RAPIDS

Privacy and Security

White Paper

Version: April 29, 2025

Contents

Document Purpose

The purpose of this document is to support you, whether you work in a primary care or disability management setting, in completing your own privacy assessments by:

1. Providing an overview of the RAPIDS guidance service
2. Clearly defining the roles and responsibilities of TELUS as the service provider
3. Clearly defining the roles and responsibilities of healthcare providers and disability management organizations
4. Providing language and guidance for responding to specific Privacy Impact Assessment (PIA) questions

RAPIDS and TELUS

TELUS Health Solutions Inc. (TELUS) has partnered with RAPIDS Health Ltd., (RAPIDS) a technology and service provider of guidance for healthcare practitioners (HCPs) for their consideration as they diagnose, treat, and mitigate the symptoms of psychiatric conditions.

TELUS is dedicated to providing better healthcare experiences for healthcare providers (HCPs) and their patients. The RAPIDS guidance service offered by TELUS supports a secure chain of protected health information throughout all stages of patient care. A vital part of maintaining patient trust is to support our HCPs and disability management organizations in meeting their privacy obligations.

RAPIDS, in keeping with the TELUS Supplier Code of Conduct, must respect the privacy of our customers and team members, and be demonstrably accountable for personal information entrusted to them by TELUS, including personal information the supplier collects or creates for TELUS. Suppliers must collect, use and disclose personal information only as directed by TELUS or required by law. Our suppliers must assist TELUS in meeting privacy obligations set out in applicable laws, contracts and TELUS' own high privacy standards. This includes facilitating access requests and fulfilling other individual rights, informing TELUS of actual or suspected data breaches, supporting TELUS responses to inquiries, complaints and investigations, implementing effective retention processes and ensuring the responsible, appropriate and accountable use of Artificial Intelligence (AI) in accordance with the TELUS Trust Model. Supplier's AI must be explainable, transparent and avoid unintended harms and bias. Our suppliers must do everything reasonable to support TELUS in living up to the commitments made in the TELUS Privacy Commitment and the TELUS Business Privacy Policy and similar policies when applicable.

The RAPIDS Service

RAPIDS is a clinical decision support service that provides psychiatric guidance, in the form of a written report, to healthcare practitioners for their consideration. The RAPIDS clinical rules engine processes patient information and provides guidance on diagnosis and treatment personalized to each patient.

RAPIDS guidance is informed by the authoritative guide to the assessment and diagnosis of mental disorders (DSM-5-TR), validated clinical scales, peer-reviewed treatment guidelines, and the latest high-quality empirical research. We provide evidence-based biopsychosocial treatment options personalized to the patient, including the top-3 pharmacological treatment options, considering tolerability, and actionable medication guidance. RAPIDS provides comprehensive guidance for mood (major depressive disorder, bipolar disorder) and anxiety disorders, insomnia and ADHD and general guidance for substance use disorders and obesity.

A general overview of the RAPIDS service follows:

1. The referrer e.g. an HCP or a case manager, provides written acceptance of the then-current privacy statement and terms of use for the RAPIDS service.

2. The referrer identifies an individual for whom a RAPIDS assessment would be beneficial.

3. The referrer explains the RAPIDS assessment process to the individual and obtains necessary consent from them to participate in a RAPIDS assessment and to be contacted by the RAPIDS team.

4. The referrer completes the RAPIDS referral form and sends it to RAPIDS by eFax.

5. RAPIDS uses the email provided by the referrer to send the individual a secure link which is used to obtain consent for collection of data directly from them and provides an electronic means of completing the appropriate psychiatric questionnaires.

6. The patient completes the online psychiatric questionnaires.

7. RAPIDS processes the data from the referrer and the individual, and generates a Guidance Report, which is delivered to the referrer within days of the individual completing the psychiatric questionnaires. If the referrer is not the patient's clinician, e.g. a case manager, then they forward the report to the clinician.

8. The clinician reviews the RAPIDS Guidance Report and formulates their treatment plan.

Privacy at TELUS

Who is accountable for privacy at TELUS?

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 clients, and for setting policies and procedures to earn and maintain our client's trust in our data handling practices. The DTO is responsible for regular monitoring and reporting on TELUS' compliance with its privacy policies, standards and procedures. 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.

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

What framework is used to manage privacy at TELUS?

The key components of TELUS' overarching privacy program are set out in our Privacy Management Program Framework (https://www.telus.com/en/about/privacy/management-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. As part of this framework, 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.

How are TELUS employees kept up to date on privacy principles, policies and legislation?

All TELUS personnel, including contractors, must successfully complete privacy and security training when joining TELUS and on an annual basis thereafter. Individuals with privileged permissions receive additional role-specific security training. Privacy training content is updated annually.

RAPIDS, in its role as a supplier to TELUS and in accordance with the TELUS Supplier Code of Conduct, aligns with this privacy management framework and has appointed a privacy officer to be accountable for ensuring privacy and data risk management measures are in place.

Privacy is a shared responsibility between TELUS, our clients, and our suppliers.

How is responsibility for the protection of the Personal Health Information (PHI) of patients participating in RAPIDS shared among TELUS, its vendors and clients?

Ensuring the safety and confidentiality of the PHI in providing the RAPIDS service follows a Shared Responsibility Model between:

a) TELUS,

b) our infrastructure and service providers, including RAPIDS Health Ltd., and

c) our clients, e.g. HCPs and case managers.

TELUS and RAPIDS are responsible for storing, managing and protecting PHI within RAPIDS on behalf of its clients. As the owner and controller of the data, clients of RAPIDS 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 subscribing to the RAPIDS service 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.

Who is the data custodian of the PHI collected for RAPIDS?

HCPs who use the RAPIDS service are the data custodians. TELUS is responsible to HCPs for the protection of patient PHI in our possession, including information that has been transferred for processing by TELUS to its service providers. However, as custodians, the ultimate responsibility, control, ownership and decision-making authority with respect to client/patient personal information rests with HCPs.

Organizations who provide disability management services who use RAPIDS are typically not data custodians; however, they act as data controllers and are accountable to protect PHI and abide by applicable legislation. As with our HCP clients, TELUS is responsible to these organizations to protect the patient PHI that is in our possession.

How does TELUS ensure that its third-party service providers are diligent regarding privacy and security?

TELUS and RAPIDS utilize third party applications and platforms, including Google Cloud, Jotform, CHR, and SR Fax. Any third party integration that involves the processing of patient data must adhere to strict TELUS PIAs, which mandate full Canada-only data residency of all PHI/PII data and compliance with PIPEDA, PHIPA, and equivalent provincial regulations. Additionally, third party providers must have appropriate Role-Based Access Controls (RBACs), resource-access logging and auditing facilities, perform regular penetration testing, and ensure that all data handling meets acceptable encryption strategies. They are also required to undergo a TELUS-led risk assessment and address all medium or higher priority findings.

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

Third party compliance is monitored as follows:

a) TELUS 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.

b) TELUS undertakes regular compliance and security reviews.

c) TELUS will take appropriate disciplinary measures where necessary to enforce customer confidentiality.

d) TELUS has established a Supplier Code of Conduct that outlines our expectations for all suppliers affiliated with our services and solutions.

e) 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.

How does TELUS ensure that its customers are diligent regarding privacy and security?

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

Privacy at RAPIDS

What certifications does the RAPIDS clinical decision tool have?

RAPIDS is subject to third-party certification as a medical device under ISO 13485:2016 (Class 1). Processors used by RAPIDS provide annual SOC2 reporting for availability, confidentiality and security controls.

Which RAPIDS team members have access to PHI?

Access to PHI data is restricted to those who need the information to perform their job duties, and their access is limited to only what is necessary. This is in accordance with the principles of ‘need to know’ and ‘least privilege’.

The following lists the roles of the people at RAPIDS with access to PHI:

- Customer Service Managers can set up and monitor case workflow.
- Case Reviewers can read and update guidance reports for quality control/clinical review purposes.
- IT Platform support team members can only access production for implementation and production related issues during a 24-hour window period and only with audited access.

Security at RAPIDS

How does RAPIDS monitor access to PHI?

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. Standard Operating Policies exist to ensure only authorized users have access to the RAPIDS system.

How is RAPIDS insured?

Our services are insured under TELUS and RAPIDS Health Ltd. policies, including comprehensive errors & omissions and cyber-liability coverage.

How do RAPIDS ensure the security of the data it processes?

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 RAPIDS 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.

How does RAPIDS encrypt data?

RAPIDS data is fully encrypted at rest and in transit. Data in transit is encrypted using TLS/SSL. Encryption at rest is performed with multiple layers of AES.

How does RAPIDS ensure the physical security of its 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.

How does RAPIDS back up data?

The RAPIDS 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.

How does RAPIDS authenticate the users who access data?

Our platform supports multi-factor authentication through SMS, Email, or third party applications like Google Authenticator or PingID, Okta.

What security scanning and testing does RAPIDS undertake?

Scanning and Testing measures for the RAPIDS platform include:

- Build-time Container Scanning
- Run-time Container Scanning
- Protection against Distributed Denial of Service (DDoS) and other web-based attacks.
- Centralized login gateway access.
- OWASP TOP-10: Adherence to the top 10 web application security risks identified by the Open Web Application Security Project.
- Penetration Testing performed annually
- Static Code Analysis
- Live Threat Detection
- Automated Library Updates
- Zero-Production Access Policy
- Automated Security Tests per build

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

What procedure does the software development lifecycle at RAPIDS follow?

The software development life cycle employed for the RAPIDS software platform aligns with 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.

Data Collection and usage at RAPIDS

How is patient consent for the RAPIDS service obtained?

Referrers who direct individuals to RAPIDS must obtain verbal consent to share their contact information with us; this consent is documented on the RAPIDS referral form completed by the referrer.

Upon receipt of a RAPIDS referral form, a member of the RAPIDS team will connect digitally with the patient to obtain their written consent for the collection, use and disclosure of their PHI. Although RAPIDS does obtain written, informed consent from the patient, 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.

What data does RAPIDS collect?

The following is a list of the types of PHI that may be collected, used or disclosed while using RAPIDS as well as the reason for its collection:

Demographic and Contact Information Elements

Element	Purpose for collection, use or disclosure
Personal Health Number or unique ID	Uniquely identifies the patient. Used to track services
Name of individual	Identifies individual
Date of birth	Identifies individual
Sex at Birth	Identifies individual
Email address	Method of contact
Phone Number	Method of contact
Referring practitioner name	Identifies the individual’s referring practitioner.
Referring practitioner address	Method of contact
Referring practitioner email	Method of contact
Referring practitioner fax	Method of contact
Referring practitioner language preference	Clinician’s Language preference

Diagnosis, treatment and care data elements

Element	Purpose for collection, use or disclosure
Height	Input for guidance service

Weight	Input for guidance service
Clinical Area of Concern	Input for guidance service
Psychometric Questionnaires & Responses	Input for guidance service
Current Medications with dosage, toleration and reason for use	Input for guidance service
Past Medications with reason for discontinuation	Input for guidance service
Recreational substance use (alcohol, cannabis, psychedelics, opioids, stimulants)	Input for guidance service
Pregnancy status (current or planning to be) and/or breastfeeding status	Input for guidance service

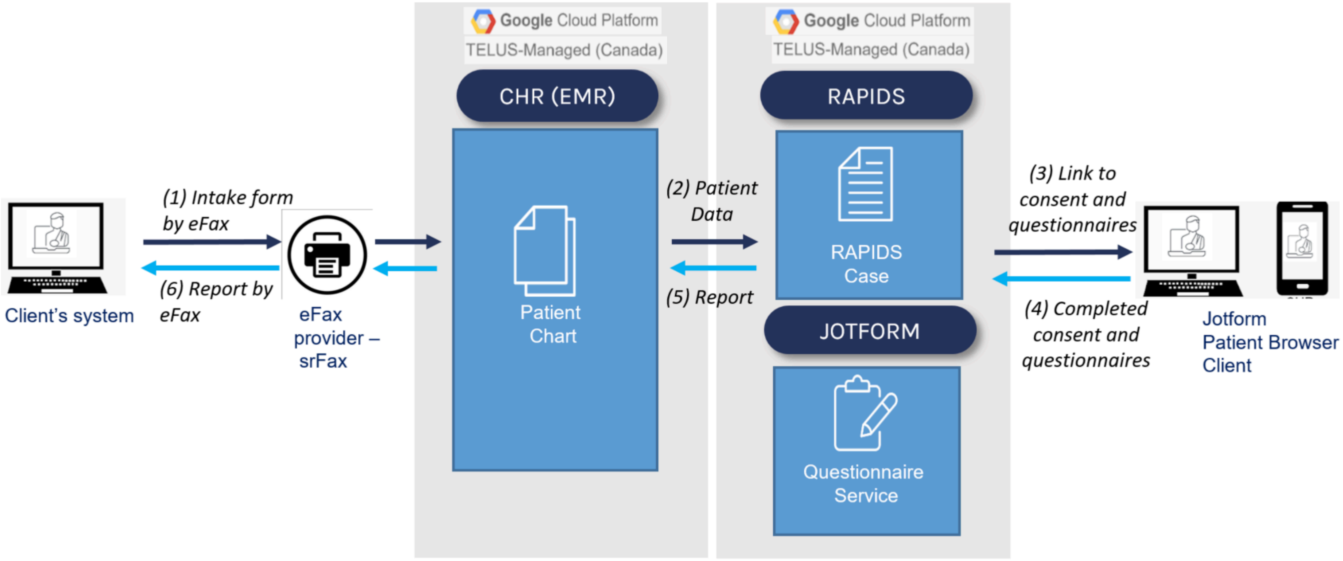
Does RAPIDS use the PHI that it collects for secondary purposes?

Unless specifically authorized by you, and the individual/patient TELUS and RAPIDS Health Ltd will only use data collected by you and processed by RAPIDS to enable the RAPIDS guidance services.

How does the data flow between the referrer, the patient and RAPIDS?

To assist you in your own PIA, we have created an information flow analysis; these typically include an information flow table and diagram and are meant to clearly describe the movement of information in RAPIDS throughout different stages of the service. 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.

Data Flow



Information Flow Table

#	Description	Type of information	Purpose
1	Referrer informs the individual about the RAPIDS guidance service and requests consent to share their information as part of the service	RAPIDS service description and need for consent	CONSENT to collect, use and disclose the individual's data to RAPIDS
2	The individual's demographic details are auto-populated into the RAPIDS Intake form from the individual's chart or manually completed by the referrer.	Demographic information.	COLLECTION Data collection as part of the RAPIDS referral process.

3	Referrer collects information about the individual's symptoms and current and past medications and adds them to the RAPIDS Intake form.	Diagnostic and treatment information.	COLLECTION Data collection as part of the RAPIDS referral process.
4	Referrer discloses intake information to the RAPIDS team by submitting the RAPIDS intake form.	Demographic, diagnostic, and treatment.	DISCLOSURE Disclosure of data as part of RAPIDS referral process.
5	RAPIDS team uses information provided in the RAPIDS intake form to create a patient chart in the RAPIDS EMR.	Demographic information.	COLLECTION Data collection as part of the RAPIDS referral process.
6	RAPIDS team uses contact information provided in the RAPIDS intake form to send the individual a link to complete a consent form and a series of psychiatric questionnaires.	Individual contact information.	COLLECTION & USE RAPIDS team uses individual's contact for data collection as part of the RAPIDS referral process.
7	The individual uses a link to complete the consent form and the psychiatric questionnaires.	Demographic and health information.	CONSENT and COLLECTION The individual's health information is collected as part of the RAPIDS referral process.
8	Data from intake form and questionnaires is entered into RAPIDS and used to generate the RAPIDS report.	Demographic and health information.	USE RAPIDS report is generated.
9	RAPIDS report is transmitted to the referrer.	Diagnostic and treatment information.	DISCLOSURE RAPIDS report is transmitted to the referrer

10	RAPIDS team uses contact information provided in the RAPIDS intake form to send the individual a link to follow-up questionnaires.	Individual’s contact information.	COLLECTION RAPIDS team uses the individual’s contact for data collection as part of the RAPIDS follow-up process.
11	The individual uses the link to complete the follow-up questionnaires.	Demographic and health information.	COLLECTION The individual’s health information is collected as part of RAPIDS follow-up process.
12	RAPIDS follow-up questionnaires are transmitted to the referrer who referred the individual.	Health information.	DISCLOSURE RAPIDS follow-up questionnaires is transmitted to the referrer
13	RAPIDS Team provides technical support to the individual in completing their questionnaires.	Contact information.	USE Technical support and troubleshooting
14	RAPIDS Team provides support to referrer during the referral process.	Contact information.	USE Technical support and troubleshooting

Data Storage at RAPIDS

How is data stored as part of the RAPIDS service?

RAPIDS employs a robust, dual-zone architecture designed to ensure the highest standards of data privacy and security while enabling analytics capabilities. Our solution leverages Google Sensitive Data Protection, a service to ensure privacy and de-risk sensitive information.

Our architecture implements two distinct zones, each with independent specific security controls and data handling protocols:

1. Production Zone (Zone 1)

- Houses the original FHIR resources (i.e., health data, stored in a standards-compliant HL7 - FHIR format) containing protected health information (PHI)
- Implements highly restrictive access controls and encryption
- Maintains complete audit trails of all data access

2. Analytics Zone (Zone 2)
    - Contains systematically de-identified FHIR resources
    - Preserves clinical utility while removing personal identifiers
    - Dedicated Google BigQuery environment for running analytics on de-identified data, structured for optimal query performance and analysis
    - Maintains segregation from PHI-containing environments
    - Implements additional security controls for de-identified data handling
    - Maintains complete audit trails of all data access

In the Production zone (zone 1), all RAPIDS data is stored in secure SOC2-certified and HIPAA/PHIPA compliant facilities as described below:

- Incoming faxes are stored in SR Fax managed secure facilities in Vancouver, British Columbia, and are deleted once retrieved. More on SR Fax's privacy policy can be seen at: https://www.srfax.com/more/security-privacy/phipa-compliance/
- All incoming RAPIDS referrals are stored in TELUS Health's Collaborative Health Record solution in TELUS Health-managed Virtual Private Clouds (VPC) hosted at Google Cloud Platform ("GCP") and Amazon Web Services ("AWS") datacenters in Canada. More on TELUS CHR's privacy policy can be seen here
- Select case details core to RAPIDS' decision engine (demographics, select chart data, and generated guidance reports) are stored in a TELUS Health-managed VPC hosted at GCP datacenters in Montreal, for the processing of the guidance report and operations monitoring and audit purposes. This "zone 1" is highly restricted and limited to case co-ordinators to introduce a case, and case reviewers performing review/quality control on a case. More on RAPIDS Health Ltd. privacy policy can be seen at https://rapidshealth.com/privacy-notice/

- Patient-filled digital data collection (DDC) scales and other related data are temporarily stored & de-identified, in a Jotform managed dedicated instance in GCP and AWS datacenters in Canada. Once completed these scales are repatriated into CHR/RAPIDS datacenters as described above, and are promptly and permanently removed from our dedicated Jotform instance. More on Jotform's privacy policy can be seen at https://www.jotform.com/privacy/

How is data de-identified before migration from the production zone (zone 1) to the analytics zone (zone 2)?

Our platform employs Google's Sensitive Data Protection service to ensure comprehensive de-identification of personal health data to, essentially, anonymize the data - i.e., personal information has been de-identified to the point that there is no serious possibility of re-identification, by any person or body using any additional data or current technology. (Per https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/de-id_20241011/#fn45). This includes:

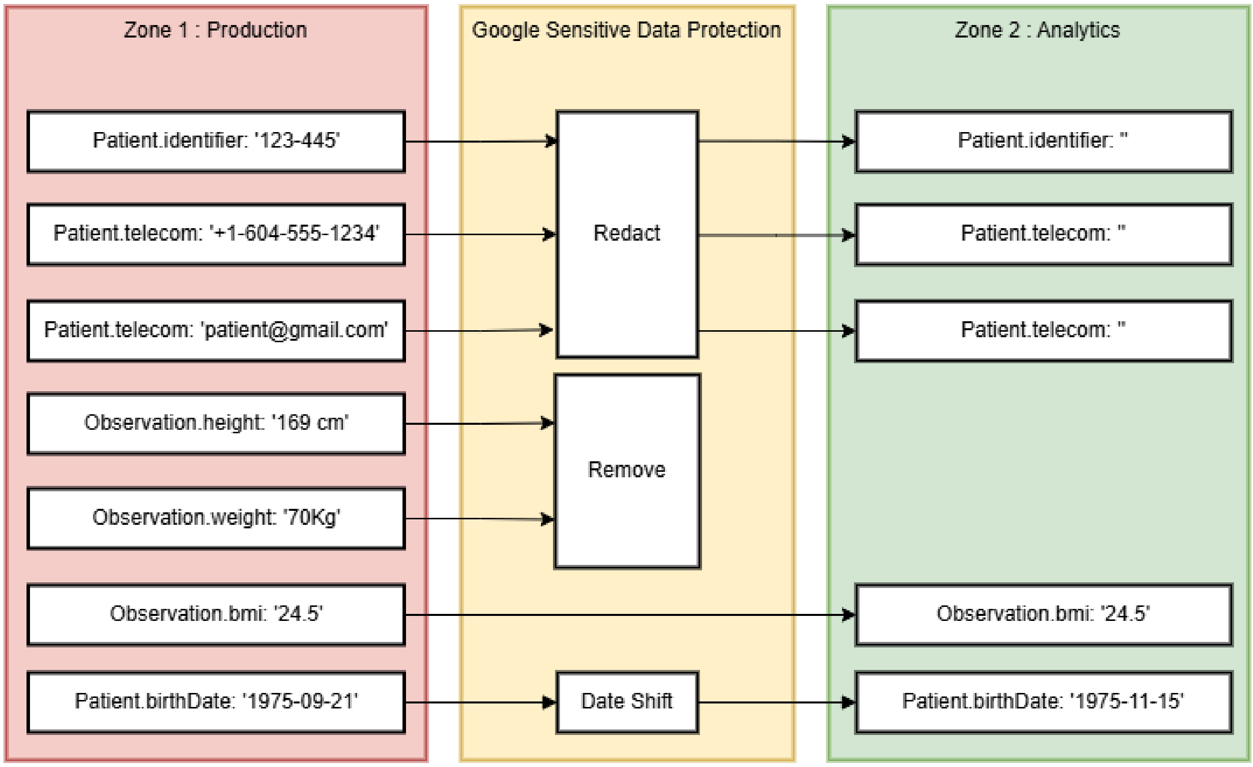
- Field-specific treatment: Each field in all FHIR resources undergoes a specific de-identification process based on its type and sensitivity.

- Redaction for identifiers and contact info: Any external system identifiers are completely redacted, leaving no trace of the original value. Both forms of contact info (phone number and email) are also fully redacted, ensuring no patient contact information remains.

- Date shifting for key date fields: Dates (including birthdates) undergo a date shift operation, which moves the date within a consistent range (typically, +/- six months). This preserves the general time frame for analytics purposes while making it difficult to identify the exact original date.

While the content of sensitive fields is removed or altered, the overall structure of all FHIR resources is maintained, allowing for consistent data handling in downstream analytics. In so doing, RAPIDS is able to protect individual patient privacy by removing or altering personally identifiable information while maintaining data utility for analytics by preserving the structure and relative temporal relationships in the data.

The image below shows how a selection of the individual's data would be deidentified as it moves from Zone 1 to Zone 2. In the diagram below the term patient is used for simplicity but the same diagram applies for individuals referred through a disability management organization:


Zone 1 : Production
Google Sensitive Data Protection
Zone 2 : Analytics
Patient.identifier: '123-445'
Patient.telecom: '+1-604-555-1234'
Patient.telecom: 'patient@gmail.com'
Observation.height: '169 cm'
Observation.weight: '70Kg'
Observation.bmi: '24.5'
Patient.birthDate: '1975-09-21'
Redact
Remove
Date Shift
Patient.identifier: ''
Patient.telecom: ''
Patient.telecom: ''
Observation.bmi: '24.5'
Patient.birthDate: '1975-11-15'

* data elements and values are representative and do not indicate the full breadth of deidentification that occurs

How can we be assured that de-identified/anonymized data cannot be re-identified?

The RAPIDS de-identification process has been evaluated by a third party firm specializing in de-identification and anonymization to assure the risk of re-identification is low.

Data Disclosure and Retention at RAPIDS

To whom does TELUS disclose data?

TELUS may share personal information with our service providers - most notably RAPIDS - who are contracted to perform services or functions on our behalf associated with delivery of the RAPIDS guidance service. Contractual controls ensure all information disclosed to our service providers is protected to the same standard as TELUS employs.

How long does RAPIDS retain data?

RAPIDS will retain information as instructed by you and to comply with appropriate regulations. This is generally set to, at a minimum, cover the relevant provincial health medical record retention requirements (e.g., 16 years for BC).

Your Responsibilities

What responsibilities do clients engaging in a RAPIDS pilot have?

TELUS does not determine or otherwise certify the compliance obligations of its customers, however here are some points you may wish to consider:

1) You should consider whether you need to conduct a privacy impact assessment (PIA).
2) It is your responsibility to send us a list of users who are authorized to send referrals to RAPIDS under the terms of your contract and to keep it up to date.
3) It is your responsibility to ensure that the individuals sending referrals under your contract (e.g. HCPs, case managers, etc.) have read and agree with the RAPIDS Terms of Use.

Contacting RAPIDS

You can contact us as follows:

- For general information: info@rapidshealth.com
- For questions or concerns about privacy related issues: privacy@rapidshealth.com.