

Les renseignements de santé et de services sociaux

Cette fiche s'adresse aux étudiants et stagiaires et est basée sur la [Loi sur les renseignements de santé et de services sociaux](#) (RLRQ. c. R-22.1)

En tant que stagiaire, étudiant, observateur d'un jour, externe ou résident œuvrant dans le réseau de la santé (les **étudiants**), vous pourriez avoir accès à des renseignements de santé concernant les usagers. Il est essentiel de comprendre ce qu'est un renseignement de santé pour mieux le protéger.

Qu'est-ce que c'est, un renseignement de santé ?

Cette notion inclut tout renseignement qui permet d'identifier une personne (en raison de la présence d'un identifiant comme le nom, la date de naissance, le numéro d'assurance-maladie, le numéro de dossier, etc.) et qui concerne la santé physique ou mentale d'une personne, par exemple : l'histoire de cas, le motif de la consultation, les résultats d'examens diagnostics (imagerie, prise de sang, etc.), la nature des soins et services offerts ou reçus, la date de la consultation et l'endroit où les soins ont été dispensés.



Le simple fait qu'une personne soit usagère d'un service ou d'un établissement constitue un renseignement de santé



La protection des renseignements de santé et de services sociaux :



une responsabilité pour tous

Ce document a pour objectif de vous sensibiliser à la manière dont les renseignements de santé et de services sociaux (les **renseignements de santé**) doivent être gérés dans le cadre de vos études, de votre stage et de votre future pratique professionnelle. Il aborde les obligations légales et éthiques relatives à la protection des renseignements de santé, les bonnes pratiques à adopter au quotidien pour assurer leur confidentialité, ainsi que les conséquences des incidents de confidentialité qui peuvent survenir.

À travers ce document, nous vous fournirons les connaissances de base et les outils nécessaires pour comprendre et appliquer les règles de protection des renseignements de santé, afin de garantir la confiance et la sécurité des usagers.

Où se retrouvent ces renseignements de santé dont la confidentialité doit être protégée ?

PARTOUT ! Cette notion inclut :

- Les renseignements contenus dans les systèmes informatiques, les dossiers électroniques ou papier, les formulaires, les listes de rendez-vous, les courriels, les notes personnelles rédigées dans le cadre de la collecte d'information;
- Les renseignements échangés de vive voix avec l'utilisateur, lors d'échanges téléphoniques ou de conversations en personne;
- Les renseignements discutés en équipe (ex : discussions d'un cas clinique avec un superviseur de stage ou un collègue de l'équipe);
- Les renseignements que l'on entend ou auxquels on est exposé;
- Etc.

Pourquoi la protection de la confidentialité des renseignements de santé est-elle si fondamentale ?

L'importance de protéger les renseignements de santé, tout comme le secret professionnel, découle de la nécessité de garantir aux personnes qui reçoivent des soins ou des services de santé la possibilité de fournir leurs renseignements de santé en ayant pleinement confiance que la confidentialité sera protégée.

Cette obligation découle du droit à la vie privée, un droit fondamental dont toute personne est titulaire. Ce droit, en contexte de soins, est essentiel à la qualité des soins et de la relation thérapeutique.

Qui doit protéger la confidentialité des renseignements de santé ?

TOUT LE MONDE !

Que ce soit un membre du personnel qui n'a pas un accès direct aux dossiers de l'utilisateur (ex : préposé à l'entretien, préposé à l'alimentation), celui qui offre directement un soin ou un service à l'utilisateur (ex : infirmière, travailleur social), le médecin, l'étudiant, le stagiaire ou le bénévole. **En fait, toutes les personnes qui contribuent à la mission de l'établissement sont responsables de protéger les renseignements de santé !**

Quelles sont mes obligations ?

Comme tout intervenant du secteur de la santé, vous avez l'obligation d'assurer la protection des renseignements de santé, ce qui inclut notamment :

- D'adopter les bonnes pratiques qui permettent de respecter la confidentialité (*voir fiche 2 sur « Les bonnes pratiques »*);
- De rapporter à votre superviseur ou supérieur immédiat toute situation qui pourrait constituer un incident de confidentialité (*voir fiche 3 sur « Les incidents de confidentialité »*).



Saviez-vous que cette obligation vous suit partout et toute votre vie ?

La fin d'un stage ou d'un lien d'emploi, par exemple, ne met pas un terme au devoir de respecter la confidentialité des renseignements de santé dont vous avez eu connaissance dans le cadre de votre stage ou votre emploi.

Votre rôle dans la protection des droits de l'utilisateur

Il est essentiel de comprendre que l'utilisateur a des droits importants concernant la gestion de ses renseignements de santé, y compris le droit de restreindre l'accès à ses renseignements de santé à un intervenant ou à une catégorie d'intervenants en particulier. **Il est donc de votre responsabilité de vous identifier clairement comme étudiant lorsque vous êtes amené à interagir avec un usager.**

Par exemple, avant toute interaction, vous devez informer l'utilisateur de votre statut d'étudiant et préciser que vous êtes sous la supervision d'un professionnel expérimenté. Dans le cas où un usager refuserait votre implication ou restreindrait l'accès à ses renseignements de santé, il est important de ne pas insister. Vous devrez immédiatement en informer votre superviseur ou supérieur immédiat, qui prendra les mesures nécessaires pour s'assurer que les droits de l'utilisateur soient respectés.



Votre rôle dans la protection des droits de l'usager (suite)

Vous pourriez également être en contact avec plusieurs types de renseignements de santé que vous devrez :

- **Recueillir**

- Par exemple, les antécédents médicaux de l'usager, comme les maladies précédentes, les allergies et les traitements en cours.

- **Consulter**

- Par exemple, le dossier médical antérieur d'un usager, pour connaître les résultats d'exams précédents.

- **Utiliser**

- Par exemple, les renseignements concernant une personne dans une situation de vulnérabilité, pour orienter cette personne vers les ressources et les services appropriés.

- **Déposer au dossier**

- Par exemple, les résultats d'une analyse de laboratoire, pour que d'autres professionnels de santé y aient accès lors des prochaines consultations.

- **Communiquer**

- Par exemple, les résultats d'un examen radiologique au patient et à son médecin référent pour assurer un suivi approprié.

- **Détruire**

- Par exemple, les doublons imprimés, qui seront déposés dans les bacs verrouillés à cet effet.

Pour bien protéger les renseignements de santé, gardez en tête :

- D'utiliser les bonnes pratiques mentionnées à la *Fiche 2*;
- De référer l'usager, ou ses proches, à votre superviseur ou supérieur immédiat en cas de doute sur vos obligations en matière de protection des renseignements de santé.

Formation sur la protection des renseignements de santé



Sachez qu'une formation sur la protection des renseignements de santé est disponible sur l'ENA ([Formation ENA #15757](#)). À noter que vous devez avoir les accès octroyés par l'établissement de santé et de services sociaux pour pouvoir suivre la formation.

Les bonnes pratiques

Cette fiche s'adresse aux étudiants et stagiaires



La protection des renseignements de santé,
c'est une question d'éthique professionnelle!

J'agis de façon éthique lorsque :

- J'accède seulement aux renseignements de santé **nécessaires** pour l'exercice de mes fonctions;
- J'utilise mon **adresse professionnelle** (ssss.gouv.qc.ca, sante.quebec), si elle m'est fournie, pour communiquer par courriel. Si je ne possède pas d'adresse courriel professionnelle et qu'il est nécessaire que j'utilise mon adresse courriel personnelle pour communiquer un document contenant des renseignements de santé ou étant autrement confidentiel, je m'assure de le **protéger avec un mot de passe**. Le mot de passe est alors transmis au destinataire dans une communication subséquente;
- J'utilise seulement **les logiciels et outils informatiques approuvés** par l'établissement de santé;
- J'imprime **seulement ce qui est nécessaire** pour mes fonctions;
- Je conserve tout document **en lieu sûr** (dans un classeur verrouillé, sur le réseau informatique, etc.) dans l'établissement de santé;
- J'enlève **ce qui permet d'identifier** l'utilisateur (ex : son nom et toute information permettant de l'identifier) lorsque je dois utiliser les renseignements de santé à des fins scolaires;
- Je m'assure que toute conversation confidentielle ait lieu dans un **endroit permettant d'assurer la confidentialité**;
- Je dépose au dossier ou je détruis tout document papier contenant des renseignements **dans les bacs confidentiels** prévus à cet effet;
- Pour les fins de prestation de soin, je partage les renseignements uniquement aux personnes qui en ont besoin pour offrir des soins ou services sociaux à l'utilisateur ou personnel qui les soutient et seulement lorsque requis. Je limite aussi cette communication aux seuls renseignements nécessaires;
- Je ne révèle pas les confidences et les informations confidentielles dont j'ai eu connaissance dans le cadre mon stage ou de mon emploi.



N'oubliez pas que vous devez protéger toutes les informations, incluant celles que vous entendez.

Pour une pratique irréprochable, privilégier **les espaces fermés** et éloignez-vous à une distance raisonnable en présence de tierces personnes lorsque vous discutez avec l'utilisateur, ou lorsque vous discutez d'un cas avec un collègue.

Les « **discussions de corridor** » dans les espaces publics (cafés, la cafétéria, bibliothèque) sont à proscrire.

À l'ère du numérique, rappelez-vous que vous devez :

- Protéger vos codes d'accès, ne pas les partager et les utiliser uniquement lorsque nécessaire à l'exercice de vos fonctions (il est strictement interdit de consulter son propre dossier, le dossier d'un proche ou de toute personne par simple curiosité);
- Ne pas enregistrer sur son ordinateur personnel de documents comportant des renseignements de santé et permettant d'identifier l'utilisateur;
- Utiliser des mots de passe sécuritaires (mélange de 8 caractères : lettres, chiffres et caractère spéciaux);
- Conserver les renseignements de santé dans un endroit sécuritaire (ex. ranger les documents dans une armoire verrouillée, dans une salle verrouillée);
- Utiliser seulement les logiciels formellement autorisés par l'établissement, incluant ceux utilisant l'intelligence artificielle. Ne jamais verser de renseignements de santé dans un logiciel gratuit en ligne (ex. : ChatGPT, Google Traduction, etc.);
- Verrouiller votre session informatique lorsque vous quittez votre bureau ou votre poste;
- Utiliser le courriel professionnel de façon sécuritaire :
 - Faire une double validation de l'adresse courriel;
 - Utiliser l'option « Confidentiel » ou « Hautement confidentiel », lorsque pertinent;
 - Configurer un accusé de réception.



Lorsque je suis en stage, je laisse mon cellulaire de côté!

Pas de textos!

Je n'utilise pas mon cellulaire pour envoyer ou recevoir des renseignements de santé par textos (incluant des photos du dossier, par exemple).

Pas de photos!

Je ne prends pas de photo du dossier, de l'utilisateur, ou de tout autre renseignement de l'établissement. J'évite de me prendre en photographie durant mes fonctions.

Pas de médias sociaux!

Je ne partage aucune information relative à l'établissement de santé, aux usagers ou à mes fonctions sur les médias sociaux. Les interactions professionnelles doivent rester privées et respectueuses de la confidentialité.

Les incidents de confidentialité

Cette fiche s'adresse aux étudiants et stagiaires

Qu'est-ce que c'est ?

Un incident de confidentialité, c'est le fait d'accéder à un renseignement de santé, de l'utiliser ou de le communiquer **alors qu'on n'y avait pas droit**. C'est aussi le fait de perdre un renseignement ou de faire toute autre chose qui est interdite avec celui-ci.



Saviez-vous que se questionner sur la protection des renseignements de santé démontre du professionnalisme dans le cadre d'un stage ! N'hésitez pas à en parler !

Un incident est si vite arrivé !

Quelques exemples d'incidents lors d'un envoi courriel :

- Envoyer un courriel à la mauvaise personne;
- Transférer l'intégralité d'une chaîne de courriels alors que seul le dernier courriel était nécessaire pour le destinataire.

Quelques exemples d'incidents lors de conversations :

- Discuter d'une histoire de cas avec un collègue dans le corridor alors que d'autres personnes peuvent entendre;
- Répéter à haute voix les renseignements recueillis par téléphone en présence de tiers.

Quelques exemples d'incidents impliquant des documents papier :

- Quitter son bureau sans avoir rangé un dossier usager dans un classeur verrouillé;
- Imprimer des renseignements de santé et oublier de les récupérer à l'imprimante;
- Oublier des documents lors d'une visite à domicile ou les laisser sans surveillance dans un endroit non protégé (ex. dans sa voiture).



Des impacts potentiels importants !

Pour l'utilisateur, ça peut ébranler sa confiance, porter atteinte à sa réputation, entraîner un vol d'identité, etc.

Pour l'organisation, ça peut occasionner une poursuite judiciaire, la perte de confiance du public, etc.

Détecter un incident de confidentialité et agir

En cas d'incident de confidentialité

1

Étape 1

Limitier l'incident autant que possible pour en atténuer les conséquences (ex : en rappelant le courriel);

2

Étape 2

Informez votre superviseur immédiatement!

3

Étape 3

En accord avec votre superviseur :

1. Documenter, au dossier, au mieux les circonstances de l'incident pour pouvoir convenablement le déclarer;
2. Procéder à la déclaration en utilisant le formulaire normalisé AH-223 et suivre la procédure de votre établissement pour la suite.



En cas de doute, il vaut mieux considérer être en contexte d'incident de confidentialité et signaler la situation à l'aide du formulaire AH-223.