Document d'orientation : La protection de la vie privée et travail à domicile

Loi sur le droit à l'information et la protection de la vie privée
Loi sur l'accès et la protection en matière de renseignements personnels sur la santé

Le but de ce document d'orientation est de fournir des conseils aux organismes publics en vertu de la *Loi sur le droit à l'information et la protection de la vie privée* et aux dépositaires de soins de santé en vertu de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*, ainsi qu'à leurs employés, pour s'assurer que les renseignements personnels et les renseignements personnels sur la santé sont protégées de manière appropriée à tout moment lorsque vous travaillez hors site ou à domicile.

À la lumière de la pandémie de COVID-19, de nombreux organismes publics et dépositaires de soins de santé ont considérablement modifié leurs opérations quotidiennes et de nombreux employés travaillent désormais à domicile. Ce document d'orientation définit les mesures que les employeurs et les employés peuvent prendre pour protéger les renseignements personnels et/ou les renseignements personnels sur la santé lorsque les employés doivent ou doivent travailler à l'extérieur ou à domicile.

Principes généraux

Malgré le changement important dans la situation de travail de nombreux employés récemment, les obligations relatives au traitement des renseignements personnels et des renseignements personnels sur la santé se poursuivent à tout moment.

Les employés ne peuvent collecter, utiliser et/ou divulguer que des renseignements personnels ou des renseignements personnels sur la santé, conformément à la loi.

Les renseignements personnels ou les renseignements personnels sur la santé impliqués dans une tâche particulière devraient être limités au minimum nécessaire pour atteindre l'objectif et ne devraient être partagés ou rendus accessibles qu'à ceux qui ont besoin de les connaître dans le cadre de leurs fonctions professionnelles.

Étapes pour les employeurs

- Assurez-vous que vous disposez de politiques, de pratiques et de lignes directrices appropriées en matière de protection des renseignements personnels et/ou des renseignements personnels sur la santé, y compris des directives sur la conservation et les processus d'élimination sécuritaire, et que les employés les connaissent et y ont facilement accès.
- Assurez-vous que les employés n'ont accès qu'aux renseignements personnels et/ou aux renseignements personnels sur la santé dont ils ont besoin pour accomplir leurs tâches professionnelles.
- Assurez-vous que les employés sont informés des applications, des plates-formes et des systèmes qui ont été approuvés pour le traitement des renseignements personnels et/ou des renseignements personnels sur la santé, y compris pour les réunions virtuelles et les vidéoconférences en ligne.

- Assurez-vous que les appareils mobiles utilisés par les employés dans le traitement des renseignements personnels et/ou des renseignements personnels sur la santé sont aussi sécurisés que possible
    - Installez la protection par mot de passe et le cryptage sur les appareils mobiles.
    - Envisagez de mettre en œuvre un suivi à distance et un effacement à distance des informations sur les appareils mobiles, en cas de perte ou de vol.
    - Envisagez d'autoriser l'accès à distance aux renseignements personnels ou aux renseignements personnels sur la santé via des réseaux privés virtuels et des serveurs sécurisés, plutôt que de laisser les employés stocker ce type d'informations à distance sur des appareils mobiles.
- Mettre en œuvre un processus de déconnexion pour les appareils mobiles et les dossiers papier pour garder une trace des employés qui ont ces articles.
- Assurez-vous que tous les employés sont informés et savent quoi faire en cas de violation de la vie privée ou de la sécurité, ainsi que les personnes à contacter pour obtenir de l'aide ou pour signaler une violation potentielle ou réelle.

Étapes pour les employés

- Consultez et suivez les politiques, les pratiques et les directives de votre employeur concernant le traitement des renseignements personnels et/ou des renseignements personnels sur la santé.
- N'utilisez que des appareils mobiles, des comptes, des plates-formes et/ou des réseaux fournis ou approuvés par votre employeur à des fins professionnelles.
    - Consultez votre employeur au sujet de l'utilisation d'appareils personnels lorsque vous travaillez à domicile.
- Dossiers papier sécurisés pendant le transport et le stockage à domicile:
    - Ne laissez jamais d'appareils mobiles ou de documents papier sans surveillance, y compris dans votre véhicule, afin de minimiser le risque d'accès non autorisé, de perte ou de vol.
- Lors de la configuration de votre espace de travail à la maison:
    - Choisissez un espace avec autant d'intimité que possible.
    - Assurez-vous que les autres ne peuvent pas voir ou accéder autrement aux renseignements personnels ou aux renseignements personnels sur la santé qui se retrouvent sur les dossiers papier ou vos appareils de travail.
    - Assurez-vous que les autres ne peuvent pas entendre les conversations dans lesquelles des renseignements personnels ou des renseignements personnels sur la santé sont discutés.
    - Utilisez uniquement des moyens approuvés par votre employeur pour partager et stocker des renseignements personnels et des renseignements personnels sur la santé:
        - Évitez d'utiliser des plateformes, des applications ou des réseaux non approuvés lors de la manipulation de renseignements personnels ou de renseignements personnels sur la santé, telles que des comptes de messagerie personnels.
    - Ne stockez pas de renseignements personnels ou de renseignements personnels sur la santé sur des appareils qui ne sont pas protégés par mot de passe et/ou cryptés.
    - Assurez-vous que les appareils mobiles sont verrouillés ou éteints lorsqu'ils ne sont pas utilisés.

  - Assurez-vous que les appareils mobiles et les dossiers papier sont stockés en toute sécurité lorsqu'ils ne sont pas utilisés, comme dans un classeur verrouillé ou dans une zone désignée à laquelle seul l'employé peut accéder.
  - Ne permettez pas à d'autres d'utiliser des appareils mobiles utilisés à des fins professionnelles.
  - Ne partagez pas les mots de passe avec les appareils mobiles utilisés à des fins professionnelles.
- Méfiez-vous des tentatives de phishing ou des activités frauduleuses potentielles qui pourraient tenter d'accéder à votre mot de passe.
  - Ne cliquez pas sur des liens ou des pièces jointes provenant de sources non fiables, car ils peuvent contenir des virus ou des logiciels malveillants.
  - Avant de répondre ou de prendre des mesures en réponse à une communication exigeant une action immédiate, vérifiez auprès de votre employeur ou du support informatique pour déterminer si elle est légitime.
- Si vous constatez une violation potentielle ou réelle des renseignements personnels ou des renseignements personnels sur la santé, informez immédiatement la personne appropriée de votre employeur afin que des mesures puissent être prises pour remédier à la situation et minimiser l'impact potentiel de la violation.

ACCESS AND PRIVACY DIVISION
DIVISION DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DE LA VIE PRIVÉE
230-65 rue Regent St., Fredericton, NB E3B 7H8
☏ 506.453.5965/877.755.2811
🖷 506.453.5963
aip-aivp@gnb.ca
www.ombudnb-aip-aivp.ca