Politique de sécurité des données du GTIC

1. **Chiffrement et protection par mot de passe.** Les chercheurs acceptent que les données du GTIC soient stockées principalement sur des serveurs ou des ordinateurs de bureau protégés par mot de passe. Si elles sont stockées sur des appareils mobiles comme des ordinateurs portables ou des dispositifs de stockage à distance, les données du GTIC restent chiffrées lorsqu'elles sont au repos.

2. **Mesures de protection physiques.** Les chercheurs conviennent de garder les serveurs et les ordinateurs de bureau qui contiennent les données du GTIC dans des locaux privés qui peuvent être verrouillés et de verrouiller les portes si les chercheurs ne sont pas sur place pour surveiller l'utilisation des données du GTIC.

3. **Mesures de protection des données.** Les chercheurs conviennent d'utiliser un logiciel reconnu de protection contre les virus et les maliciels sur les ordinateurs de bureau, les ordinateurs portables et les dispositifs de stockage à distance (s'ils peuvent être dotés d'une telle protection) qui hébergent les données du GTIC.

4. **Mesures de protection organisationnelles.** Les chercheurs conviennent de mettre en œuvre et de respecter des pratiques organisationnelles qui améliorent la sécurité des données. L'accès aux données doit être limité au personnel autorisé. Le personnel autorisé demeure concrètement tenu de rendre des comptes aux dirigeants de l'établissement, ainsi qu'à l'établissement en soi.

5. **Destruction des données.** Les chercheurs conviennent de détruire les données du GTIC au moment établi dans le formulaire d'accès aux données ou un document équivalent. Les chercheurs conviennent d'utiliser une méthode vérifiable de destruction des données pour éliminer les données du GTIC. Les chercheurs conviennent de conserver des documents qui attestent la destruction des données du GTIC et de les mettre à la disposition du GTIC, sur demande.

6. **Formation.** Les chercheurs conviennent de faire en sorte que le chercheur principal, le personnel autorisé, les étudiants autorisés et d'autres personnes de leur établissement qui accèdent aux données du GTIC reçoivent une formation sur la sécurité et la confidentialité des données dont le niveau convient à leur rôle et à leurs responsabilités.

7. **Tenue de registres.** Les chercheurs conviennent de tenir des registres des personnes qui accèdent aux données du GTIC qui sont sous leur contrôle ou en leur possession. Les chercheurs conviennent de consigner l'intervalle de consultation et la portée des éléments de données accessibles à chaque utilisateur approuvé. Il faut aussi tenir des registres d'information sur la destruction des données.

8. **Surveillance et vérification.** Les registres qui concernent l'accès aux données du GTIC et la destruction de celles-ci doivent être stockés à l'aide de moyens technologiques qui permettent une vérification à l'interne et par les chercheurs externes. Une vérification de l'activité des utilisateurs doit être effectuée de façon périodique ou immédiatement en cas d'activité inhabituelle.

9. **Violations des données.** Les chercheurs doivent utiliser les mécanismes technologiques conformes aux normes du secteur qui conviennent pour protéger les données sur la santé contre toute violation des données et pour détecter de telles violations. Advenant une violation

confirmée ou soupçonnée des données du GTIC, le GTIC doit en être informé immédiatement et doit recevoir tous les renseignements connus sur la violation des données.

10. **Gestion des vulnérabilités.** Les chercheurs conviennent de prendre des mesures immédiates pour corriger toutes les vulnérabilités des logiciels et les autres vulnérabilités en matière de sécurité touchant les données du GTIC qui peuvent être découvertes. Les chercheurs conviennent de mettre en place des politiques aux fins de la correction rapide et continue des vulnérabilités et de les mettre en œuvre de manière efficace.

11. **Fournisseurs de services tiers.** Les chercheurs conviennent d'adopter toutes les mesures contractuelles et autres mesures nécessaires pour faire en sorte que les fournisseurs de services tiers respectent les modalités de la présente politique et soient concrètement tenus de rendre des comptes au GTIC.

12. **Stockage en nuage et infonuagique**. Les chercheurs conviennent d'adopter toutes les mesures contractuelles et autres mesures nécessaires pour faire en sorte que les fournisseurs de services de stockage en nuage et de services infonuagiques qui accèdent aux données du GTIC ou qui les utilisent rendent des comptes aux chercheurs et au GTIC. Ces mesures peuvent comprendre, sans s'y limiter, la remise de renseignements détaillés sur les aspects suivants (qui garantissent la possibilité de les vérifier) : les lieux de stockage des données du GTIC, les pratiques de conservation et de destruction des données, la séparation des données du GTIC et des autres données, la mise en œuvre des mesures de sécurité appropriées, la gestion de registres d'accès adéquats et l'adoption des procédures appropriées d'opposition à tout accès obligatoire aux données du GTIC.