Collaborative Health Record

Privacy and security white paper

Confidentiality and restricted use

TELUS® Health

Table of contents

Background

TELUS Health Solutions Inc. (hereinafter referred to as “TELUS”) is dedicated to providing better healthcare experiences and improved access to healthcare for Health Service Providers (HSPs) and their patients. TELUS digital healthcare solutions support a secure chain of protected health information throughout all stages of patient care. A vital part of maintaining patient trust is to support our HSPs in meeting privacy obligations.

Ensuring the safety and confidentiality of Personal Health Information (PHI) in the Collaborative Health Record (CHR) system is a shared responsibility between TELUS, our infrastructure and service providers, and our clinical users. TELUS is responsible for storing, managing and protecting PHI within the application on behalf of HSPs. As the owner and controller of the data, HSPs are accountable for ensuring compliance with the legislative and regulatory requirements in each jurisdiction in which they operate for the collection, use and disclosure of personal information.

TELUS encourages all clients to perform independent Privacy Impact Assessments (PIAs) prior to implementing the CHR and upon any material change to the flow of data. PIAs are an effective method of assessing and addressing privacy risks associated with a software or service, and are legally required in some jurisdictions.

The purpose of this document is to support you in completing your own privacy assessments by:

1. Providing an overview of the TELUS privacy framework and CHR software

2. Clearly defining the roles and responsibilities of TELUS as the software vendor

3. Clearly defining the roles and responsibilities of HSPs and clinic owners

4. Providing language and guidance for responding to specific PIA questions

Collaborative Health Record (CHR)

The CHR offers a single, comprehensive digital health solution from which any HSP can run their practice. It combines an electronic medical record (EMR), personal health record (PHR) and online health practice management solutions to accommodate both enterprise healthcare service providers and smaller, independent practices. The CHR offers a full suite of tools for collaboration, patient engagement, automation and data optimization that can be customized based on the needs of each HSP's practice and preferred clinical pathways.

Tools

Virtual visits

Various options for secure communication with patients via video, audio or text.

Charting

Customizable templates where users can connect common patient history variables directly into notes, avoiding redundant data entry.

Referrals and waitlist management

Built-in referral management functionalities work with the organization's workflows. Patients are assigned to filterable waitlists and triaged patients are sent automated questionnaires.

Questionnaires

Integrated questionnaires can be used for onboarding and patient follow-up, and to build tools that can produce high-quality data while engaging with patients in their healthcare journey.

Integrated calendar

A powerful scheduling system to organize appointments and follow-up visits or to review results.

Private and public billing functionalities

The integrated billing platform generates bills, produces invoices and receipts, and reconciles patient accounts.

Patient portal

Integrated patient communication functionality is an integral component of the platform. Through a secure portal, patients can access their files, notes, online booking and messages sent from the organization.

Third-party service providers

The CHR leverages various third-party service providers, also known as sub-processors, to deliver modular functionality within an integrated solution.

Third party service providers are subject to TELUS privacy and security due diligence prior to integration with the CHR. Technical and contractual measures are applied to establish a secure chain of custody for PHI.

CHR employment and contractor agreements include contractual provisions for the safeguarding and proper usage of confidential information (including client/patient personal information) accessible to TELUS employees and contractors. TELUS will take appropriate disciplinary measures where necessary to enforce customer confidentiality.

In addition, TELUS has established a Supplier Code of Conduct that outlines our expectations for all suppliers affiliated with our services and solutions. Periodic supplier reviews are performed through a risk-based approach to monitor compliance with privacy and security obligations, with a focus on quality management practices.

Privacy at TELUS

Accountability

At TELUS we are responsible to HSPs for client/patient personal information in TELUS' possession, including information that has been transferred for processing by TELUS to its service providers. However, the ultimate responsibility, control, ownership and decision-making authority with respect to client/patient personal information rests with HSPs.

Overall accountability for privacy management at TELUS resides at the highest level of the organization, the TELUS Corporation board of directors.

TELUS Data and Trust Office

TELUS has appointed a chief data and trust officer to oversee the TELUS Data and Trust Office (DTO). The DTO is responsible for maintaining an accountable privacy management program specifically designed to protect the privacy of our HSPs end-users, and for setting policies and procedures to earn and maintain our HSPs trust in our data handling practices.

The key components of TELUS' overarching privacy program are set out in our Privacy Management Program Framework. The framework documents our core program commitments to protecting privacy. The framework also sets out some of the ways in which we have operationalized those commitments and the organizational structure we have implemented to do so.

Secondary use of data

Unless specifically authorized by you, TELUS will only use data generated through your use of the CHR to enable your digital health services.

Privacy and security assessments

TELUS conducts assessments for the design of, or changes to, products, services, initiatives, processes and systems that involve access to, collection, storage, use or disclosure of data.

Training and awareness

All TELUS personnel, including contractors, must successfully complete privacy and security training when joining TELUS and on a periodic basis thereafter. Individuals with privileged permissions receive additional role-specific security training.

Privacy training content is updated annually.

Privacy compliance monitoring, audit and enforcement

Compliance monitoring

The CHR is subject to third-party certification as a medical device under ISO 13485:2016 as well as annual SOC2 reporting for availability, confidentiality and security controls.

TELUS' Compliance Monitoring Program measures business units on a regular basis against a set of key compliance indicators established by the DTO.

The DTO is responsible for regular monitoring and reporting on TELUS' compliance with its privacy policies, standards and procedures.

TELUS does not determine or otherwise certify the compliance obligations of its customers.

Audit logging and user access monitoring

All software activity is logged both within the application and within hosted environments. Audit logs cannot be altered, establishing a formal baseline for forensic system investigations.

Within the CHR, HSP administrative users can generate activity reports by user or health record. While TELUS does not proactively perform activity audits, we recommend that HSPs perform periodic reviews of user activity within their CHR accounts and TELUS can support setup and configuration of relevant reporting.

Collection, use and disclosure

Collection and use

All information entered into the CHR is in the custody of TELUS and will only be used to provide CHR services, unless specifically requested and authorized by you.

Consent and notification

As TELUS does not have a direct relationship with your clients/patients, we rely on you to ensure consent and notification requirements in your jurisdiction have been met for the collection, use and disclosure of patient information.

Data elements

The following is a list of the types of PHI that may be collected, used or disclosed while using the TELUS CHR:

Registration data elements

Element	Purpose for collection, use or disclosure
Personal health number (PHN)	Uniquely identifies the patient. Used to track health services.
Name of patient	Identifies patient
Date of birth	Identifies patient
Sex	Identifies patient
Gender identity	Identifies patient
Email address	Method of contact
Phone number	Method of contact
Address of patient	Method of contact
Emergency contact's name	Identifies patient's emergency contact.
Emergency contact's phone number	Method of contact
Emergency contact's relationship to patient	Identifies patient's emergency contact.
Primary practitioner	Identifies the patient's primary practitioner.
Family doctor	Identifies the patient's family doctor.
Referring practitioner	Identifies the patient's referring practitioner.
Administration notes	Scheduling services

Diagnosis, treatment and care data elements

Element	Purpose for collection, use or disclosure
Vitals	Patient care
Latest lab results	Patient care
Progress notes	Patient care
Active medications	Patient care
Vaccines / immunizations	Patient care
Allergies	Patient care
Referrals	Patient care
Forms (e.g., laboratory requisitions)	Patient care
Documents received from other healthcare providers or health data repositories	Patient care
Appointments	To process, verify and reimburse claims healthcare providers submit for payment to the relevant provincial health insurance plans or private health insurance providers.
Questionnaires and responses	Standardized collection of information from patients.
Preferred pharmacy	Prescription management
Social history (smoking, alcohol, occupation)	Inform provider of potential concerns.

Billing and payment data elements

Element	Purpose for collection, use or disclosure
Patient's insurance company, insurance ID, group number, provincial plan	To process, verify and reimburse claims healthcare providers submit for payment to the relevant provincial health insurance plans or private health insurance providers.

Disclosure

TELUS may share personal information with our service providers, who are contracted to perform services or functions on our behalf in associating with delivery of the CHR application. We use contractual controls to ensure all information disclosed to our service providers is protected to the same standard as described in the TELUS B2B Privacy Policy.

As an HSP, you may disclose information through our services for the provision of care (treatment, referrals, consultations with other HSPs and billing) and as authorized by the privacy legislation in your jurisdiction.

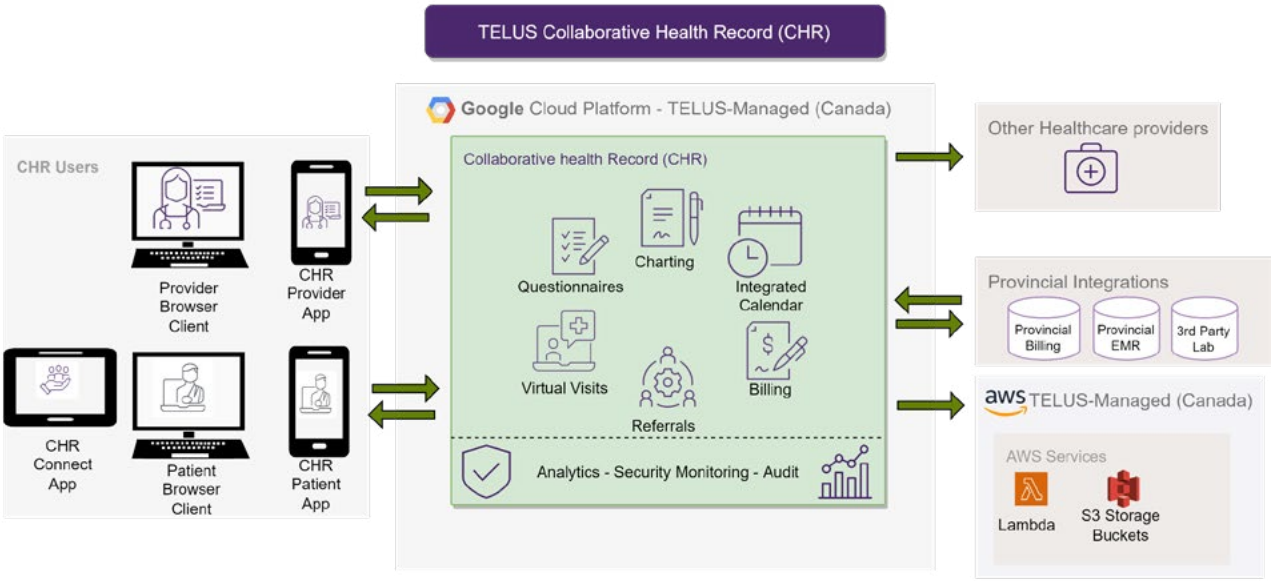
Information flow analysis

An information flow analysis typically includes an information flow table and diagram and is meant to clearly describe the movement of information in the CHR throughout different stages of care as well as the legal authority for the collection, use and disclosure of that information. The information table and diagram below provide some suggested language that can be modified, as needed, to reflect the process in place at your clinic and the legislative authorities in your jurisdiction.

Information flow table

#	Description	Type of information	Purpose
1	HSP collects demographic details and contact information from the patient or caregiver.	Registration information.	Collection and use: Enrolling patients in the clinic, CHR and patient portal; creation of a patient profile and chart; contacting patient as required.
2	HSP collects information throughout the course of treatment and care from patient or caregiver.	Diagnostic, treatment and care information.	Collection and use: Providing health services to the patient.
3	HSP collects medical information from another provider.	Diagnostic, treatment and care information.	Collection and use: Receiving referrals and for consultation with other members of the care team.
4	HSP discloses medical information to another HSP.	Diagnostic, treatment and care information.	Disclosure: Sending referrals and for consultation with other members of the care team.
5	HSP collects insurance and coverage information from patient or caregiver.	Billing and payment.	Collection and use: Reimbursement.
6	HSP submits invoice for services provided to patient insurance provider.	Billing and payment Diagnostic, treatment and care information.	Disclosure: Determining or verifying the eligibility of an individual to receive a health service; reimbursement.
7	HSP contacts EMR help desk.	All (registration; diagnostic treatment and care; billing and payment).	Disclosure and use: Technical support and troubleshooting.
8	TELUS EMR help desk provides support.	All (registration; diagnostic treatment and care; billing and payment).	Collection: Technical support and troubleshooting.
9	WCB e-injury reporting and claims.	Registration information. Diagnostic treatment and care information.	Disclosure and use: Required WCB reporting; obtaining or processing payment for health services (internal management purposes).
10	HSP accesses patient information stored in shared health information systems.	Registration information Diagnostic treatment and care information.	Collection: Viewing, copying, downloading or transcribing patient PHI available via integration with provincial or federal health information databases.
11	HSP provides information to provincial or federal public bodies.	Registration information Diagnostic treatment and care information.	Disclosure: Disclosure via technical integration with provincial or federal health information databases.
12	HSP performs analytics.	Diagnostic treatment and care information.	Use: Practice improvement; quality assurance; planning.

Information flow diagram



Access control

Access to all data in the custody of TELUS is provided based on the principles of 'need to know' and 'least access', meaning that access is granted to individuals that require the information to perform their role, and their access is restricted to the least amount of the information necessary. For example, a technical support agent may have access to more information than their supervisor given that the supervisor does not require access to detailed client data in order to perform their role.

In the healthcare context, it is notable that HSP access privileges should be granted with a view to minimizing negative impacts to patient care and safety. This means that administrative access controls (such as professional practice standards and college bylaws), training and internal policies play a larger role than technical access restrictions.

Any entity responsible for provisioning access to personal information should maintain an access control policy to ensure a clear and consistent processes for provisioning and deprovisioning access as part of the onboarding and offboarding process for staff.

HSPs are accountable for managing access to their CHR account by all individuals within the clinical CHR domain. The table below is a sample access framework that can be modified as needed. CHR account owners are responsible for customizing roles according to their particular practice requirements.

Position/ job title	User role	Type of access (read, write, edit)	Description of information this user can access
Clinic manager / EMR owner	Administrator	Add/edit/delete users	HSP information including demographic, professional, academic and personal contact information.
Physician	User	Create/write/edit	Patient registration; diagnosis, treatment and care; billing and payment.
Nurse practitioner	User	Create/write/edit	Patient registration; diagnosis, treatment and care; billing and payment.
Other HSP / allied health	User	Create/write/edit	Patient registration; diagnosis, treatment and care; billing and payment.
Medical office assistant	Admin support	Create/write/edit Add/edit/delete users	Patient registration; diagnosis, treatment and care; billing and payment.
IM/IT provider	Technical support and system maintenance	Create/write/edit Add/edit/delete users System modifications	Demographic information (e.g., full name, PHN, phone number, address). Diagnostic, treatment.

Security

Our information security controls follow risk-based industry standards to protect against real-world threats targeting PHI. Security controls are reviewed on an annual basis and updated as required to reflect the evolving threat climate.

The security controls applied to the CHR reflect the sensitivity of the PHI held within the platform. TELUS establishes contractual commitments with healthcare providers that we use reasonable and appropriate security controls, reflective of the sensitive nature of Personal Health Information.

Responsibility and accountability

The TELUS Health chief security officer is responsible for the identification and mitigation of security risks. Security personnel are segregated from operations and accountable to executive leadership. The CHR's compliance team provides internal auditing of security practices.

Training

All TELUS personnel are trained on security practices during on-boarding and on an annual basis thereafter. Individuals with privileged permissions receive additional role-specific security training.

Physical security and shared responsibility on infrastructure

Our software services are hosted within a virtual private cloud (VPC) within data center infrastructure managed by leading global cloud providers. This infrastructure combines scalability, cost-effectiveness, and the ability to regionalize for data residency purposes. Both infrastructure-as-a-service and platforms-as-a-service are managed through a shared responsibility model with these third-party cloud providers. Physical security is managed by infrastructure providers, including environmental (e.g. physical access controls, fire, water, flood) and technical controls (e.g. network security, disk encryption). TELUS remains responsible for managing virtualized resources within these hosted environments. Shared responsibility of infrastructure providers is monitored via annual SOC2 and ISO27001 auditing.

Encryption

All clinic data is encrypted throughout the lifecycle, including both in transit (TLS) and at rest (AES). At rest, data is encrypted on the disk, within the container, and within the applicable database.

Backup, disaster recovery and business continuity

The clinic databases are protected with rolling back-ups held within physically disparate data center infrastructure. Back-ups are tested periodically and subject to annual business continuity tests.

Multi-factor authentication

Our software supports multi-factor authentication through SMS, Email, or third-party applications like Google Authenticator or 1Password. In addition, access controls can be configured for single sign-on via SAML 2.0.

Change control and software development lifecycle

TELUS's software development life cycle is subject to ISO 13485:2016 Quality Management Systems (QMS). Design and development practices are comprehensively documented with associated requirements for supporting documentation. Change management practices are governed within detailed QMS release controls, including quality assurance practices.

Access control

Our software supports granular permissions with options for both user-based or role-based access. Functionality for lock-boxes and glass-breaking is available through customization of the permissions configuration.

Network security

Each clinic's software instance is accessible on the internet via public-URL. Access to back-end production infrastructure is limited to privileged CHR users through a secured VPN connection and intermediary jump server.

Penetration testing and vulnerability management

Our services undergo periodic third-party penetration testing. Vulnerabilities are triaged within each software's development practices and remediated or mitigated according to risk-based prioritization.

Logging and monitoring

All software activity is logged, including both front-end usage as well as any changes made to back-end production infrastructure. Within the CHR, administrative users can generate activity reports by user or by health record.

The CHR is monitored by hosted application security agents to identify and alert threats in real-time. Threat databases are updated with third party databases of known threat profiles.

Our software development tools and practices are subject to internal periodic internal audits.

Contacting us

Inquiries or complaints about the manner in which TELUS or its HSPs treat client/patient PHI can be forwarded on a confidential basis to our chief data and trust officer at privacyhealth@telus.com. TELUS maintains procedures for addressing and responding to all inquiries or complaints about TELUS' handling of PHI.

TELUS maintains procedures for addressing and responding to all inquiries or complaints about THPS's handling of Personal Information.

APPENDIX A

Compliance overview

TELUS privacy and security controls are managed, standardized, tested and externally audited to protect personal health information.

TELUS internal compliance efforts span privacy, security and quality management systems in accordance with regulatory, audit and contractual requirements. In addition, our software is subject to rigorous third-party accreditations, standards and reviews:

- SOC2 Type II - available for the CHR to existing and prospective clients
- ISO 13485 (medical devices) - certified for the CHR
- Penetration testing - performed at least annually
- OntarioMD certified EMR - CHR

Our services are insured under TELUS policies, including comprehensive errors and omissions as well as cyber-liability coverage.

Collaborative Health Record

Privacy and security white paper

TELUS® Health