa, le 9 mai 2018. Le vol a été signalé à la police d'Ottawa, au superviseur des employés et à l'administrateur en chef de la protection des renseignements médicaux du ministère de la Santé et des Services sociaux (MSSS) le jour même.

QUESTION Quels types de renseignements l'ordinateur portatif contenait-il?

RÉPONSE L'ordinateur portatif contient différents ensembles de données aux fins d'analyses statistiques pour générer des résultats sur des populations. Ces données comprennent les types de renseignements médicaux personnels suivants : renseignements sur le patient, y compris le nom, la date de naissance, la collectivité de résidence et le numéro de carte d'assurance maladie. Selon l'ensemble de données, les renseignements sur les patients pourraient également inclure l'état d'infection par une maladie, l'état immunitaire ou des résultats de tests de laboratoire.

QUESTION À quelle fin les renseignements sur l'ordinateur portatif étaient-ils utilisés?

RÉPONSE Les données sur l'ordinateur portatif ont été recueillies en vertu de la *Loi sur sur la santé publique*. L'ordinateur portatif était utilisé à des fins de suivi et d'établissement de rapports sur l'état de santé de la population. Cela comprend l'analyse de données utilisées pour orienter la prestation de services de première ligne en matière de couverture vaccinale (grippe et VPH), ainsi que la gestion des maladies infectieuses (y compris les infections transmissibles sexuellement, l'influenza, la tuberculose, les maladies invasives, l'entérocoque résistant à la vancomycine [ERV], le Staphylococcus aureus résistant à la méthicilline [SARM], et le *Clostridium difficile*, entre autres).

QUESTION L'ordinateur portatif était-il protégé?

RÉPONSE Oui. L'ordinateur avait un mot de passe fort. Le Centre de services technologiques (CST) du gouvernement des Territoires du Nord-Ouest utilise une

technologie dernier cri pour chiffrer tous les appareils qu'il prend en charge. Cela dit, dans le cas présent, l'appareil était capable de chiffrement, mais le processus de chiffrement avait échoué, avait été manqué ou n'avait pas été détecté par le CST.

QUESTION Pourquoi les données n'étaient-elles pas chiffrées?

RÉPONSE Dans le cadre de l'enquête interne, le Centre de services technologiques (CST) du ministère de l'Infrastructure a informé le MSSS que cet ordinateur portatif faisait partie d'un très petit groupe de nouveaux appareils en cours de projet-pilote (environ 16). Le CST utilise une technologie dernier cri pour chiffrer tous les appareils qu'il prend en charge. Cela dit, dans le cas présent, l'appareil était capable de chiffrement, mais le processus de chiffrement avait échoué, avait été manqué ou n'avait pas été détecté par le CST.

QUESTION Existe-t-il d'autres ordinateurs portatifs pilotes utilisés par le ministère de la Santé et des Services sociaux qui ne sont pas chiffrés?

RÉPONSE Non.

QUESTION Y a-t-il d'autres ordinateurs portatifs du MSSS ne faisant pas partie du groupe pilote qui comportent des données qui ne sont pas chiffrées?

RÉPONSE Le Centre de services technologiques a pour norme de chiffrer tous les ordinateurs portatifs et les tablettes prises en charge avant de les remettre au personnel. Le CST a confirmé que tous les ordinateurs portatifs et les tablettes utilisés par le personnel du MSSS et pris en charge par le CST sont chiffrés; le CST ne peut effectuer le suivi des appareils dont le statut est « inactif », c.-à-d. non connecté au réseau parce qu'un employé est en vacances, en congé, etc.

QUESTION Pourquoi le Ministère signale-t-il le vol de l'ordinateur portatif maintenant?

RÉPONSE La politique sur les atteintes à la vie privée exige la tenue d'une enquête complète avant de pouvoir faire une déclaration. L'administrateur en chef de la protection des renseignements médicaux a conclu son enquête initiale le 18 juin 2018. Les résultats de l'enquête ont permis de conclure qu'il y avait eu atteintes à la vie privée. Une atteinte à la vie privée se produit lorsque des données ne sont plus contrôlées par le dépositaire (employé).

QUESTION Quels types de renseignements l'ordinateur portatif contenait-il? Les Ténois sont-ils confrontés à un risque d'usurpation d'identité?

RÉPONSE Il n'y a aucun risque pour les soins aux patients étant donné que l'ordinateur portatif ne contenait pas de dossiers médicaux. L'appareil contenait des renseignements médiaux, y compris des noms, des dates de naissance, des numéros de carte d'assurance maladie et des collectivités de résidence. Selon l'ensemble de données concerné, les renseignements sur les patients pourraient aussi inclure l'état d'infection par une maladie, l'état immunitaire ou des résultats de tests de laboratoire. Ces renseignements sur la santé avaient été recueillis à des fins d'analyse statistique et ne contenaient aucun autre renseignement personnel. Une carte d'assurance maladie des TNO n'est pas un document officiel et n'est pas utilisée pour confirmer une identité (p. ex., pour des documents ou des programmes comme le permis de conduire, la carte d'identité générale, le passeport, etc.). Aux TNO, le personnel administratif des services de santé est tenu de confirmer l'identité d'une personne qui présente une carte d'assurance maladie afin de recevoir des traitements avec des questions supplémentaires ou une preuve d'identité. Toutefois, un vol d'identité peut se produire dans certains cas même s'il y a peu de renseignements, par exemple un nom et une date de naissance, donc il existe un risque que les renseignements soient utilisés à des fins illégales.

QUESTION Dois-je remplacer ma carte d'assurance maladie?

RÉPONSE Non. Une carte d'assurance maladie des TNO n'est pas un document officiel et n'est pas utilisée pour confirmer une identité (p. ex., pour des documents ou programmes comme le permis de conduire, le passeport, la carte d'identité générale, etc.). Aux TNO, le personnel administratif des services de santé est tenu de confirmer l'identité d'une personne qui présente une carte d'assurance maladie afin de recevoir des traitements avec des questions supplémentaires ou une preuve d'identité.

QUESTION Quelles mesures le Ministère a-t-il prise pour empêcher que cela se reproduise?

RÉPONSE Il est difficile d'empêcher un vol dans un véhicule verrouillé; toutefois, le Ministère a rappelé aux employés de ne pas laisser d'ordinateurs portatifs dans les véhicules, et de s'assurer que le personnel utilise des mots de passe forts sur leurs appareils portatifs. Le Centre de services technologiques du GTNO continuera ses efforts afin de chiffrer tous les appareils.

QUESTION Les patients ont-ils été informés?

RÉPONSE Par mesure de précaution, nous avisons tous les résidents des TNO de cet incident étant donné que le nombre total de patients visés est inconnu.

QUESTION Est-ce que le Commissariat à l'information et à la protection de la vie privée a été informé?

RÉPONSE Oui, le Commissariat à l'information et à la protection de la vie privée en a été informé le 26 juin 2018. Cela s'est fait dès que l'enquête a été achevée.

QUESTION Le Ministère est-il légalement tenu de signaler cette atteinte et d'en informer les patients?

RÉPONSE La politique sur les atteintes à la vie privée du ministère de la Santé et des Services sociaux exige qu'une notification aux personnes touchées soit effectuée dans la mesure du possible. Par ailleurs, les atteintes réelles ou potentielles sur les renseignements médicaux personnels sont soumises à la *Loi sur les renseignements sur la santé*.

QUESTION La police a-t-elle été informée?

RÉPONSE Oui. La police d'Ottawa a été informée le jour du vol.

QUESTION Avec qui les résidents peuvent-ils communiquer au sein du Ministère s'ils ont des questions ou des préoccupations?

RÉPONSE Les résidents peuvent communiquer avec l'intervenant pivot du MSSS au 1-855-846-9601 ou à l'adresse hss_navigator@gov.nt.ca.

QUESTION Quelles sont les politiques actuelles sur les données personnelles détenues sur des appareils portatifs?

RÉPONSE La Loi sur les renseignements sur la santé et la politique sur le transfert et la conservation électroniques de l'information *(Electronically Stored and Transferred Information Policy)* régissent l'utilisation des renseignements personnels par les employés du MSSS. Cette politique énonce différentes exigences, par exemple l'entreposage des appareils portatifs, la protection des renseignements stockés, le transfert des renseignements et la sécurité des appareils portatifs.

QUESTION Comment les politiques sont-elles appliquées? Y a-t-il des possibilités de formation régulière ou des vérifications ponctuelles?

RÉPONSE Avec l'adoption de la *Loi sur les renseignements sur la santé*, une formation complète a été fournie aux dépositaires de renseignements sur la santé dans

l’ensemble du GTNO, y compris les médecins, les pharmaciens et les employés du MSSS. Tout le personnel du Ministère doit suivre une formation sur la protection de la vie privée. Des cours supplémentaires sont offerts toute l’année.

QUESTION Quelles mesures le Ministère prend-il pour s’assurer que les politiques et les procédures sont en place aux Territoires du Nord-Ouest?

RÉPONSE Le sous-ministre a envoyé un communiqué au personnel du Ministère et aux autorités du ministère de la Santé et des Services sociaux des Territoires du Nord-Ouest afin de confirmer les attentes concernant la sécurité de l’entreposage et de la manipulation des renseignements sur les appareils portatifs. Des formations ciblées sont offertes par l’administrateur en chef de la protection des renseignements à tous les employés qui traitent des renseignements personnels.

QUESTION Qui est l’employé qui s’est fait voler et, le cas échéant, quelles seront les mesures disciplinaires appliquées?

RÉPONSE Le Ministère ne fera aucun commentaire sur les questions liées à ses employés.