Audit d'Internet

C'est une évaluation périodique basée sur des critères définis vérifiant l'application des normes en vigueur.

Exemple : Tous les utilisateurs ayant un accès Internet sont susceptibles de se faire auditer sur les sites Internet auxquels ils accèdent ainsi que le temps qu'ils y passent, afin de vérifier si l'usage qu'ils en font est adéquat (usage professionnel ou cyberflânage ?)

Il est interdit d'installer des bornes sans fil sans l'approbation du Responsable de la sécurité de l'information de la Direction des ressources informationnelles.

Saviez-vous que nous savions ?

L'usage d'Internet doit **demeurer professionnel** en tout temps; n'oubliez pas que la Sécurité de l'information du CISSS de Chaudière-Appalaches surveille tous les utilisateurs dans leurs habitudes de navigation.

Pornographie = TOLÉRANCE ZÉRO

Soyez responsables et naviguez en toute sécurité!

Appareils de télécommunication sans fil

« Les appareils sans fil » désignent tous les types d'appareils électroniques portatifs pouvant potentiellement se connecter aux réseaux sans fil du CISSS de Chaudière-Appalaches.

De plus, **il est interdit de photographier des données personnelles et/ou confidentielles**, ainsi qu'un usager sans le consentement de ce dernier, et ce, même dans un cadre d'enseignement, et de transférer ces photos à qui que ce soit par courriel ou texto.

Exemple : Un étudiant photographiant la plaie d'un patient dans le but de l'utiliser pour ses travaux.

Il est interdit de contourner les systèmes mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs.

Qu'est-ce que le DIC?

- **Disponibilité :** Propriété des données d'être accessibles et utilisables en temps voulu.
- **Intégrité :** Propriété d'une information de n'être ni modifiée, ni altérée, ni détruite d'une façon non autorisée.
- **Confidentialité :** Propriété d'une donnée ou d'une information dont l'accès et l'utilisation sont réservés à des personnes désignées et autorisées.

Exemple : Dossier patient

Sanctions

Lorsqu'un utilisateur contrevient à la Politique de sécurité de l'information ou y déroge en lien avec tous les documents qui en découlent, il s'expose à :

- Des mesures disciplinaires et administratives ou à toutes les autres sanctions appropriées, conformément aux directives de l'organisme, aux règlements et aux conventions collectives en vigueur;
- La révocation de certains droits d'accès aux équipements et services visés par cette politique;
- Un remboursement de toute somme à l'organisme. Cela inclut un jugement prononcé par tout tribunal ou organisme réglementaire.

La sécurité de l'information, on s'en occupe!

Soyez vigilants!

COM 2020-079

Centre intégré de santé et de services sociaux de Chaudière-Appalaches
Québec

www.cisssca.com

Québec

Les principes directeurs qui sous-tendent la Politique de sécurité de l'information proviennent de la Politique provinciale de sécurité de l'information (ratifiée en 2015), du Cadre de gestion sur la sécurité de l'information ainsi que de la Règle particulière sur la sécurité organisationnelle du MSSS.

La Règle particulière sur la sécurité organisationnelle du MSSS précise les orientations et les obligations que doivent respecter les établissements du réseau de la santé et des services sociaux.

Le CISSS de Chaudière-Appalaches fait signer un engagement de confidentialité à tous ses utilisateurs, et ce, par l'intermédiaire du Responsable de la sécurité de l'information, de façon électronique, au moyen de l'accès au réseau ou du format papier.

L'utilisateur doit notamment :

- Lire la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches dans l'Intranet sous l'onglet « *Outils de travail/ Règlements, politiques, procédures, protocoles et processus* »;
- Faire part de toute situation problématique susceptible de compromettre la sécurité des actifs informationnels du CISSS de Chaudière-Appalaches en écrivant à : **incident.sécuriteinformatique.cisssca@ssss.gouv.qc.ca**

L'utilisateur est imputable de son manquement à la Politique de sécurité de l'information

Soyez vigilants!

Plateformes virtuelles de travail

Trois plateformes s'offrent à vous selon le contexte :

- TEAMS, pour la collaboration interprofessionnelle, les réunions intraéquipes et avec d'autres professionnels du CISSS de Chaudière-Appalaches;
- ZOOM pour des rencontres avec des usagers en téléconsultation, des rendez-vous instantanés, des rendez-vous planifiés, etc.;
- REACTS, pour des besoins de téléconsultation spécialisés qui requièrent une qualité d'image optimale et mieux définie (soins de plaies, pathologie, multiples caméras), intégration à un chariot de téléconsultation spécialisé, intégration à un logiciel médical (DMÉ, etc.), la solution REACTS est favorisée.

N'oubliez pas d'obtenir le consentement de l'usager avant d'envoyer le lien de consultation.

Confidentialité des renseignements personnels et leur communication

Le dossier des usagers est soumis à la plus stricte confidentialité, comme l'exigent les différentes lois. **Aucun renseignement ne peut en être tiré sans le consentement de l'individu concerné.** L'article 19 de la Loi sur les services de santé et les services sociaux prévoit quelques exceptions. Par exemple, le législateur prévoit que le directeur de la Santé publique n'a pas à obtenir le consentement de l'usager en ce qui concerne les maladies à déclaration obligatoire (MADO).

Il est strictement interdit de visualiser ou d'imprimer des rapports de diagnostic ou listes de patients pour un usage autre que professionnel.

Le fait d'avoir accès au dossier de l'usager ne justifie en aucun cas un usage personnel de ces données.

Exemple : Consulter ses propres résultats d'examens ou ceux d'un proche est interdit.

Mots de passe

La sécurité informatique repose en grande partie sur le mot de passe, qui protège l'accès à l'information. Son efficacité dépend de sa confidentialité. Pour préserver cette confidentialité, il faut l'entourer de mesures et de règles.

La valeur du mot de passe est liée à la volonté de l'utilisateur de le **garder secret**. La négligence et l'insouciance contribuent à la fraude. Prenez ces précautions :

- Ne révélez jamais votre mot de passe à qui que ce soit;
- N'utilisez jamais le mot de passe d'un tiers;
- Mémorisez votre mot de passe et ne l'écrivez pas, à moins de le conserver dans un endroit aussi personnel que votre porte-monnaie;
- Votre mot de passe devrait contenir des lettres, des chiffres et au moins une majuscule.

Ne pas respecter un mot de passe est considéré comme une **usurpation d'identité** et cet incident sera noté à votre dossier en Sécurité de l'information et sera, dans certains cas, rapporté à la Direction des ressources humaines, des communications et des affaires juridiques.

Changez votre mot de passe dès que vous soupçonnez qu'il a été découvert. Rappelez-vous que le mot de passe est un moyen de contrôle pour identifier un utilisateur; **le titulaire d'un code d'accès est donc responsable de tous les accès effectués sous son code.**

Courrier électronique

- Le transfert d'informations personnelles et confidentielles que détient un utilisateur doit être effectué en accord avec la personne concernée (utilisez le formulaire d'autorisation pour l'utilisation d'un moyen de communication électronique #REG0307 (GDE) ou le formulaire #8408 (papier) disponible à la reprographie et faites-le parvenir au dossier de l'usager.
- L'utilisateur du CISSS de Chaudière-Appalaches doit se servir d'une adresse électronique du Réseau de la Santé et des Services sociaux.
- L'usage du courrier électronique est interdit pour des fins de propagande (syndicale, politique, commerciale, illégale ou inappropriée).
- La redirection automatique vers une adresse électronique externe est interdite.

Utilisation d'Internet

Internet est mis à la disposition des employés pour une utilisation professionnelle (tâches reliées à l'exercice de leurs fonctions).

Il doit être utilisé avec vigilance, en respectant les droits d'auteur, la propriété intellectuelle, les règles des licences de logiciels, les droits de propriété, la confidentialité des informations et des données, tout en faisant bon emploi des ressources et des outils disponibles et en respectant les lois et règlements en vigueur.

Certaines catégories de sites sont bloquées pour faire respecter la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches.

En voici quelques-unes :

- Sites sexuellement explicites (pornographie);
- Sites de jeux;
- Sites d'accès à distance (afin de se connecter sur un poste à l'extérieur du réseau de l'établissement).