Dossier Collaboratif Santé

Livre blanc sur la sécurité et la protection de la vie privée

Document confidentiel à diffusion restreinte

TELUS Santé

Table des matières

Contexte

TELUS Solutions en santé inc. (ci-après nommée « TELUS ») s'emploie à améliorer l'accès aux soins de santé et l'expérience des usagers pour les fournisseurs de services médicaux et leurs patients. Les solutions numériques de TELUS en matière de soins de santé permettent de sécuriser la chaîne de renseignements médicaux protégés à toutes les étapes des soins aux patients. Pour maintenir la confiance de ces derniers, il est essentiel d'aider les fournisseurs de services médicaux à respecter leurs obligations en matière de protection de la vie privée.

Assurer la sécurité et la confidentialité des renseignements médicaux personnels (RMP) dans le système de Dossier Collaboratif Santé (DCS) est une responsabilité partagée entre TELUS, ses fournisseurs d'infrastructure et de services et ses utilisateurs cliniques. TELUS est responsable de l'hébergement, de la gestion et de la protection des RMP dans l'application au nom des fournisseurs de soins de santé. En tant que propriétaires et contrôleurs de ces données, les fournisseurs de soins sont quant à eux responsables du respect des exigences légales et réglementaires de chaque territoire de compétence où ils exercent leurs activités relativement à la collecte, à l'utilisation et à la divulgation de renseignements personnels.

TELUS encourage tous ses clients à réaliser une évaluation indépendante des facteurs relatifs à la vie privée (ÉFVP) avant de mettre en place un système de DCS ou d'apporter des changements importants aux flux de données. Les ÉFVP constituent une méthode efficace pour évaluer et gérer les risques d'atteinte à la vie privée associés à un logiciel ou à un service, et sont légalement requises dans certains territoires de compétence.

Ce document est conçu pour vous aider à réaliser vos propres évaluations des facteurs relatifs à la vie privée en :

1. Vous donnant un aperçu du cadre de protection de la vie privée et du logiciel de DCS de TELUS.
2. Définissant clairement les rôles et les responsabilités de TELUS en tant que fournisseur du logiciel.
3. Définissant clairement les rôles et les responsabilités des fournisseurs de services médicaux et des propriétaires de cliniques.
4. Proposant des pistes de solution et des conseils pour répondre aux questions sur les ÉFVP.

Dossier Collaboratif Santé (DCS)

Le DCS représente une solution de santé numérique unique et complète à partir de laquelle tout fournisseur de services médicaux peut gérer sa pratique. Il combine un dossier médical électronique (DME), un dossier de santé personnel (DSP) et des solutions de gestion de pratique en ligne pour répondre aux besoins des grands fournisseurs de services médicaux comme des petits cabinets indépendants. Il offre une gamme complète d'outils de collaboration, de gestion participative du patient, d'automatisation et d'optimisation des données qui peuvent être personnalisés en fonction de la pratique et des parcours cliniques de chaque fournisseur de services médicaux.

Outils

Visites virtuelles

Différentes options de communication sécurisée avec les patients, par vidéo, audio ou texte.

Consignation des données

Modèles personnalisables grâce auxquels les utilisateurs peuvent lier des variables courantes de l'historique du patient à des notes, évitant ainsi la saisie de données redondantes.

Gestion des demandes de consultation et des listes d'attente

Outils de gestion des demandes de consultation qui s'intègrent aux processus de travail des organisations et permettent d'inscrire les patients sur des listes d'attente filtrables et de soumettre des questionnaires automatisés aux patients triés.

Questionnaires

Questionnaires intégrés pour l'accueil et le suivi des patients, qui permettent également la création d'outils capables de produire des données de haute qualité en plus de favoriser la collaboration avec le patient.

Calendrier intégré

Puissant système de calendrier pour l'organisation des rendez-vous et des visites de suivi ou l'analyse des résultats.

Fonctions de facturation privée et publique

Plateforme de facturation intégrée qui permet la production de factures et de reçus ainsi que le rapprochement des comptes de patients.

Portail des patients

Outil pleinement intégré à la plateforme permettant la communication avec les patients via un portail sécurisé, grâce auquel ils peuvent accéder à leurs dossiers, notes, réservations en ligne et messages de l'organisation

Tiers fournisseurs de services

Des tiers fournisseurs de services (ou sous-traitants) sont appelés à fournir des fonctions modulaires au sein d'une solution de DCS intégrée.

Avant toute chose, ces fournisseurs sont soumis au processus de diligence raisonnable de TELUS en matière de sécurité et de protection de la vie privée. La chaîne de possession des renseignements médicaux personnels est sécurisée au moyen de mesures techniques et contractuelles.

Les contrats d'emploi et de sous-traitance liés au DSC comprennent des dispositions relatives à la protection et à l'utilisation appropriée des renseignements confidentiels (y compris les renseignements personnels des clients et des patients) auxquels ont accès les employés et les sous-traitants de TELUS. S'il y a lieu, TELUS prendra les mesures disciplinaires appropriées pour faire respecter la confidentialité des données.

De plus, TELUS s'est dotée d'un Code de conduite à l'intention des fournisseurs qui définit ses attentes à l'égard de tous les fournisseurs affiliés à ses services et solutions. Pour garantir le respect, par les fournisseurs, de leurs obligations en matière de sécurité et de protection de la vie privée, ceux-ci sont soumis à des examens périodiques s'inscrivant dans une approche fondée sur le risque et axée sur les pratiques de gestion de la qualité.

La protection de la vie privée chez TELUS

Responsabilisation

TELUS s'engage auprès des fournisseurs de services médicaux à protéger tout renseignement personnel de clients ou de patients en sa possession, y compris les renseignements transférés par TELUS à ses fournisseurs de services à des fins de traitement. La responsabilité, le contrôle et la propriété des renseignements personnels des clients et des patients ainsi que le pouvoir décisionnel afférent reviennent toutefois aux fournisseurs de services médicaux.

La responsabilité globale de la gestion de la protection de la vie privée à TELUS se situe au plus haut niveau de l'organisation, soit le conseil d'administration de TELUS Corporation.

Bureau du chef des données et des relations de confiance de TELUS

TELUS s'est dotée d'un chef des données et des relations de confiance pour superviser le bureau responsable de ces questions. Le rôle du Bureau du chef des données et des relations de confiance consiste à offrir un programme de gestion de la protection de la vie privée, spécialement conçu pour protéger les renseignements personnels des clients des fournisseurs de services médicaux. Le Bureau doit aussi établir des politiques et des procédures pour gagner et conserver la confiance de ces fournisseurs à l'égard de nos pratiques de traitement des données.

Les fondements du programme global de protection de la vie privée de TELUS sont définis par le cadre de gestion des renseignements personnels de l'entreprise. Ce document-cadre énonce les engagements liés à notre programme de protection de la vie privée. Il précise également certains des moyens par lesquels nous veillons à concrétiser ces engagements, et la structure organisationnelle que nous avons mise en place à cette fin.

Utilisation secondaire des données

Sauf autorisation expresse de votre part, TELUS utilisera les données générées par votre utilisation du DCS uniquement pour permettre la mise en œuvre de vos services médicaux numériques.

Évaluation de la sécurité et de la confidentialité des données

TELUS effectue des évaluations pour la conception ou la modification de produits, de services, d'initiatives, de processus et de systèmes impliquant l'accès aux données, leur collecte, leur stockage, leur utilisation ou leur divulgation.

Formation et sensibilisation

Tous les membres du personnel de TELUS, y compris les contractuels, doivent suivre avec succès une formation sur la sécurité et la protection de la vie privée lorsqu'ils se joignent à TELUS et périodiquement par la suite. Les personnes disposant d'autorisations privilégiées reçoivent une formation supplémentaire sur la sécurité propre à leur rôle.

Le contenu des formations sur la protection de la vie privée est mis à jour chaque année.

Surveillance, vérifications et contrôles

Surveillance de la conformité

En tant que dispositif médical conforme à la norme ISO 13485:2016, le DCS fait l'objet d'une certification indépendante ainsi que d'un rapport annuel SOC 2 portant sur la disponibilité, la confidentialité et les contrôles de sécurité.

Le programme de surveillance de la conformité de TELUS comprend l'évaluation régulière des unités d'affaires selon un ensemble d'indicateurs de conformité établis par le Bureau du chef des données et des relations de confiance.

Le Bureau exerce des fonctions de surveillance et produit régulièrement des rapports sur la conformité de TELUS à ses politiques, normes et procédures de protection de la vie privée.

TELUS ne détermine et ne certifie pas les obligations de conformité de ses clients.

Collecte des données de vérification et contrôle de l'accès des utilisateurs.

Toute activité logicielle est consignée à la fois dans l'application et dans les environnements hébergés. Les rapports d'activité ne peuvent pas être modifiés, ce qui établit une base de référence formelle pour les enquêtes informatiques judiciaires sur les systèmes.

Dans le DCS, les utilisateurs administratifs du fournisseur de services médicaux peuvent générer des rapports d'activité par utilisateur ou par dossier de santé. TELUS n'effectue pas de vérifications proactives des activités, mais elle recommande aux fournisseurs de services médicaux d'examiner périodiquement l'activité des utilisateurs dans leurs comptes de DCS et peut les aider à configurer la production des rapports pertinents.

Collecte, utilisation et divulgation des données

Collecte et utilisation

Tous les renseignements figurant dans le DCS sont sous la garde de TELUS et ne servent qu'à fournir les services du DCS, à moins d'une demande et d'une autorisation expresse de votre part.

Consentement et avis

Comme TELUS n'a aucune relation directe avec vos clients et patients, nous comptons sur vous pour vous assurer que les exigences de votre territoire de compétence en matière de consentement et de transmission d'avis sont respectées pour la collecte, l'utilisation et la divulgation des renseignements sur les patients.

Éléments de données

Voici une liste des types de renseignements médicaux personnels pouvant être recueillis, utilisés ou divulgués lors de l'utilisation du DCS de TELUS :

Éléments de données liés à l'enregistrement

Élément	Objectif de la collecte, de l'utilisation ou de la divulgation
Numéro d'assurance maladie	Identifier le patient et faire le suivi des services médicaux reçus
Nom du patient	Identifier le patient
Date de naissance	Identifier le patient
Sexe	Identifier le patient
Identité de genre	Identifier le patient
Adresse de courriel	Communiquer avec le patient
Numéro de téléphone	Communiquer avec le patient
Adresse du patient	Communiquer avec le patient
Nom d'une personne à joindre en cas d'urgence	Identifier la personne à joindre en cas d'urgence
Numéro de téléphone de la personne à joindre en cas d'urgence	Communiquer avec cette personne
Lien entre la personne à joindre et le patient	Identifier la personne à joindre en cas d'urgence
Médecin traitant	Identifier le médecin traitant du patient
Médecin de famille	Identifier le médecin de famille du patient
Médecin demandeur	Identifier le médecin demandeur du patient
Notes administratives	Planifier et gérer les services

Éléments de données liés au diagnostic, au traitement ou aux soins

Élément	Objectif de la collecte, de l'utilisation ou de la divulgation
Signes vitaux	Fournir des soins au patient
Résultats des derniers tests en laboratoire	Fournir des soins au patient
Notes de progression	Fournir des soins au patient
Médicaments actifs	Fournir des soins au patient
Vaccins et immunisation	Fournir des soins au patient
Allergies	Fournir des soins au patient
Demandes de consultations	Fournir des soins au patient
Formulaires (p. ex. une demande de test en laboratoire)	Fournir des soins au patient
Documents provenant d'autres fournisseurs de services médicaux ou d'une banque de données médicales	Fournir des soins au patient
Rendez-vous	Traiter, vérifier et rembourser les demandes de remboursement soumises par les fournisseurs de services médicaux aux régimes provinciaux d'assurance maladie ou aux assureurs privés concernés
Questions et réponses	Collecte normalisée d'informations auprès du patient
Pharmacie habituelle	Gérer les ordonnances
Antécédents sociaux (tabagisme, consommation d'alcool, profession, etc.)	Informer le fournisseur de services médicaux de problèmes potentiels

Éléments de données liés à la facturation et aux paiements

Élément	Objectif de la collecte, de l'utilisation ou de la divulgation
Assureur du patient, identifiant d'assurance, numéro de groupe, régime provincial	Traiter, vérifier et rembourser les demandes de remboursement soumises par les fournisseurs de services médicaux aux régimes provinciaux d'assurance maladie ou aux assureurs privés concernés

Cette liste n'est pas exhaustive et chaque instance de DCS peut être personnalisée par les fournisseurs de services médicaux en fonction de tout élément de données pertinent pour leur pratique.

Divulgation

TELUS peut transmettre des renseignements personnels à des fournisseurs de services responsables de certaines fonctions du DCS. Nous prenons des mesures de contrôle contractuelles pour nous assurer que tous les renseignements transmis à nos fournisseurs de services sont protégés selon les mêmes normes que celles décrites dans la Politique sur la protection des renseignements personnels des clients d'affaires de TELUS.

En tant que fournisseur de services médicaux, vous pouvez divulguer des renseignements par l'entremise de nos services pour la prestation de soins (traitements, demandes de consultation, communication avec d'autres professionnels de la santé et facturation), conformément aux lois et règlements sur la protection de la vie privée de votre territoire de compétence.

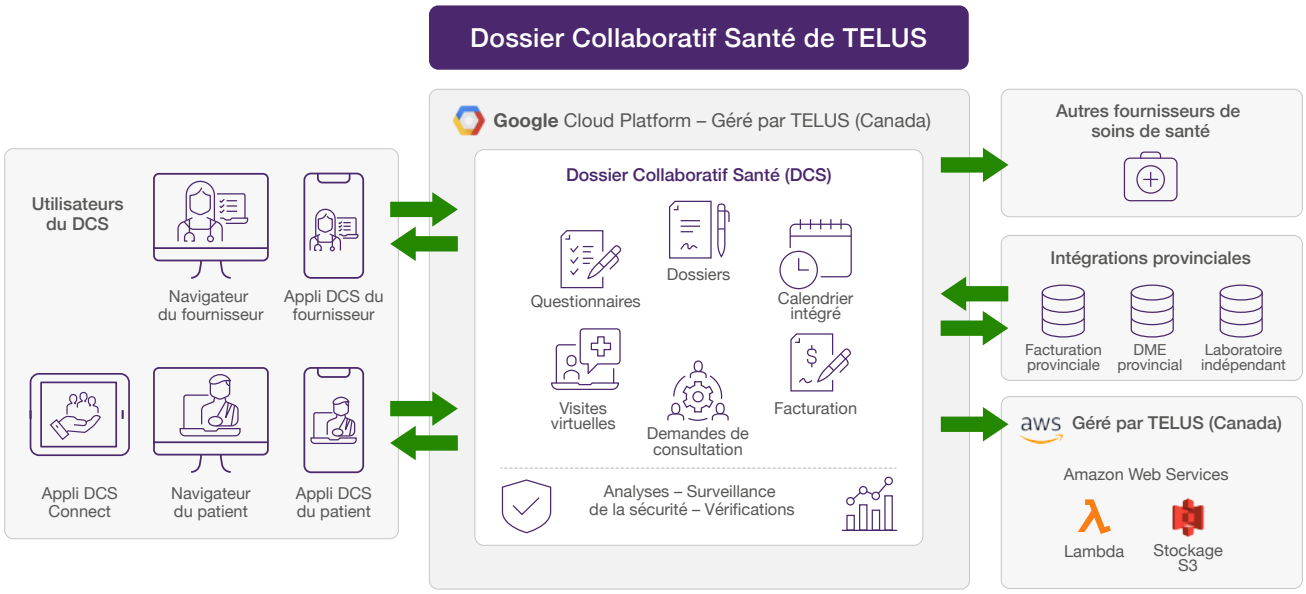
Analyse du flux d'information

Une analyse du flux d'information comprend généralement un tableau et un diagramme décrivant clairement la circulation des données dans le DCS aux différentes étapes du processus de soins. Elle établit également l'autorité légale pour la collecte, l'utilisation et la divulgation de ces données. Le tableau et le diagramme ci-dessous fournissent un libellé pouvant être modifié au besoin en fonction des processus de votre clinique et des autorités légales de votre territoire de compétence.

Tableau de flux d'information

N°	Description	Type de renseignement	Objectif
1	Le fournisseur de services médicaux (FSM) recueille les caractéristiques démographiques et les coordonnées auprès du patient ou du soignant.	Données d'enregistrement	Collecte et utilisation : Inscription du patient à la clinique, au DCS et au portail; création d'un profil et d'un dossier de patient; communication avec le patient au besoin.
2	Le FSM recueille des renseignements tout au long du traitement et des soins auprès du patient et du soignant	Diagnostic, traitement et soins	Collecte et utilisation : Prestation de services médicaux au patient.
3	Le FSM recueille des renseignements médicaux auprès d'un autre fournisseur de soins.	Diagnostic, traitement et soins	Collecte et utilisation : Réception de demandes de consultation et communication avec les autres membres de l'équipe soignante.
4	Le FSM transmet des renseignements médicaux à un autre fournisseur de soins.	Diagnostic, traitement et soins	Divulgation : Envoi de demandes de consultation et communication avec les autres membres de l'équipe soignante
5	FSM recueille des renseignements relatifs à la couverture d'assurance médicale auprès du patient ou du soignant.	Facturation et paiement	Collecte et utilisation : Remboursement
6	Le FSM soumet la facture des services fournis à l'assureur du patient.	Facturation et paiement Diagnostic, traitement et soins	Divulgation : Détermination ou vérification de l'admissibilité à un service médical; remboursement.
7	Le FSM communique avec le centre d'assistance du DME.	Tous types (inscription; diagnostic, traitement et soins; facturation et paiement)	Divulgation et utilisation : Soutien technique et dépannage.
8	Le centre d'assistance du DME de TELUS fournit du soutien.	Tous types (inscription; diagnostic, traitement et soins; facturation et paiement)	Collecte : Soutien technique et dépannage.
9	Une déclaration ou une réclamation est soumise sous forme électronique à la Commission des accidents du travail (CAT).	Données d'enregistrement Diagnostic, traitement et soins	Divulgation : Rapport obligatoire auprès de la CAT. Utilisation : Obtention ou traitement du paiement des services médicaux (gestion interne).
10	Le FSM accède aux renseignements médicaux du patient dans un système d'information sur la santé partagé.	Données d'enregistrement Diagnostic, traitement et soins	Collecte : Consultation, copie, téléchargement ou transcription des RMP du patient à partir d'une base de données provinciale ou fédérale sur la santé.
11	Le FSM fournit des renseignements à des organismes publics provinciaux ou fédéraux.	Données d'enregistrement Diagnostic, traitement et soins	Divulgation : Divulgation par intégration technique aux bases de données provinciales ou fédérales sur la santé.
12	Le FSM effectue des analyses.	Diagnostic, traitement et soins	Utilisation : Amélioration de la pratique; assurance qualité; planification.

Diagramme de flux d'information



Contrôle d'accès

L'accès à toutes les données dont TELUS a la garde est géré selon les principes du « besoin de savoir » et du « moindre accès ». Cela signifie que l'accès est accordé uniquement aux personnes qui ont besoin de l'information pour accomplir leur travail, et que leur accès est limité à la plus petite quantité d'information nécessaire. Par exemple, un agent de soutien technique peut avoir accès à plus de renseignements que son superviseur, puisque ce dernier n'a pas besoin d'accéder à des données détaillées sur les clients pour accomplir son travail.

Dans le contexte de la santé, notons que les privilèges d'accès des fournisseurs de soins médicaux doivent être accordés de façon à minimiser tout effet négatif sur la sécurité et les soins fournis aux patients. Cela signifie que les contrôles d'accès administratifs, comme les normes de pratique professionnelle et les règlements des collèges, la formation et les politiques internes jouent un rôle plus important que les restrictions d'accès techniques.

Toute entité responsable d'autoriser l'accès à des renseignements personnels doit avoir une politique de contrôle afin de garantir des processus clairs et cohérents pour l'octroi et le retrait des droits d'accès dans le cadre des processus d'intégration et de départ du personnel.

Les fournisseurs de soins médicaux sont responsables de gérer l'accès à leur compte de DCS par toutes les personnes de leur domaine clinique. Le tableau ci-dessous présente un cadre d'accès qui peut être modifié au besoin. Les propriétaires de compte de DCS sont responsables de la personnalisation des rôles en fonction des exigences particulières de leur pratique.

Poste	Rôle de l'utilisateur	Type d'accès (lecture, écriture, modification)	Renseignements auxquels l'utilisateur peut accéder
Directeur de clinique / propriétaire de DME	Administrateur	Ajout, modification, suppression de profils d'utilisateurs	Données du FSM (profils démographiques, renseignements professionnels, données de formation, coordonnées personnelles, etc.)
Médecin	Utilisateur	Lecture, écriture, modification	Enregistrement des patients; diagnostics, traitements et soins; facturation et paiements
Infirmière praticienne	Utilisateur	Lecture, écriture, modification	Enregistrement des patients; diagnostics, traitements et soins; facturation et paiements
Autre FSM / fournisseur de services paramédicaux	Utilisateur	Lecture, écriture, modification	Enregistrement des patients; diagnostics, traitements et soins; facturation et paiements
Aide de bureau	Soutien administratif	Lecture, écriture, modification Ajout, modification, suppression de profils d'utilisateurs	Enregistrement des patients; diagnostics, traitements et soins; facturation et paiements
Fournisseur de services informatiques ou de gestion de l'information	Assistance technique et maintenance du système	Lecture, écriture, modification Ajout, modification, suppression de profils d'utilisateurs Modification du système	Profils démographiques (nom complet, no d'assurance maladie, no de téléphone, adresse, etc.) Diagnostics et traitements

Sécurité

Nos contrôles de sécurité de l'information correspondent aux normes fondées sur le risque en vigueur dans le secteur, de sorte à protéger les fournisseurs de services médicaux contre les menaces du monde réel. Ils sont revus chaque année et mis à jour en fonction de l'évolution des menaces.

Les contrôles de sécurité appliqués au DCS sont à la hauteur de la sensibilité des renseignements médicaux personnels conservés sur la plateforme. TELUS s'engage contractuellement auprès des fournisseurs de soins médicaux à maintenir des contrôles de sécurité raisonnables, appropriés et adaptés à la nature sensible de ces renseignements.

Responsabilité et reddition de compte

Le chef de la sécurité de TELUS Santé est responsable de déterminer et d'atténuer les risques de sécurité. Le personnel de sécurité est séparé des activités d'exploitation et relève de la haute direction, tandis que l'équipe chargée de la conformité du DCS vérifie les pratiques de sécurité à l'interne.

Formation

Tous les membres du personnel de TELUS reçoivent une formation sur les pratiques de sécurité au moment de leur intégration et chaque année par la suite. Les personnes disposant d'autorisations privilégiées reçoivent une formation supplémentaire sur la sécurité propre à leur rôle.

Sécurité physique et responsabilité partagée concernant l'infrastructure

Nos services logiciels sont hébergés dans un nuage privé, à l'intérieur d'une infrastructure de centre de données gérée par les principaux fournisseurs mondiaux de services infonuagiques. Cette infrastructure allie évolutivité, efficacité par rapport au coût et possibilité de régionalisation à des fins de résidence des données. L'infrastructure-service et les plateformes-services sont gérées selon un modèle de responsabilité partagée avec ces tiers fournisseurs de services infonuagiques. La sécurité physique est gérée par les fournisseurs d'infrastructure et comprend les contrôles environnementaux (accès physique, incendie, eau, inondation, etc.) et techniques (sécurité du réseau, chiffrement des lecteurs, etc.). TELUS demeure responsable de la gestion des ressources virtualisées dans ces environnements hébergés. La responsabilité partagée des fournisseurs d'infrastructure est contrôlée au moyen de vérifications annuelles (rapport SOC 2 et norme ISO27001).

Chiffrement des données

Toutes les données des cliniques sont chiffrées tout au long de leur cycle de vie, y compris en transit (TLS) et au repos (AES). Au repos, les données sont chiffrées sur le lecteur, dans le répertoire ainsi que la base de données applicable.

Sauvegarde, reprise après sinistre et continuité des activités

Les bases de données des cliniques sont protégées au moyen de sauvegardes en continu conservées dans une infrastructure de centre de données physiquement distincte. Les sauvegardes sont testées périodiquement et font l'objet de tests annuels de continuité des activités.

Authentification multifacteur

Notre logiciel prend en charge l'authentification multifactorielle par message texte, courriel ou application tierce, comme Google Authenticator ou 1Password. De plus, les contrôles d'accès peuvent être configurés pour l'authentification unique via SAML 2.0.

Contrôle des changements et cycle de vie du développement logiciel

Le cycle de vie du développement logiciel de TELUS est soumis à la norme ISO 13485:2016 relative aux systèmes de gestion de la qualité. Les pratiques de conception et de développement sont documentées de manière exhaustive, avec des exigences spécifiques pour la documentation de soutien. Les pratiques de gestion des changements sont régies par des contrôles détaillés des versions intégrant des mesures d'assurance de la qualité.

Contrôle des accès

Notre logiciel prend en charge les autorisations granulaires avec des options d'accès basées sur les utilisateurs ou les rôles. Des fonctions de verrouillage et de surveillance sont disponibles au moyen de la personnalisation de la configuration des autorisations.

Sécurité du réseau

L'instance du logiciel de chaque clinique est accessible sur internet via une URL publique. L'accès à l'infrastructure de production fondamentale est limité aux utilisateurs privilégiés du DCS et se fait par l'entremise d'un réseau privé virtuel sécurisé et d'un serveur intermédiaire.

Tests d'intrusion et gestion des vulnérabilités

Nos services sont soumis à des tests d'intrusion périodiques effectués par des tiers. Les vulnérabilités sont triées dans le cadre des pratiques de développement de chaque logiciel et sont corrigées ou atténuées en fonction d'un ordre de priorité fondé sur les risques.

Journalisation et surveillance

Toute l'activité du logiciel est enregistrée, y compris l'utilisation directe et les modifications apportées à l'infrastructure de production fondamentale. Dans le DCS, les utilisateurs administratifs peuvent générer des rapports d'activité par utilisateur ou par dossier médical.

Le DCS est surveillé par des agents de sécurité applicative hébergée, qui détectent et signalent les menaces en temps réel. Les bases de données sur les menaces sont mises à jour à partir de bases de données tierces qui recensent les menaces connues.

Nos outils et pratiques de développement logiciel font l'objet de vérifications internes périodiques.

Nous joindre

Les demandes de renseignements et les plaintes concernant la manière dont TELUS ou ses fournisseurs de services médicaux traitent les renseignements médicaux personnels des clients et des patients peuvent être soumises de manière confidentielle à notre chef des données et des relations de confiance à l'adresse privacyhealth@telus.com. TELUS a mis en place des procédures de traitement de toutes les demandes et les plaintes concernant sa gestion des renseignements médicaux personnels.

TELUS a également mis en place des procédures de traitement des demandes et des plaintes concernant la gestion des renseignements personnels par TELUS Santé et Solutions de paiement (TSSP).

ANNEXE A

Aperçu de la conformité

Les contrôles de confidentialité et de sécurité de TELUS sont gérés, normalisés, testés et vérifiés à l'externe afin de protéger les renseignements médicaux personnels.

Les efforts de conformité internes de TELUS couvrent la confidentialité des données, la sécurité et la gestion de la qualité, conformément aux exigences réglementaires, de vérification et contractuelles. Nos logiciels sont par ailleurs soumis à des processus de certification, à des normes et à des examens indépendants rigoureux :

- SOC 2 Type II – disponible pour le DCS, pour les clients actuels et potentiels
- ISO 13485 (dispositifs médicaux) – certification pour le DCS
- Tests d'intrusion – effectués au moins une fois par an
- DME certifié par OntarioMD – DCS

Nos services sont assurés en vertu des polices d'assurance de TELUS, qui comprennent une couverture complète en matière d'erreurs, d'omissions et de cyber-responsabilité.

Dossier Collaboratif Santé

Livre blanc sur la sécurité et la protection de la vie privée

TELUS Santé