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 sauvegardée sur des supports amovibles destinés à des clients externes. La communication de données à des clients externes est assujettie à la norme relative au transfert sécuritaire de l'information (*Secure Information Transfer Standard* — en anglais seulement).

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 sur l'utilisation acceptable des systèmes d'information de l'ICIS (*Acceptable Use Policy* — en anglais seulement).

Renseignements confidentiels, pour les besoins de la présente politique, englobe les renseignements de nature très délicate qui doivent être protégés durant tout leur cycle de vie contre la perte ou le vol et contre l'accès, la divulgation, la reproduction, l'utilisation et la modification non autorisés afin que leur confidentialité, leur intégrité et leur disponibilité soient assurées. Les renseignements confidentiels comprennent entre autres les renseignements personnels sur la santé, les renseignements personnels, les renseignements personnels sur les travailleurs de la santé, les données dépersonnalisées et l'information technique.

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.

Renseignements personnels sur les 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.

Appareil mobile désigne 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.

Renseignements personnels sur la santé désigne les renseignements sur la santé d'une personne 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.

Renseignements personnels désigne tout renseignement factuel ou subjectif, quel que soit son format, qui peut être utilisé, seul ou en combinaison avec d’autres renseignements, pour identifier une personne, ce qui comprend les photographies et les vidéos. Les renseignements personnels excluent les renseignements relatifs au poste ou aux fonctions d’une personne (p. ex. son poste ou son titre, l’adresse de l’entreprise, et son numéro de téléphone ou son adresse courriel au travail).

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 désigne l’information portant sur les réseaux, les serveurs, les applications ou les environnements informatiques de l’ICIS. L’information technique comprend entre autres

- les technologies utilisées à l’ICIS;
- les fichiers journaux et les fichiers de vidage;
- les topologies et les schémas de réseau et d’applications;
- les systèmes d’exploitation, les logiciels et le matériel informatiques, ainsi que leurs différentes versions;
- les technologies et outils de développement des applications;
- l’information sur les mécanismes de contrôle de la sécurité de l’information de l’ICIS;
- le code d’application;
- les fichiers de configuration du système;
- l’information sur les modèles de données et le schéma des bases de données;
- les résultats des vérifications de la sécurité de l’information visant à évaluer les systèmes de traitement de l’information de l’ICIS.

Politique

1.0 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 :

1.1 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, ni à l'interne ni à l'externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées, conformément à la norme relative au transfert sécuritaire de l'information;
- ne doivent être stockés dans aucun appareil mobile ni support d'information amovible;
- ne doivent pas être accessibles à partir du réseau privé virtuel (RPV ou VPN) de l'ICIS à l'extérieur du Canada.

1.2 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, ni à l'interne ni à l'externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées, conformément à la norme relative au transfert sécuritaire de l'information;
- ne doivent être stockés dans aucun appareil mobile ni support d'information amovible;
- ne doivent pas être accessibles à partir du réseau privé virtuel (RPV ou VPN) de l'ICIS à l'extérieur du Canada.

1.3 Les données dépersonnalisées

- ne doivent pas être transportées hors des locaux de l'ICIS en format papier;
- ne doivent pas être envoyées par courriel, ni à l'interne ni à l'externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées, conformément à la norme relative au transfert sécuritaire de l'information;
- ne doivent être stockées dans aucun appareil mobile ni support d'information amovible;
- ne doivent pas être accessibles à partir du réseau privé virtuel (RPV ou VPN) de l'ICIS à l'extérieur du Canada.

1.4 L’information technique

- ne doit pas être transportée hors des locaux de l’ICIS en format papier;
- ne doit pas être envoyée par courriel à l’externe, sauf avec autorisation et dans le respect des mesures de sécurité appropriées, conformément à la norme de divulgation de l’information technique à une tierce partie (*Third-Party Technical Information Disclosure Standard* — en anglais seulement);
- 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.

2.0 **Conditions ou restrictions relatives au stockage de renseignements personnels sur la santé sur un appareil mobile**

- Sans objet; l’ICIS interdit de conserver sur des appareils mobiles des renseignements personnels sur la santé, des renseignements personnels sur les travailleurs de la santé et des données dépersonnalisées.

3.0 **Accès à distance**

Le personnel de l’ICIS peut travailler à distance sur le réseau privé virtuel (RPV ou VPN) de l’ICIS à l’aide d’ordinateurs portatifs chiffrés fournis par l’ICIS. Il lui est interdit d’accéder à distance à des renseignements personnels sur la santé si d’autres renseignements (p. ex. des données dépersonnalisées ou agrégées) peuvent suffire pour parvenir aux fins définies. Il lui est aussi interdit d’accéder à distance à plus de renseignements personnels sur la santé que raisonnablement nécessaire pour parvenir aux fins définies.

Seuls les appareils autorisés appartenant à l’ICIS peuvent se connecter aux réseaux de l’ICIS via le RPV. Le personnel de l’ICIS doit respecter les conditions et les restrictions énumérées dans la politique sur l’utilisation acceptable des systèmes d’information de l’ICIS (*Acceptable Use Policy* — en anglais seulement), dont les suivantes :

- L’utilisateur doit protéger la sécurité physique de l’appareil.
- L’appareil ne peut être utilisé que pour accomplir le travail relatif à l’ICIS et ne peut pas être utilisé par une autre personne que l’utilisateur autorisé.
- Le stockage de données sur les ordinateurs portatifs et de bureau fournis par l’ICIS est interdit.

En plus des mesures de sécurité de l’information mises en place sur les appareils internes, le chiffrement complet du disque est utilisé sur tous les ordinateurs portatifs et de bureau capables de se connecter aux réseaux de l’ICIS via le RPV.

Le processus d'approbation pour l'accès aux Renseignements personnels sur la santé, que ce soit via le RPV ou à l'aide d'appareils internes, est décrit à l'article 10 des procédures et politiques de respect de la vie privée de l'ICIS.

Respect, vérification et application

Le Code de conduite de l'ICIS (en anglais seulement) 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. Le personnel est tenu de se conformer au code ainsi qu'aux politiques, procédures et protocoles de l'ICIS. La conformité est encadrée par le programme de vérification du respect de la vie privée et le programme de vérification de la sécurité de l'information de l'ICIS. Les contraventions au code sont référées aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

Avis de violation

Les cas de non-conformité aux politiques en matière de respect de la vie privée et de sécurité 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, en vertu duquel le personnel doit signaler tout incident ou toute violation à incident@icis.ca.

Pour de plus amples renseignements :

securite@icis.ca

vieprivee@icis.ca

Comment citer ce document :
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*. Ottawa, ON : ICIS; 2023.