

Fiche d'information

L'utilisation d'appareils mobiles et de technologies de l'information au travail

Les appareils mobiles offrent différentes fonctions, dont les technologies de l'information (TI) – par exemple, les messages textes, les courriels, les images et les applications. Vous trouverez dans le présent document, qui ne remplace d'aucune façon les lois applicables ou les politiques de l'employeur, des informations factuelles sur l'utilisation des appareils mobiles et des TI au travail et les répercussions de cette utilisation sur la profession infirmière.

Avant d'utiliser l'une ou l'autre de ces technologies au travail, l'infirmière immatriculée (II) ou l'infirmière praticienne (IP) doit se poser la question suivante : existe-t-il des politiques qui autorisent ou régissent l'utilisation de telles technologies au travail? Si la réponse est non, les II et les IP devraient alors en réclamer.

Pour éviter de s'exposer à d'éventuelles conséquences fâcheuses sur le plan personnel ou professionnel, il faut bien comprendre les risques posés par l'utilisation des appareils mobiles et des TI. Voici quelques éléments clés à prendre en considération lors de l'utilisation d'appareils mobiles ou de TI au travail.

Atteinte à la vie privée

Les II et les IP ont l'obligation professionnelle et légale de protéger les renseignements personnels sur la santé (RPS) des clients. Pour ce faire, des mots de passe robustes et le chiffrement sont souvent exigés comme mesures de protection des RPS communiqués électroniquement au moyen d'appareils mobiles. En règle générale, les employeurs ont en place des politiques à l'appui de ce genre de mesures de protection (Société de protection des infirmières et infirmiers du Canada [SPIIC], 2013).

Intégration dans le milieu de travail

Il est maintenant courant de voir dans le secteur de la santé des programmes qui autorisent ou même encouragent les employés à apporter leur propre appareil mobile au travail. Ces employeurs ont généralement établi des politiques, des protocoles et des systèmes pour justement permettre aux professionnels de la santé d'interagir en toute sécurité avec leurs collègues et d'accéder aux dossiers des clients au moyen de leur appareil sans fil (SPIIC, 2013).

Gestion des attentes

En plus des préoccupations que soulèvent ces communications pour la protection de la vie privée et la sécurité, les II et les IP doivent également gérer les attentes des clients quant aux fins permises pour ces communications, aux délais de réponse aux requêtes et aux mesures à prendre si l'II ou l'IP n'est pas disponible. Des limites et des délais de réponse raisonnables peuvent alors être clairement communiqués aux clients (SPIIC, 2013).

Prévention des infections

L'étude de Kanayama *et al.* (2017) a montré la présence du *Staphylococcus aureus* résistant à la méthicilline (SARM) et d'autres formes de bactéries sur les appareils mobiles ainsi que sur les paumes et les doigts du personnel infirmier. Pour cette raison, le lavage des mains doit être répété après l'utilisation d'un appareil mobile et avant tout contact avec les clients.

D'autres renseignements importants que doivent considérer les II et les IP

Les considérations suivantes ne constituent pas une liste exhaustive – les II et les IP doivent toujours se référer aux mesures législatives et aux politiques de l'employeur. De plus, les II et les IP à leur compte doivent avoir des politiques qui portent sur l'utilisation des appareils mobiles et des TI au travail. Veuillez noter que l'AIINB n'appuie pas ni n'encourage l'utilisation des appareils mobiles ou de toute TI.

Technologie de l'information	Aspect important à considérer
Messages textes	- Vérifiez les politiques de l'employeur pour déterminer si la transmission d'information par message texte est permise. - Si elle est permise, déterminez le type de contenu qui peut être transmis par message texte. - Renseignez-vous sur les types d'appareil mobile permis au travail, c.-à.-d. appareil mobile personnel ou appareil mobile fourni par l'employeur. - Avant d'envoyer un texte, faites preuve de prudence pour assurer la sécurité du client et la confidentialité de ses renseignements. - Faites très attention à l'auto-correcteur et aux fautes de frappe : les erreurs peuvent parfois entraîner de graves préjudices. - Exigences de la tenue de dossiers : consultez les Normes pour la tenue de dossiers et les politiques de l'employeur.
Courriels	- Connaissiez et suivez les politiques de l'employeur pour les courriels. - Envisagez d'obtenir le consentement écrit du client avant de lui transmettre des RPS par courriel, ou consignez au dossier le consentement verbal du client. - Utilisez le chiffrement pour l'envoi de courriels à des destinataires externes. - Confirmez l'adresse de courriel du destinataire avant de lui transmettre des RPS. - N'échangez jamais de RPS identifiables avec un client en utilisant votre adresse de courriel personnelle.
Photos	- L'employeur a-t-il des politiques claires sur l'utilisation des appareils mobiles pour prendre des photos de clients? - Évitez d'utiliser votre appareil mobile personnel et, dans la mesure du possible, utilisez celui fourni par l'employeur en raison du risque élevé. - Le client doit consentir au préalable à la prise de toute photo. - Le consentement doit être consigné au dossier. - La photo fait partie du dossier de santé et doit être supprimée de l'appareil mobile immédiatement après son utilisation. - PAUSE – demandez-vous : EST-CE VRAIMENT NÉCESSAIRE? Y a-t-il une autre option?

Applications liées aux soins de santé	- Utilisez uniquement des applications qui proviennent de sources fiables, qui sont mises à jour fréquemment et qui sont approuvées par l'employeur, s'il y a lieu. - Assurez-vous d'avoir une formation et une connaissance suffisantes pour comprendre comment utiliser l'application. - Examinez et réglez les paramètres de protection de la vie privée sur les applications et les appareils mobiles. - Évitez d'avoir recours à des applications pour effectuer une tâche que, sinon, vous ne pourriez pas effectuer par vous-même. - N'oubliez pas que LES APPLICATIONS NE REMPLACENT JAMAIS LE JUGEMENT PROFESSIONNEL. - Faites des mises à jour fréquentes des applications pour vous assurer qu'elles existent toujours. - Évitez de recommander des applications aux clients à moins que vous ayez pleinement confiance dans l'application et, s'il y a lieu, que l'application a reçu l'aval de l'employeur.
---------------------------------------	---

Information tirée du webinaire de la SPIIC sur les médias sociaux et la technologie qui a eu lieu le 13 février 2019.

Ressources

[Accès et protection de la vie privée](#) (GNB)

[Code de conduite pour les infirmières immatriculées et les infirmières praticiennes](#) - Vie privée et confidentialité (5.4)

[Fiche d'information : Le caractère confidentiel des renseignements personnels sur la santé](#) (AIIC)

[Risques juridiques liés à l'utilisation du courrier électronique – Première partie : Préoccupations relatives à la protection des renseignements personnels](#) (SPIIC)

[Risques juridiques liés à l'utilisation du courrier électronique – Deuxième partie : Considérations d'ordre pratique](#) (SPIIC)

[Legal Case Study: Distraction by Cell Phone](#) (SPIIC) (disponible en anglais seulement)

[Appareils mobiles au travail](#) (SPIIC)

[Social Media In Professional Practice: The Courts' Perspective Webinar - Resources](#) (SPIIC) (disponible en anglais seulement)

[Applis mobiles en santé](#) (SPIIC)

Références

Kanayama, A.K., Takahashi, H., Yoshizawa, S., Tateda, K., Kaneko, A., & Kobayashi, I. (2017). Staphylococcus Aureus Surface Contamination of Mobile Phones and Presence of Genetically Identical Strains on the Hands of Nursing Personnel. *American Journal of Infection Control*, 45, 929-931. <http://dx.doi.org/10.1016/j.ajic.2017.02.011>

Société de protection des infirmières et infirmiers du Canada. (2013). Mobile Devices in the Workplace. *infoLAW*, 21(1), 1-2.