Institut canadien d'information sur la santé

Politique sur la sécurité de l'information confidentielle et l'utilisation d'appareils mobiles et de supports d'information amovibles

But

La présente politique vise à garantir que

a. les renseignements confidentiels sont protégés et conservés uniquement sur des appareils et supports informatiques autorisés de l'ICIS dans des lieux autorisés;

b. les renseignements confidentiels conservés provisoirement sur les appareils mobiles et les supports d'information amovibles de l'ICIS sont en sécurité en cas de vol ou de perte et sont protégés contre l'utilisation, l'accès, la reproduction, la modification, la divulgation ou l'élimination non autorisés.

Portée

La présente politique vise tous les membres du personnel de l'ICIS.

La politique ne s'applique pas à l'information gravée sur des CD ou des DVD destinés à des clients externes. La communication de données à des clients externes est assujettie aux normes relatives aux méthodes de diffusion (document *Methods of Dissemination Standard*).

Institut canadien d'information sur la santé
Canadian Institute for Health Information

Définitions

« Appareils et supports informatiques de l'ICIS » désigne tout appareil ou support informatique sous la garde ou le contrôle de l'ICIS ou fourni par l'ICIS aux membres de son personnel, ce qui comprend notamment tout appareil mobile.

« Personnel de l'ICIS » désigne les employés à temps plein ou à temps partiel de l'ICIS, les employés contractuels, les personnes travaillant à l'ICIS en détachement, les étudiants, les travailleurs temporaires et certains conseillers ou fournisseurs externes qui ont besoin d'accéder aux données ou aux systèmes d'information de l'ICIS et y sont autorisés, conformément à la Politique d'utilisation acceptable des systèmes d'information de l'ICIS.

« Renseignements confidentiels », pour les besoins de la présente politique, englobe les renseignements personnels sur la santé, les renseignements personnels sur les travailleurs de la santé, les données dépersonnalisées et l'information technique.

« Renseignements personnels sur la santé » signifie des renseignements sur la santé d'une personne qui permettent d'identifier cette personne, ou qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne, ou qui peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient la personne.

« Renseignements personnels des travailleurs de la santé » désigne les renseignements au sujet d'un dispensateur de services de santé qui permettent d'identifier cette personne, qui peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne, ou qui peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient la personne.

« Données dépersonnalisées » désigne les renseignements personnels sur la santé ou les renseignements personnels sur la main-d'œuvre de la santé qui ont été modifiés au moyen de processus de dépersonnalisation appropriés de sorte que l'identité de la personne ne peut être déterminée selon une méthode raisonnablement prévisible.

« Appareil mobile » signifie tout appareil électronique qui offre une connectivité mobile aux réseaux de l'ICIS, ce qui comprend entre autres les téléphones intelligents, les tablettes et les ordinateurs portables.

« Gestion des risques liés au respect de la vie privée et à la sécurité » désigne un processus officiel et reproductible qui vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leurs éventuelles incidences.

« Support d'information amovible » désigne tout appareil amovible permettant d'emmagasiner de l'information, ce qui comprend entre autres les CD, les DVD et les clés USB.

« Information technique » signifie l’information portant sur les réseaux et les serveurs et dans les applications ou les environnements informatiques de l’ICIS. L’information technique comprend entre autres

- les fichiers journaux;
- l’information sur la topologie de réseau;
- les systèmes d’exploitation, les logiciels et le matériel informatiques, ainsi que leurs différentes versions;
- les technologies de développement des applications;
- l’information sur les mécanismes de sécurité de l’ICIS relativement au matériel et aux logiciels informatiques de l’ICIS;
- le code d’application;
- les fichiers de configuration du système.

Politique

Le personnel de l’ICIS doit accomplir son travail soit dans les locaux de l’ICIS, soit via ses réseaux sécurisés, au moyen des appareils et supports informatiques fournis par l’ICIS, dans le respect des politiques, procédures, normes et directives de l’ICIS visant le respect de la vie privée et la sécurité, sauf circonstances exceptionnelles, comme décrit plus bas.

Plus particulièrement :

Les renseignements personnels sur la santé

- ne doivent pas être transportés hors des locaux de l’ICIS en format papier;
- ne doivent pas être envoyés par courriel à l’interne ni à l’externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées;
- ne doivent être stockés dans aucun appareil mobile ou support d’information amovible, sauf dans certaines circonstances particulières et exceptionnelles, sous réserve d’une évaluation des risques liés au respect de la vie privée et à la sécurité et avec l’approbation préalable du vice-président compétent.

Les renseignements personnels sur les travailleurs de la santé

- ne doivent pas être transportés hors des locaux de l'ICIS en format papier;
- ne doivent pas être envoyés par courriel à l'interne ni à l'externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées;
- ne doivent être stockés dans aucun appareil mobile ou support d'information amovible, sauf dans certaines circonstances particulières et exceptionnelles, sous réserve d'une évaluation des risques liés au respect de la vie privée et à la sécurité et avec l'approbation préalable du vice-président compétent.

Les données dépersonnalisées

- ne doivent pas être transportées hors des locaux de l'ICIS en format papier;
- ne doivent pas être envoyées par courriel à l'interne ni à l'externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées;
- ne doivent être stockées dans aucun appareil mobile ou support d'information amovible, sauf dans certaines circonstances particulières et exceptionnelles, sous réserve d'une évaluation des risques liés au respect de la vie privée et à la sécurité et avec l'approbation préalable du vice-président compétent.

L'information technique

- ne doit pas être transportée hors des locaux de l'ICIS en format papier;
- peut être envoyée par courriel à l'interne seulement;
- ne doit être stockée dans aucun appareil mobile ni support d'information amovible, à moins que cet appareil ou support ne soit chiffré conformément aux normes actuelles de chiffrement de l'ICIS.

Il est interdit au personnel de l'ICIS de conserver des renseignements confidentiels sur un appareil mobile ou un support informatique amovible si d'autres renseignements (p. ex. des données dépersonnalisées ou agrégées) serviront aux mêmes fins. Les conditions suivantes s'appliquent lors de l'utilisation approuvée au préalable, comme décrit plus haut, d'appareils mobiles ou de supports informatiques amovibles :

1. Seuls les renseignements confidentiels nécessaires aux fins pour lesquelles ils seront utilisés peuvent être conservés provisoirement sur des appareils mobiles ou des supports informatiques amovibles.
2. Une fois les renseignements confidentiels utilisés aux fins prévues exigeant leur conservation provisoire sur des appareils mobiles ou des supports d'information amovibles, ils doivent être déplacés ou détruits, le cas échéant, dans un délai de 5 jours.

3. Les renseignements confidentiels conservés provisoirement sur des appareils mobiles ou des supports d'information amovibles seront
   a. enregistrés dans un appareil fourni par l'ICIS;
   b. dépersonnalisés dans toute la mesure du possible;
   c. chiffrés et protégés par un mot de passe conformément aux normes actuelles de chiffrement et de protection par mot de passe de l'ICIS (voir les documents *File Encryption Procedures* et *User Name and Password Standard* de l'ICIS, en anglais seulement). Tout dispositif mobile doit être protégé par un mot de passe.

Conformité

Le *Code de conduite de l'ICIS* définit les comportements éthiques et professionnels au chapitre des relations, des renseignements, y compris des renseignements personnels sur la santé, et du milieu de travail. Les employés sont tenus de respecter le contenu du code ainsi que l'ensemble des politiques, des procédures et des protocoles de l'ICIS. La conformité au Programme de respect de la vie privée et de sécurité de l'ICIS fait l'objet d'un contrôle, et les cas de non-conformité sont traités conformément au *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS. Les contraventions au code, y compris les contraventions aux politiques, aux procédures et aux protocoles de respect de la vie privée et de sécurité sont référées aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

Pour de plus amples renseignements :

securite@icis.ca

vieprivee@icis.ca