

Journalisation de l'accès et de l'usage des dossiers d'utilisateurs en format électronique (DUFE)			
Direction(s) responsable(s)	Direction de la qualité, de l'innovation, de la performance et de l'éthique	Adopté	2026-09-22
		Révisé	
Personne(s) concernée(s)	Tous les utilisateurs, responsables de systèmes d'information, pilotes des dossiers d'utilisateurs en format électronique, les gestionnaires de ces personnes, l'équipe des relations de travail de l'Établissement et les responsables de la protection des renseignements personnels (PRP)		
Document(s) associé(s)	CDR-10362 Cadre de référence sur la gestion, la tenue et l'accès aux dossiers des usagers POL-10372 Gouvernance en matière de protection des renseignements personnels ADM-DQIPE-10003 Engagement de confidentialité à l'égard des renseignements personnels Feuille d'information - Engagement de confidentialité à l'égard des renseignements personnels		

1. Énoncé

Santé Québec Montérégie-Ouest s'engage à mettre en place des mesures permettant d'assurer un usage approprié de ses systèmes d'information pour protéger les renseignements personnels et les renseignements de santé et de services sociaux de ses usagers.

L'une de ces mesures consiste à appliquer une procédure de journalisation concernant l'utilisation de dossiers d'utilisateurs en format électronique (ci-après DUFE), afin d'évaluer l'état de la confidentialité de ses dossiers ainsi que d'en assurer un usage approprié et conforme à la législation en vigueur.

L'une de ces mesures consiste à mettre en place des mécanismes de journalisation concernant l'accès et l'utilisation de dossiers d'utilisateurs en format électronique (ci-après DUFE), afin d'évaluer leur état de la confidentialité, d'en assurer un usage approprié et conforme à la législation en vigueur et, le cas échéant, prendre les mesures appropriées.

Cette procédure découle directement des documents d'encadrement suivants :

- CDR-10362 Cadre de référence sur la gestion, la tenue et l'accès aux dossiers des usagers;
- [POL-10372 Gouvernance en matière de protection des renseignements personnels](#)

Le premier a pour but d'uniformiser les modes de pratique de l'ensemble des installations de l'Établissement et de servir d'outil de référence pour informer et sensibiliser le personnel et les membres du Conseil des médecins, dentistes, pharmaciens et sage-femmes (CMDPSF) au respect de la confidentialité du dossier de l'utilisateur et de ses différentes composantes. Les circonstances permettant à un salarié et à un membre du CMDPSF de l'Établissement d'accéder à un dossier d'utilisateur détenant des renseignements de santé et de services sociaux et de services sociaux confidentiels y sont précisées.

Le cadre de référence précise également que tout intervenant ou employé qui accède ou divulgue de l'information se trouvant au dossier d'un usager, qui accède à son propre dossier ou au dossier médical d'un tiers relié (ex. : enfant, parent, conjoint, sœur, frère, etc.), qui consulte celui d'un membre de sa famille ou de toute autre personne sans y être expressément autorisé, s'expose à des sanctions

Quant à la politique-cadre sur l'accès à l'information et la gouvernance des renseignements personnels, elle établit un cadre de gouvernance visant à assurer à la fois l'accès à l'information et la protection des renseignements personnels, en précisant les mécanismes, les responsabilités et les pratiques à mettre en place au sein de Santé Québec.

2. Champ d'application/Contexte légal

En vertu de la *Loi sur les renseignements de santé et de services sociaux et de services sociaux et de services sociaux (LRSSS)*, l'accès non conforme au dossier de l'utilisateur est passible de sanctions et d'amendes. La présente procédure précise ainsi les rôles et responsabilités de chacune des parties prenantes impliquées afin de permettre la gestion et l'utilisation adéquate des renseignements de santé et de services sociaux compris dans les DUFÉ.

De plus, la journalisation de l'usage et des accès aux DUFÉ fait partie des obligations incombant aux organismes du RSSS en vertu de la *LRSSS*. La consultation de dossiers des utilisateurs sans justification va à l'encontre de plusieurs lois, politiques et dispositions, telles que les suivantes, mais sans être exhaustives :

- L'article 5 de la *Charte des droits et libertés de la personne* stipule que « Toute personne a droit à sa vie privée »;
- L'article 3 du *Code civil* stipule que « Toute personne est titulaire de droits de la personnalité, tels les droits à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation et de sa vie privée »;
- L'article 35 du *Code civil* stipule que « Toute personne a droit au respect de sa réputation et de sa vie privée »;
- L'article 2088 du *Code civil* stipule que « Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et honnêteté et ne pas faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail [...] »;
- L'article 38 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* : « Un intervenant qui est un professionnel au sens du *Code des professions* (chapitre C-26) peut être informé de l'existence d'un renseignement détenu par un organisme et y avoir accès dans les cas suivants :
 - 1° il lui est nécessaire pour offrir à la personne concernée des services du domaine de la santé et des services sociaux ;
 - 2° il lui est nécessaire à des fins d'enseignement, de formation ou de pratique réflexive ».
- L'article 39 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* : « Un intervenant qui n'est pas un professionnel au sens du *Code des professions* (chapitre C-26) peut être informé de l'existence d'un renseignement détenu par un organisme et y avoir accès aux conditions déterminées par un règlement du gouvernement dans les cas suivants:
 - 1° il lui est nécessaire pour offrir à la personne concernée des services du domaine de la santé et des services sociaux ;
 - 2° il lui est nécessaire pour fournir des services de soutien technique ou administratif à un autre intervenant qui offre des services du domaine de la santé et des services sociaux à la personne concernée ».
- L'article 62 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* : « Un renseignement personnel est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions »;
- La *Loi sur les renseignements de santé et de services sociaux* explique les circonstances dans lesquelles un Établissement peut divulguer certaines informations de santé sans le consentement de l'utilisateur ;
- Cette présente procédure est applicable aux DUFÉ suivants :
 - Dossier médical électronique (DMÉ) organisationnel ;
 - Dossier clinique informatisé (DCI) organisationnel ;
 - Dossier de santé numérique (DSN) organisationnel ou provincial ;

Les systèmes d'information ne sont pas couverts par la présente procédure s'ils ne traitent pas principalement des renseignements de santé et n'ont pas pour vocation d'agir à titre de DUFÉ, par exemple :

- I-CLSC;
- SIPAD;
- eClinibase;
- Etc.

3. Définitions

Audit: Démarche d'examen, de contrôle et d'évaluation fondée sur l'analyse ciblée des données de journalisation, visant à déterminer dans quelle mesure une action ou un ensemble d'actions respecte les objectifs, les normes ou les exigences établis. L'audit comporte des activités de vérification, de surveillance, d'inspection et de contrôle.

Auditeur : personne chargée de l'audit de l'usage et de l'accès à un système d'information. L'auditeur est généralement le pilote du système d'information visé.

Autorisation d'accès : attribution de droits d'accès à une personne par une autorité.

Authentifiant : information confidentielle détenue par une personne et permettant son authentification.

Authentification : acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

Cadre responsable du DUFE: employé désigné par un organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, dont le rôle est notamment de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de son unité administrative. Le cadre responsable du système DUFE est généralement le gestionnaire du pilote du DUFE (auditeur) ainsi que le gestionnaire responsable de l'audit.

CMDPSF: Conseil des médecins, dentistes, pharmaciens et sages-femmes;

Confidentialité : désigne la pratique consistant à protéger les renseignements personnels et à prévenir leur divulgation, leur accès ou leur partage non autorisés.

Continuum de soins: gamme complète et coordonnée des services de santé et sociaux. Il s'assure qu'un patient reçoit les soins appropriés, au bon moment et par le bon professionnel, tout au long de l'évolution de son état ou de sa maladie, sans interruption dans son parcours (vitrine linguistique).

Contrôle d'accès : processus par lequel les données d'authentification fournies par une personne, ou toute autre entité, pour avoir accès à un système d'information, sont comparées avec des valeurs de référence définies touchant cette personne, permettant ainsi l'autorisation, ou le refus de l'accès demandé.

Détenteur du système d'information : employé désigné par un organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, dont le rôle est notamment de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité d'une de ses unités administratives. Cette personne est généralement le directeur de la direction comprenant l'unité administrative détenant le rôle d'assurer notamment la sécurité de l'information et des ressources détenues et utilisant son système d'information.

Dossier clinique informatisé (DCI) : version numérique du dossier d'utilisateur, utilisée au sein d'un établissement de santé (hôpital, CLSC) pour centraliser, en temps réel, l'ensemble des renseignements cliniques consignés par les professionnels. Il remplace le papier pour faciliter l'accès, la continuité et la qualité des soins (www.msss.gouv.qc.ca).

Dossier médical électronique (DMÉ) : version numérique sécurisée du dossier papier d'un utilisateur, regroupant ses antécédents, diagnostics, médicaments et résultats d'examen. Utilisé principalement par les cliniciens, il permet un accès rapide aux informations, améliorant la coordination des soins et l'efficacité administrative (www.canada.ca).

Dossier usager : document à valeur clinique et juridique dans lequel sont consignés tous les renseignements relatifs à l'utilisateur qui demande ou reçoit des soins et des services professionnels, ainsi que tout renseignement pertinent à ses soins et services (CISSS de Lanaudière, 2018).

Disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Identifiant : information associée à une personne, connue de celle-ci ou contenue sur un support informatique, dont elle est la détentrice, et qui permet son identification. À titre d'exemples, la carte informatique servant aux transactions bancaires effectuées au guichet automatique, ainsi que le nom d'utilisateur sont des identifiants. Ils sont respectivement couplés, la plupart du temps, à un numéro d'identification personnel (NIP) et à un mot de passe, lesquels sont des éléments d'authentification.

Identification : opération qui consiste, pour une personne demandant l'accès au système d'information, à communiquer à ce dernier l'identité dont elle se réclame. L'identification s'effectue notamment par la saisie d'un code utilisateur; il s'agit soit d'un nom, soit d'un numéro spécifique à la personne.

Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

Intervenant : gestionnaires, employés des directions cliniques, médecins, dentistes, pharmaciens, stagiaires, étudiants, externes et résidents exerçant une fonction dans l'établissement ou rattachée à l'établissement pour la prestation du soin ou de services sociaux.

Journalisation: enregistrement chronologique et automatique des événements, opérations ou transactions effectués au sein d'un système d'information, d'une base de données ou d'un réseau. Ces enregistrements permettent de suivre l'activité, de garantir la sécurité et de faciliter le dépannage (Vitrine linguistique).

Non-Conformité : la collecte, la communication, la transmission ou la destruction d'un renseignement personnel d'une manière allant à l'encontre de la Loi, des règlements et de la présente procédure. La non-conformité peut avoir un caractère intentionnel ou non. Par exemple, est considérée comme une non-conformité, la consultation d'un renseignement personnel sans autorisation.

Pilote applicatif : personne clé en informatique qui fait le lien entre les équipes de développement (Build) et les utilisateurs ou l'exploitation (Run). Il est garant du bon fonctionnement des logiciels et de leur maintenance au quotidien.

Programme clinique: ensemble structuré de soins, de thérapies et de suivis prodigués par une équipe multidisciplinaire.

Renseignements personnels (RP) : un renseignement personnel est toute information concernant une personne physique permettant de l'identifier directement (nom, photo) ou indirectement (adresse IP, numéro de client, numéro de téléphone) (*Commission d'accès à l'information, 2026*)

Renseignement de santé (RS): au sens de la *Loi sur les renseignements de santé et de services sociaux et de services sociaux et de services sociaux*, est un renseignement de santé et de services sociaux tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes :

- 1° il concerne l'état de santé physique ou mental de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne;
- 2° il concerne tout matériel prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant ou toute orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne;
- 3° il concerne les services du domaine de la santé ou des services sociaux offerts à cette personne, notamment la nature de ces services, leurs résultats, les lieux où ils ont été offerts et l'identité des personnes ou des groupements qui les ont offerts;
- 4° il a été obtenu dans l'exercice d'une fonction prévue par la Loi sur la santé publique (chapitre S- 2.2);
- 5° toute autre caractéristique déterminée par règlement du gouvernement.

De plus, un renseignement personnel est un renseignement de santé et de services sociaux lorsqu'il est accolé à un renseignement visé au premier alinéa ou qu'il est recueilli en vue de l'enregistrement, de l'inscription ou de l'admission

de la personne concernée dans un établissement ou de sa prise en charge par un autre organisme du secteur de la santé et des services sociaux.

Par conséquent, les renseignements concernant les usagers de l'Établissement sont des RS.

Système d'information : ensemble structuré de ressources matérielles, logicielles et humaines qui permettent la collecte, le stockage, le traitement et la diffusion d'information (vitrine linguistique).

Unité de soins : regroupement d'activités de [soins et de services de santé](#) et sociaux. Celle-ci peut être représentée géographiquement ou par une thématique de soins. Pour les besoins de la présente procédure, le terme unité de soins englobera également la notion de programme clinique.

Usager : toute personne qui reçoit, a reçu ou aurait dû recevoir des services d'un établissement de santé et de services sociaux, d'un organisme communautaire, d'une résidence pour personnes âgées ou d'un service préhospitalier d'urgence.

Usage inapproprié : le fait par un utilisateur d'utiliser un renseignement personnel ou un renseignement de santé à une fin non prévue lors de la collecte ou par la Loi, les règlements et la présente procédure.

Sécurité de l'information : ensemble des mesures mises en place visant à assurer la confidentialité, l'intégrité et la disponibilité de l'information tout au long de son cycle de vie, afin de protéger les actifs informationnels contre les menaces et garantir la continuité des soins et des services sociaux.

Utilisateur : toute personne physique qui fait usage d'un ou de plusieurs systèmes d'information sous la responsabilité de l'établissement, notamment les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel, les bénévoles et les tiers.

4. Objectifs

La journalisation et la surveillance des accès est une mesure nécessaire permettant de soutenir l'Établissement dans ses obligations de protection des renseignements personnels (RP) et des renseignements de santé et de services sociaux (RS) des usagers. Cette procédure vise autant à assurer la confidentialité et l'intégrité des données des usagers disponibles dans les DUFE que l'usage approprié de ces systèmes, contribuant ainsi à leur sécurité.

Rappelons que par « usage inapproprié », le *ministère de la Santé et des Services sociaux (MSSS)* entendait notamment, dans une reddition de comptes transmise aux présidents-directeurs généraux et directeurs généraux des *Établissements publics de santé et services sociaux* le 19 mai 2023 :

- L'accès par un professionnel qui n'a pas, ou qui n'est pas impliqué dans le continuum de soins de l'usager;
- L'utilisation des dossiers pour une autre fin que la prestation de soins et services, sauf dans la mesure où le professionnel aura reçu préalablement une autorisation par une personne désignée (ex.: fins de recherche);
- La consultation de son propre dossier (*Savoie D., 2023*).

Selon la *Loi*, un incident de confidentialité correspond à tout accès, usage ou communication non autorisés par la *Loi d'un renseignement personnel*, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection (*Commission d'accès à l'information du Québec, 2024*).

La gestion des accès, comprenant également l'usage, joue ainsi un rôle de premier ordre dans le contrôle et la réduction des risques de sécurité de l'information. Elle s'étend à plusieurs domaines, tels que la conformité à la réglementation, l'efficacité opérationnelle et la gestion des accès privilégiés, entre autres.

La gestion des accès constitue un élément fondamental de la sécurité de l'information, en encadrant l'accès aux renseignements de santé et de services sociaux et en assurant leur utilisation conforme par les personnes autorisées. Elle permet notamment l'établissement de mécanismes de contrôle en cas d'écart et assure la traçabilité des accès et des opérations.

La mise en place d'un processus de journalisation permet notamment, mais sans s'y limiter:

- De renforcer la sécurité de l'information de l'organisation, en garantissant la cohérence d'attribution des droits d'accès aux ressources appropriées aux systèmes informatiques;
- D'assurer un usage approprié et sécuritaire des nombreux systèmes informatiques en vue d'en garantir la confidentialité et la protection des données des usagers;
- De répondre aux exigences légales et réglementaires;
- De mettre en place les structures de gouvernance pour une saine gestion d'accès aux données et aux systèmes informatiques;
- D'assurer une traçabilité des accès et des consultations effectuées dans les systèmes informatiques;
- De servir d'éléments probants lors de la conduite d'enquête, advenant un incident ou un écart d'usage décelé;
- D'assurer la présence de contrôles adéquats pour détecter, vérifier et valider les accès aux systèmes informatiques et le respect des directives et procédures de sécurité de l'établissement.

5. Rôles et responsabilités

5.1. Généralités

Les événements importants à journaliser doivent être établis selon une stratégie de journalisation qui respecte les critères de classification (valeur, nature sensible et importance) des systèmes informatiques autant que l'analyse des risques et menaces, par exemple :

- *Un événement sentinelle impliquant un médecin, une infirmière, un professionnel, une agente de bureau, ou tout autre événement médiatisé, un cas connu, un drame chez un employé, etc.;*
- *À la suite d'une demande spécifique ou d'une incertitude relevée quant à un usage inapproprié.*

Les événements à journaliser peuvent être liés à des incidents de sécurité — tels que des tentatives d'intrusion ou des accès et consultations non autorisés — ou être consignés de manière aléatoire. La gestion et la revue des journaux doivent être réalisées par un nombre restreint de personnes préalablement autorisées par le détenteur du système informatique, généralement le pilote et son gestionnaire (généralement le cadre responsable du système informatique). Le responsable de la protection des renseignements personnels et confidentiels (PRP) peut aussi demander à auditer la journalisation de tout système.

L'analyse des journaux d'événements permet de découvrir les sources d'écarts d'usage et d'accès, les conditions d'utilisation, les tentatives de violation des règles, la récurrence, etc. L'analyse des événements à journaliser ainsi que les informations à conserver sur ces événements doivent être formellement documentées dans un fichier de consignation (voir modèle à l'annexe 1 – Fichier d'audit de journalisation). La documentation pour chacun des événements journalisés doit comprendre les informations suivantes :

- *Le nom du DUFE journalisé;*
- *L'identité de l'utilisateur journalisé;*
- *L'identité de l'utilisateur :*
- *La nature de l'acte ou de la transaction que l'utilisateur a accomplis (ex. : création, consultation, modification, etc.);*
- *La date et l'heure auxquelles la transaction a été effectuée (dans les cas où plus d'une transaction a été effectuée, chacune d'entre elles doit être identifiée séparément dans le fichier);*
- *Le nombre de transactions inappropriées, selon le type d'usage inapproprié.*

Considérant que la *Loi sur les renseignements de santé et de services sociaux et de services sociaux et services sociaux* oblige les Établissements à journaliser l'usage des utilisateurs sur leurs systèmes informatiques, ces derniers doivent être avisés, dès leur embauche, que leurs actions posées sur les systèmes informatiques sont journalisées et sont passibles de sanctions disciplinaires en cas d'anomalies détectées.

Les preuves de vérification des journaux d'événements, fichiers ou mécanismes de journalisation des systèmes informatiques sont conservées en format électronique, par le service des archives médicales. L'accès à la documentation relative à ces dossiers audités est disponible seulement aux personnes autorisées (détenteur d'actif,

le pilote du système informatique et son gestionnaire) afin d'être protégées contre toute tentative de désactivation, de modification ou de destruction.

La période de conservation des événements audités doit respecter les lois concernant le cadre juridique des technologies de l'information et sur les services de santé et les services sociaux ou toute autre exigence spécifique, selon le cas. La conservation des événements audités relève du gestionnaire de l'auditeur.

5.2 Démarches de journalisation automatisée

Lorsque ce type de fonctionnalité est offerte dans le DUFE, elle doit être utilisée par les pilotes applicatifs sur une base régulière et minimalement une fois par mois :

- Ex. : Accès d'un utilisateur à son propre dossier;
- Ex. : Accès d'un utilisateur au dossier d'un membre de sa famille;
- Ex. : Accès d'un utilisateur à un dossier par simple curiosité;

Si cette fonctionnalité fait défaut ou s'avère insuffisante, les procédures manuelles de journalisation décrites aux points 5.3.1 et 5.3.2 seront appliquées.

5.3. Démarches de journalisation manuelles (audit)

Afin d'évaluer l'état de la confidentialité des DUFE, le pilote d'applicatif informationnel, ci-après nommé auditeur, procède à la journalisation, c'est-à-dire l'audit de l'usage des DUFE. Cette journalisation s'effectue selon les 2 types d'échantillonnage suivants :

- Échantillonnage aléatoire simple (« simple random sampling »);
- Échantillonnage en grappes (« cluster sampling »).

Chaque DUFE doit faire l'objet d'un échantillonnage et d'une fréquence d'échantillonnage qui tient compte du nombre d'utilisateurs ayant accès au DUFE.

Les demandes de journalisation des accès faites par les usagers eux-mêmes et permettant de documenter les employés de l'Établissement ayant accédé à leur DUFE sont considérées comme faisant partie des démarches de journalisation manuelles.

5.3.1 Échantillonnage aléatoire simple

Les critères d'échantillonnage suivants sont utilisés :

- La taille de l'échantillon sera de 25 dossiers et de 25 utilisateurs audités par tranche de 1 000 utilisateurs du DUFE;
- La période de journalisation visée sera celle des 30 jours calendriers précédant la date du début de l'audit;
- La fréquence de l'audit sera de 10 fois par année (excluant les mois de juillet et août).

La démarche de journalisation est la suivante :

1. L'auditeur sélectionne, aux périodes visées, l'échantillon de dossiers d'utilisateurs et d'utilisateurs actifs de l'établissement dans le DUFE visant à évaluer ledit état de la confidentialité des dossiers usagers qui y sont consignés;
2. L'auditeur analyse les événements à la recherche d'écarts potentiels en matière de respect de la confidentialité et d'usage inapproprié. Les anomalies ou écarts potentiels sont compilés à titre d'anomalie décelée dans le fichier d'audit de journalisation, selon le type d'usage inapproprié:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier.

3. Les rapports d'événements journalisés réalisés par l'auditeur sont compilés dans un répertoire informatique spécifique protégé, selon un plan de classement permettant de rapidement repérer :

- Le DUFE audité;
- Le type d'audit;
- L'année et le mois de l'audit.

4. Pour l'audit aléatoire lié aux dossiers d'utilisateurs, l'auditeur complète un fichier de journalisation qui contient, au minimum, les informations suivantes :

- Date de l'audit;
- Identification du dossier d'utilisateur visé par l'audit;
- Nom du/des DUFE(s) audité(s);
- Nombre d'accès non conformes détectés
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services
 - Consultation de son propre dossier;
- Direction des ressources humaines (volet relations de travail) avisée;
- Divulgence à la Commission d'Accès à l'information (CAI) faite;

5. Pour l'audit aléatoire lié aux utilisateurs actifs du DUFE, l'auditeur complète un fichier de journalisation qui contient, au minimum, les informations suivantes :

- Date de l'audit;
- Identification de l'employé visé par l'audit;
- Nom du/des DUFE(s) audité(s);
- Nombre d'accès non conformes détectés:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier;
- Direction des ressources humaines (volet relations de travail) avisée;
- Divulgence à la Commission d'Accès à l'information (CAI) faite.

5.3.2 • Échantillonnage en grappes (« cluster sampling »)

La notion de "grappe" dans le contexte de journalisation réfère à la notion d'unité de soins.

Les critères d'échantillonnage suivants sont utilisés:

- La taille de l'échantillon sera l'ensemble des dossiers d'utilisateurs ou des utilisateurs rattachés à une unité de soins;
- La période de journalisation visée sera celle des 30 jours calendriers qui précèdent la date du début de l'audit pour les secteurs hors-hospitalier et des 7 jours calendriers qui précèdent la date du début de l'audit pour les secteurs hospitaliers;
- La fréquence de ce type d'audit sera de 6 fois par année (excluant les mois de juillet et août);
- L'audit touchera, en alternance, les dossiers d'utilisateurs rattachés à une unité de soins et les utilisateurs rattachés à une unité de soins;
- Les unités de soins seront sélectionnées au hasard parmi les unités de soins disponibles et parmi celles n'ayant pas fait l'objet d'un audit au cours des 12 derniers mois;

La démarche de journalisation est la suivante :

1. L'auditeur sélectionne, 6 fois par année, une unité de soins de l'Établissement dans le DUFE visant à évaluer ledit état de la confidentialité des dossiers usagers qui y sont consignés;
2. Lorsque le DUFE inclut des renseignements de santé provenant d'unités de soins dédiées en santé mentale, la direction responsable pourra exiger des journalisations supplémentaires de ceux-ci jusqu'à concurrence de 4 fois par année;

3. L'auditeur analyse les événements à la recherche d'écarts potentiels en matière de respect de la confidentialité et d'usage inapproprié. Les anomalies ou écarts potentiels sont compilés à titre d'anomalie décelée dans le fichier d'audit de journalisation, selon le type d'usage inapproprié:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier.
4. Les rapports d'événements journalisés réalisés par l'auditeur sont compilés dans un répertoire informatique spécifique protégé, selon un plan de classement permettant de rapidement repérer:
 - Le DUFE audité;
 - Le type d'audit;
 - L'année et le mois de l'audit.
5. Pour l'audit en grappes relié aux dossiers d'utilisateurs, l'auditeur complète un fichier de journalisation qui contient, au minimum, les informations suivantes :
 - Date de l'audit;
 - Identification du dossier d'utilisateur visé par l'audit;
 - Nom du/des DUFE(s) audité(s);
 - Nombre d'accès non conformes détectés:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier.
 - Direction des ressources humaines (volet relations de travail) avisée;
 - Divulgence à la Commission d'Accès à l'information (CAI) faite.
6. Pour l'audit en grappe relié aux utilisateurs actifs du DUFE, l'auditeur complète un fichier de journalisation qui contient, au minimum, les informations suivantes:
 - Date de l'audit;
 - Identification de l'employé visé par l'audit;
 - Nom du/des DUFE(s) audité(s);
 - Nombre d'accès non conformes détectés:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier;
 - Direction des ressources humaines (volet relations de travail) avisée;
 - Divulgence à la Commission d'Accès à l'information (CAI) faite.

5.3.3 Journalisation de dossiers individuels

Une demande de journalisation d'un dossier ou de dossiers individuel(s) d'utilisateurs peut être demandée dans les circonstances suivantes:

- Lors d'un événement médiatisé;
- Lors d'un événement tragique;
- Lors de suspicion de violation de la confidentialité;
- Dans le cadre de l'application de l'article 18 de la *Loi sur les renseignements de santé et de services sociaux*;
- La demande de ce type de journalisation doit être faite par:
 - a. Chef médical, chef médical adjoint, DMSP-adjoint ou DMSP;
 - b. Gestionnaire;
 - c. Conseiller-cadre à la protection des renseignements personnels;
 - d. Usager lui-même ou son représentant légal;

La demande de journalisation doit être faite par écrit et de façon à pouvoir confirmer l'identité du demandeur. Dans le cas d'une demande faite par un utilisateur ou son représentant légal, le formulaire du MSSS intitulé "Autorisation de communiquer des renseignements contenus au dossier" (AH-216) peut être utilisé.

La démarche de journalisation est la suivante:

1. L'auditeur sélectionne le ou les dossier(s) d'utilisateur(s) visés par la demande dans le DUFE afin d'évaluer ledit état de la confidentialité;
2. L'auditeur analyse les événements à la recherche d'écarts potentiels en matière de respect de la confidentialité et d'usage inapproprié. Toutes anomalies ou écarts potentiels sont compilés à titre d'anomalie décelée dans le fichier d'audit de journalisation, selon le type d'usage inapproprié:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier.
3. Les rapports d'événements journalisés réalisés par l'auditeur sont compilés dans un répertoire informatique spécifique protégé, selon un plan de classement permettant de rapidement repérer:
 - Le DUFE audité;
 - Le type d'audit;
 - L'année et le mois de l'audit.
4. L'auditeur complète un fichier de journalisation qui contient, au minimum, les informations suivantes:
 - Date de l'audit;
 - Identification du dossier d'utilisateur visé par l'audit;
 - Nom du/des DUFE(s) audité(s);
 - Nombre d'accès non conformes détectés:
 - Personnel non impliqué dans le continuum de soins;
 - Consultation à une autre fin que la prestation de soins/services;
 - Consultation de son propre dossier.
 - Direction des ressources humaines (volet relations de travail) avisée;
 - Divulgence à la Commission d'Accès à l'information (CAI) faite.
5. L'auditeur communique les résultats de la démarche de journalisation au demandeur.

5.3.4 Autres journalisations

Dans un processus d'amélioration continue de la qualité, le service des archives médicales pourra ajouter d'autres modalités de journalisation des accès que celles prévues à la présente procédure, suite, entre autres, à l'identification d'enjeux précis.

6. Analyse et gestion des non-conformités (employés de Santé Québec Montérégie-Ouest, pharmaciens et sages-femmes)

1. L'auditeur identifie les gestionnaires des employés pour lesquels des anomalies sont décelées et inscrit l'information dans le fichier d'audit de journalisation.
2. Lorsque des anomalies sont décelées au niveau de la consultation de son propre dossier ou du dossier d'un membre de la famille de l'employé, le gestionnaire de l'auditeur fait une demande d'accompagnement au service des relations de travail ([Demande d'accompagnement RT](#)) à la Direction des ressources humaines (DRH), afin d'obtenir l'accompagnement d'un agent de gestion du personnel (AGP). Il informe également le gestionnaire de l'employé audité de la situation.
3. Lorsque des anomalies sont décelées au niveau des 2 autres éléments de non-conformité:

- Personnel non impliqué dans le continuum de soins;
- Consultation à une autre fin que la prestation de soins/services.

Le gestionnaire de l'auditeur (cadre responsable du système informatique) ou le gestionnaire des archives médicales avise le gestionnaire de l'employé audité, afin que celui-ci revoie les anomalies suspectées et effectue une analyse plus en profondeur, afin de cerner réellement la non-conformité (usage inapproprié). Cette analyse doit être effectuée SANS ÉCHANGE avec l'employé audité.

4. Advenant que l'utilisateur audité soit un gestionnaire, le supérieur immédiat de la direction concernée sera interpellé par le gestionnaire de l'auditeur.

5. Le gestionnaire de l'employé audité informe le gestionnaire de l'auditeur (cadre responsable du système informatique) ou le gestionnaire des archives médicales de la conformité de l'accès ou de l'usage du DUFE, le cas échéant, dans les 15 jours calendrier de la demande.

6. En cas d'absence de l'employé dont la durée prévue est supérieure à 15 jours calendrier, le gestionnaire de l'employé audité fait une demande d'accompagnement au service des relations de travail ([Demande d'accompagnement RT](#)) à la Direction des ressources humaines (DRH) afin d'obtenir l'accompagnement d'un agent de gestion du personnel (AGP).

7. Lorsque les non-conformités sont confirmées ou lorsque la conformité ne peut être établie SANS échanger avec l'employé audité, le gestionnaire de l'employé audité fait une demande d'accompagnement au service des relations de travail ([Demande d'accompagnement RT](#)) à la Direction des ressources humaines (DRH) afin d'obtenir l'accompagnement d'un agent de gestion du personnel (AGP).

8. Une fois l'analyse du dossier finalisée par les Relations de travail de la DRH et l'application de sanctions conséquentes aux écarts de confidentialité, le cas échéant, l'agent de gestion du personnel aux Relations de travail informe le gestionnaire de l'auditeur des conclusions de l'enquête (violation de la confidentialité, divulgation, mesure disciplinaire émise, etc.) afin de faire les suivis appropriés :

a. Si l'utilisateur visé par la mesure fait partie d'un ordre professionnel, les non-conformités quant à un usage inapproprié seront transmises également au chef de service des relations de travail (RT). Ce dernier aura à entreprendre des démarches avec la Direction soutien en pratique professionnelle (DSI, DSM, DMSP) concernée afin qu'ils déterminent la nécessité de faire une déclaration au Syndic de l'ordre professionnel. Le cas échéant, la Direction soutien en pratique professionnelle procède à la déclaration avec les informations fournies par la cheffe des RT.

9. L'équipe des relations de travail compile les sanctions mises en place ainsi que les recommandations émises dans un document à cet effet et en assure le suivi périodique.

10. Tout échantillon audité, qui conclut à une sanction par les relations de travail de l'Établissement, est consigné par l'auditeur à titre de non-conformité dans le fichier de consignation de l'information de journalisation. L'utilisateur visé verra son usage journalisé à nouveau par l'auditeur dans un délai maximal de trois mois à la suite de l'application de sa sanction.

11. En cas de non-réponse du gestionnaire de l'employé audité dans les 15 jours calendrier de la demande, le gestionnaire de l'auditeur (cadre responsable du système informatique) ou le gestionnaire des archives médicales relance celui-ci et informe également son supérieur immédiat de la situation.

7. Analyse et gestion des non-conformités (médecins et dentistes)

1. Lorsque des anomalies sont décelées à la suite d'une journalisation, impliquant un médecin, le gestionnaire de l'auditeur informe le DMSP (directeur médical et des services professionnels) ou le DMSPA (directeur médical et des services professionnels adjoint).

2. Une collecte de la version des faits du médecin concerné doit être effectuée par le chef de département ou, en son absence, par le DMSPA responsable.

3. En cas de non-réponse du chef de département dans les 15 jours calendrier de la demande, le DMSP ou le DMSPA responsable effectue une relance auprès de celui-ci.
4. Advenant qu'un manquement soit confirmé, la situation doit être prise en charge conformément au processus disciplinaire en vigueur.
5. Le DMSP ou le DMSPA responsable doit aviser le gestionnaire de l'auditeur de la conclusion quant à la conformité de l'accès par le médecin ou dentiste concerné.
6. Tout échantillon audité, qui conclut à une non-conformité d'accès est consigné par l'auditeur à ce titre dans le fichier de consignment de l'information de journalisation.

8. Mécanismes de journalisation organisationnels

La démarche de journalisation organisationnelle (ANNEXE E).

9. PARTAGE DES RESPONSABILITÉS

9.1 Direction des ressources humaines

- Informe tout nouvel employé de l'existence de la politique de sécurité de l'information et de la protection des renseignements personnels par le biais du programme d'accueil organisationnel;
- Engage le nouvel employé au respect de cette dernière politique en lui faisant signer un formulaire d'engagement qui est consigné au dossier de l'employé. Cette politique est également rendue disponible à tout le personnel de l'organisation via l'Intranet organisationnel;
- Est responsable des enquêtes en cas de non-conformités décelées et de l'application des sanctions associées à cette présente procédure, en collaboration avec les gestionnaires des utilisateurs visés ou les supérieurs immédiats des gestionnaires et/ou médecins visés ainsi que le responsable de la PRP, le cas échéant;
- Assure l'application de la présente procédure dans son service concerné.

9.2 Direction médicale et des services professionnels

- Informe tout nouveau membre du CMDPSF de l'existence de la politique cadre de gouvernance des renseignements personnels et des renseignements de santé et de services sociaux ;
- Engage le nouveau membre du CMDPSF au respect de cette dernière politique en lui faisant signer un formulaire d'engagement qui est consigné au dossier du membre. Cette politique est également rendue disponible aux médecins et dentistes de l'organisation via l'Intranet organisationnel;
- Est responsable des enquêtes en cas de non-conformités décelées et de l'application des sanctions associées à cette présente procédure;

9.3 Les utilisateurs

- S'assurent de respecter les engagements à la confidentialité à l'égard des renseignements personnels [Feuillet d'information - Engagement de confidentialité à l'égard des | d... -](#);
- Répondent avec honnêteté et au meilleur de leur mémoire, aux questions qui leur sont adressées par l'Établissement en lien avec les motifs d'accès et d'utilisation des DUFE.

9.4 Le pilote du DUFE (l'auditeur)

- S'assure que tous les utilisateurs des systèmes sont informés de l'existence et du contenu de la présente procédure;
- Documente les audits réalisés avec les rapports d'événements journalisés, par dossier individuel;
- Compile l'information nécessaire à l'application de la présente procédure;
- Archive l'information de façon sécuritaire dans le répertoire informatique prévu à cet effet;
- Avise son gestionnaire de toute anomalie potentielle liée à un usage inapproprié lors de l'analyse d'un événement et consigne l'information à même le fichier d'audit de journalisation;

- Avise immédiatement son gestionnaire de toute anomalie détectée dans les rapports de journalisation susceptible d'être médiatisée ou de porter atteinte à la réputation de l'Établissement;
- Réalise les audits et en effectue le suivi aux périodes déterminées.

9.5 Cadre responsable du DUFE (gestionnaire d'un auditeur)

- Sensibilise son personnel et ses nouveaux employés à la présente procédure et en rappelle régulièrement l'importance;
- Assure la compilation de la documentation de l'audit ainsi que la complétion du fichier d'audit de journalisation dûment complété par son auditeur;
- Analyse et révise les anomalies détectées lors de la journalisation par l'auditeur;
- Communique les constats et les non-conformités relevés à l'issue de son analyse au gestionnaire de l'utilisateur visé ainsi qu'à l'équipe des relations de travail;
- Assure le suivi de la conclusion de la non-conformité avec l'agent des relations de travail et en cas de sanctions appliquées, effectue le suivi du dossier avec son auditeur dans les délais établis;
- Veille à l'application de la présente procédure au sein de son propre service;
- Avise immédiatement la Direction de la qualité, de l'innovation, de la performance et de l'éthique ou tout service qui lui a été désigné de toute anomalie détectée dans les rapports de journalisation susceptible d'être médiatisée ou de porter atteinte à la réputation de l'Établissement;

9.6 Gestionnaire de l'utilisateur

- S'assure d'une gestion rigoureuse des accès aux RP-RS pour le personnel sous son autorité;
- Veille à ce que son personnel et ses nouveaux employés soient informés et régulièrement sensibilisés à l'importance de leurs responsabilités concernant la protection des RP et RS;
- Applique les modalités prévues dans la présente procédure;
- En collaboration avec l'agent aux relations de travail à la DRH attitré à l'utilisateur visé, assure la rencontre de ce dernier afin de valider la non-conformité détectée;
- Soutien et assure le suivi de la sanction appliquée par les relations de travail en lien avec la gravité de l'écart de confidentialité, si tel est le cas.

9.7 Direction de la qualité, de l'innovation, de la performance et de l'éthique

- Assure une vigie de l'application de la présente procédure et de son mécanisme de journalisation par l'ensemble des directions concernées de l'Établissement;
- Effectue le suivi de la performance des audits de journalisation au sein de l'organisation;
- Communique et diffuse les résultats d'audits de journalisation au sein de l'organisation;
- Le responsable de la PRP assure la mise en place et le suivi du cadre législatif entourant la confidentialité et la protection des renseignements personnels. Il assume ainsi un rôle-conseil pour soutenir la prise de décision concernant une violation de la confidentialité, en s'appuyant sur les décisions arbitrales pertinentes et les principes qui ressortent de la jurisprudence;
- Avise immédiatement la Direction générale (DG) de toute anomalie détectée dans les rapports de journalisation susceptible d'être médiatisée ou de porter atteinte à la réputation de l'Établissement;

9.8 Directions cliniques - Soutien à la pratique professionnelle (soins infirmiers, services multi-disciplinaires, services médicaux et professionnels)

- Collabore avec la DRH lorsque la violation de la confidentialité concerne un professionnel faisant partie d'un ordre professionnel et assure la déclaration auprès du syndic de l'ordre professionnel, le cas échéant.

10. MÉCANISMES DE SUIVI

La réalisation des audits de journalisation des accès au DUFE sera suivi au moyen d'un calendrier de suivi (voir annexe 4 pour exemple).

Les résultats sommaires et dénominalisés des audits seront publiés et remis chaque trimestre à la suite des audits effectués aux personnes suivantes:

- Cadre responsable du DUFÉ;
- Conseiller-cadre PRP;
- Comité de concertation des directeurs adjoints;
- Comité de direction.

L'Établissement envisage procéder annuellement à l'évaluation de la conformité des mécanismes de journalisation ainsi que de l'efficacité des mesures de sécurité mises en place pour assurer la protection des renseignements qu'il détient. Le cas échéant, il révisera ces mécanismes et ces mesures.

La liste des différents accès octroyés aux DUFÉ concernés continuera d'être validée avec les gestionnaires d'utilisateurs et les actions requises d'ajustement, de maintien ou de retrait des accès seront actualisées.

6. Liste des annexes

ANNEXE A – Aide-mémoire pour le gestionnaire de l'utilisateur visé – lors d'écarts relevés suite à un audit

ANNEXE B – Exemple de fichier d'audit de journalisation (exemple)

ANNEXE C – Exemple de communication destinée au gestionnaire de l'utilisateur visé lors d'écarts relevés suite à un audit

ANNEXE D – Exemple de calendrier de suivi des audits de journalisation

ANNEXE E – La démarche de journalisation organisationnelle

7. Références

S.O.

8. Historique		
Processus d'élaboration		
Rédigé par	Hélène Jean-Baptiste, coordonnatrice accueil et archives, DPSCS	2026-03-11
Consultation(s)	Marie-Josée Lalonde, cheffe, archives médicales, DPSCS	2026-04-15
	Sandra Tremblay, cheffe, archives médicales, DPSCS	2026-04-15
	Maude Lefebvre, cheffe, archives médicales, DPSCS	2026-04-15
	Martin Berthelot, cheffe, archives médicales, DPSCS	2026-04-15
	Marie-Ève Tremblay-Gauthier, pilote, DMÉ, DPSCS	2026-04-15
	Patricia Horvath, pilote DMÉ, DPSCS	2026-04-15
	Annie Paquin, pilote DMÉ, DPSCS	2026-04-15
	Gabriel Trépanier, conseiller-cadre PRP, DQIPE	2026-05-04
	Stéphanie Truchon, cheffe du service des relations de travail par intérim, (DRHDOA)	2026-04-13
	Nicolas Poissant-Gilbert, chef de service transformation et santé numérique, DQIPE	2026-05-04
	Mariana Contasel, cheffe de secteur transformation et santé numérique, DQIPE	2026-06-05
	Dre Dominique Dupuis, chef adjointe du département de médecine spécialisée, Pôle 2	2026-05-04
	Dre Ariane Courville-Le Bouyonnec, médecin spécialisée en médecins de famille	2026-05-04
	Audrée Leboeuf, coordonnatrice clinico-administrative, DACCESS	2026-05-04
	Lucette Robert, directrice DPSCS	2026-05-20
	Martin Turcotte, directeur adjoint, DPSMD	2026-05-20
	Dre Caroline Bourassa-Fulop, DMSP	2026-06-15
	Christelle Robert, coordonnatrice aux activités cliniques et pratiques professionnelles en soins infirmiers, DSIEU	2026-05-20
	Dre Cynthia Landry, DMSPa	2026-05-22
	Catherine Besner, DSMSSS, Chef de service – développement et évolution des pratiques	2026-05-20
	Emilie Laberge, coordonnatrice de l'accueil, l'orientation, l'intégration et du développement et transformation (DSIEU)	2026-05-20
	Elisabeth Picard, DQIPE, chef de service gestion de la qualité et des risques DSHAPPA-DSSADG	2026-06-02
	Sophie Comman, DQIPE, adjointe à la directrice	2026-06-05
	Annie Tremblay, APPR, DPDR	2026-06-18
Instance(s) de consultation		
Instance(s) consultative(s)	Service des affaires juridiques	2026-09-03
Historique du document		
Recommandé par	Comité de concertation des directeurs adjoints	2026-08-19
Adopté par	Comité de direction	2026-09-22
Commentaires		

ANNEXE A

Aide-mémoire pour le gestionnaire de l'utilisateur visé – lors d'écarts relevés suite à un audit

Merci de prendre la version de l'outil de travail « Aide-mémoire pour le gestionnaire de l'utilisateur visé lors d'écarts relevés suite à un audit » disponible sur Intranet.



Aide-mémoire pour le gestionnaire de l'utilisateur visé - lors d'écarts de confidentialité relevé suite à un audit de journalisation

MARCHE A SUIVRE

1. Le gestionnaire de l'auditeur (cadre responsable de l'actif informationnel et/ou cadre responsable de l'audit) contacte le gestionnaire de l'utilisateur visé par l'audit et lui remet la (les) non-conformité(s) détectée(s) quant à un usage inapproprié. Le gestionnaire de l'auditeur place l'équipe des relations de travail (RT) en copie.
2. Le gestionnaire de l'utilisateur visé **analyse** les écarts (maximum 15 jours calendrier) – **sans l'employé**.
3. Le gestionnaire de l'utilisateur confirme ou infirme la (les) non-conformité(s) détectée(s) à l'équipe des RT. Un résumé des faits et écarts est également transmis.
 - a. Advenant que le gestionnaire n'est pas en mesure d'analyser l'ensemble des écarts se rapportant aux usages inappropriés décelés, il doit convenir du déroulement de la démarche à adopter avec les RT pour consulter l'utilisateur visé avant de confirmer/infirmer les non conformités détectées.
4. Advenant que des anomalies soient constatées (confirmation d'un usage inapproprié), l'équipe des RT accompagne le gestionnaire dans la préparation d'une rencontre avec l'utilisateur visé.
5. Le gestionnaire de l'utilisateur visé et l'équipe des RT rencontrent l'utilisateur visé pour recueillir sa version des faits et consignent le tout dans le dossier spécifique protégé de l'utilisateur visé.
6. L'équipe des RT finalise l'analyse du dossier et transmet les avis ou les lettres à remettre à l'utilisateur visé, le cas échéant. Advenant la nécessité, des sanctions disciplinaires pourront être entreprises auprès de l'utilisateur visé fautif.
 - a. Si l'utilisateur visé par la mesure fait partie d'un ordre professionnel, les non-conformités quant à un usage inapproprié seront transmises également au chef de service des RT. Ce dernier aura à entreprendre des démarches avec la direction soutien en pratique professionnelle (DSI, DSM, DSPEUPC) concernée afin qu'ils déterminent la nécessité de faire une déclaration au Syndic de l'ordre professionnel. Le cas échéant, la direction soutien en pratique professionnelle procède à la déclaration avec les informations fournies par la chef des RT.
7. Le gestionnaire de l'utilisateur visé fait une rétroaction au cadre responsable de l'audit du résultat de l'analyse des écarts relevés.
8. Le cadre responsable de l'audit ou l'auditeur consigne le résultat dans le « *Fichier d'audit de journalisation* ».
9. Advenant la confirmation d'un usage inapproprié, l'auditeur ou le cadre responsable de l'audit avise le responsable de la protection des renseignements personnels (PRP).
10. Le responsable PRP analyse et peut contacter les RT ou le gestionnaire de l'utilisateur visé afin de vérifier si on doit faire une divulgation à la Commission d'accès à l'information ;
11. L'utilisateur visé sera audité pendant deux périodes, les étapes précédentes s'appliqueront à nouveau.

Important

Les étapes 1 à 9 doivent être faites dans un délai de 30 jours calendrier.

Il est très important de faire ces étapes. Pour les RT, il sera difficile d'intervenir si des mesures administratives doivent être appliquées et que les délais n'ont pas été respectés.

Même si vous avez la qualité et les fonctions pour recevoir l'information, la notion de nécessité doit prévaloir.

ANNEXE B
Fichier d'audit de journalisation (exemple)

Journalisation													
Date	Demandeur	Utilisateur	Logiciel	Bris O/N	# Dossiers concernés	Avis RH	Nbre transaction	Nbre non conformes			Divulgaration CAI	Préjudice	Commentaire
								Raison 1- Professionnel non impliqué dans le continuum de soins	une autre fin que la prestation de soins/services	Raison 3- Consultation de son propre dossier ou d'un tiers relié			

ANNEXE C

Communication destinée au gestionnaire de l'utilisateur visé lors d'écarts relevés suite à un audit (exemple)

Bonjour,

Les archives médicales communiquent avec vous aujourd'hui dans le cadre d'un audit portant sur les accès et l'utilisation des dossiers d'utilisateurs conservés en format numérique, soit dans le dossier médical électronique (DMÉ) organisationnel (MYLE) ou dans le DCI HarrisFlex.

La démarche vise à assurer la conformité aux règles de confidentialité et à l'utilisation appropriée du

☐ Dossier médical électronique ou du ☐ Dossier clinique informatisé organisationnel.

Validations déjà effectuées par les pilotes

Lors de cet audit, les validations suivantes de la conformité des accès ont déjà été effectuées par les pilotes applicatifs:

- Est-ce qu'une action a été posée par l'utilisateur au moment de l'accès:
 - Ajout/modification d'un rendez-vous;
 - Indexation d'un document pdf;
 - Vérification de messages / tâches;
 - Confirmation de la présence à un rendez-vous;
 - Ajout d'une note;
 - Etc
- Est-ce que l'utilisateur a effectué des recherches avec un nom similaire (afin d'éliminer la possibilité d'une erreur de recherche) à la date à laquelle l'accès a eu lieu;
- Est-ce que l'utilisateur avait un des soins et/ou services (rendez-vous, admission, etc.) prévus à la date à laquelle l'accès a eu lieu;
- Est-ce que l'utilisateur ayant accédé au dossier de l'utilisateur se retrouve parmi les contacts/membre de la famille inscrits dans le dossier dudit usager.

Malgré ces validations, la conformité de l'accès demeure à déterminer.

Ce qui est attendu

À titre de gestionnaire de l'utilisateur concerné par cet audit (**Insérer le nom de l'utilisateur ici**) votre rôle est essentiel. Nous sollicitons donc votre collaboration afin de :

- Prendre connaissance de la situation;
- Effectuer les validations requises (**sans l'employé(e)**);
- Validez que les accès réalisés étaient justifiés dans le cadre des fonctions exercées dans les **15 jours** suivants l'envoi de la présente communication;

Voici les détails nécessaires à la réalisation de ces vérifications :

➤ **Insérer le tableau de journalisation des accès ici**

ANNEXE C (suite)

Communication destinée au gestionnaire de l'utilisateur visé lors d'écarts relevés suite à un audit (exemple)

Prochaines étapes

Nous joignons à notre envoi, un aide-mémoire à utiliser pour les prochaines étapes à suivre:

2. Le gestionnaire de l'utilisateur visé **analyse** les écarts (maximum 15 jours calendrier) – **sans l'employé**.
3. Le gestionnaire de l'utilisateur confirme ou infirme la (les) non-conformité(s) détectée(s) à l'équipe des RT. Un résumé des faits et écarts est également transmis.
 - a. Advenant que le gestionnaire n'est pas en mesure d'analyser l'ensemble des écarts se rapportant aux usages inappropriés décelés, il doit convenir du déroulement de la démarche à adopter avec les RT pour consulter l'utilisateur visé avant de confirmer/infirmer les non conformités détectées.
4. Advenant que des anomalies soient constatées (confirmation d'un usage inapproprié), l'équipe des RT accompagne le gestionnaire dans la préparation d'une rencontre avec l'utilisateur visé.

A) S'il s'avère que l'accès au dossier de l'utilisateur était justifié, SVP nous en aviser. Prendre note qu'il est possible que l'accès découle d'une erreur d'utilisateur (ex: employé(e) voulait accéder au dossier d'un utilisateur ayant les mêmes noms et prénoms).

B) S'il s'avère que l'accès au dossier de l'utilisateur n'était pas justifié ou si vous avez de la difficulté à identifier les raisons pouvant justifier l'accès sans en parler avec l'employé(e), vous devez contacter l'équipe des relations de travail au moyen du formulaire suivant : [Demande d'accompagnement RT](#).

Cette communication n'aurait pas dû vous être adressée

Si jamais ce courriel aurait dû être envoyé à un autre gestionnaire que vous, svp bien vouloir lui faire suivre en mettant l'expéditeur en copie conforme (cc).

Des questions ?

Si vous avez besoin de davantage d'informations sur la journalisation des accès de l'employé(e) concerné(e), vous pouvez un(e) des pilotes suivant(es):

DMÉ organisationnel	Marie-Ève Tremblay-Gauthier Annie Paquin Patricia Horvath
DCI HarrisFlex	À compléter

Nous vous remercions de votre collaboration et demeurons disponibles pour toute question ou précision supplémentaire.

Merci

ANNEXE D

Exemple de calendrier de suivi des audits de journalisation

Audits en grappe						Période auditée		Auditeur
Mois	DUFÉ	Prévu	Réalisé	Unité de soins auditée	Type audit	Début	Fin	
Janvier		Oui	✓ Réalisé					
Février		Oui	✓ Réalisé					
Mars		Oui	✓ Réalisé					
Avril		Oui	✓ Réalisé					
Mai		Oui	⚠ En retard					
Juin		Oui						
Juillet		Non						
Août		Non						
Septembre		Oui						
Octobre		Oui						
Novembre		Oui						
Décembre		Oui						

ANNEXE E
La démarche de journalisation organisationnelle

