priusmed®

medCLOUD™

Privacy and Security Overview

Key Points

- **Secure web applications**: TLS 1.3 strong cyphers-encrypted server communications, built-in multi-factor authentication, double encryption for sensitive data elements, no data of any kind (including PHI) stored on the end-user device.
- **Secure cloud platform**: built on top of Google Cloud Compute Engine, following best practices for the entire application development lifecycle.
- **Low-latency streaming**: 120-ms master system clock with sub-50 millisecond native end-to-end latency ensures near-instantaneous response.
- **Light IT footprint**: no servers or on-premise hardware to install; PriusMED handles all server upgrades and maintenance.
- **Security by design**: 2FA with device activation pre-requisite, rotating session tokens, user account control, roles and permissions, geolocation of activity, extensive logging.
- **Reliable and scalable**: geographic redundancy, horizontally scalable, vertically scalable.

Architecture

- Native web application (PWA) technology, accessed via secure URLs. No apps to install, no app store dependency of any kind.
- Fine-grained control with separate URLs for the first responder, remote assistant, case reviewer, and organization administrator.
- Platform and APIs run on Google Compute Engine (GCE) infrastructure.

- Low-latency streaming technology leveraging Google's fiber backbone ensures near-instantaneous broadcasting of video, audio, and patient vitals across the globe.
- Proprietary cloud architecture with built-in automatic vertical and horizontal scalability.
- Proprietary encryption and authentication protocols go way beyond the industry-standard OAuth2 and REST to minimize the attack footprint and add an additional layer of resilience to protect against zero-day exploits which typically target standard protocols used by the majority.

Corporate & Software Development Practices

- Documented and enforced corporate policies and procedures covering privacy, security, and cybersecurity risk management.
- Secure software development lifecycle with strict change-management processes.

Protected Health Information (PHI)

PriusMED implements administrative, physical, and technical safeguards to ensure the security, availability, and integrity of PHI.

- Providers create and share certain PHI via the medCLOUD platform including:
    - Patient Demographics, Main Concern, Date & Time of Encounter, Providers & Medical Organizations Information
    - Audio, Video, Vital Signs (Waveforms, Numerics & Trends), Snapshots, Clinical Annotations & Clinical Notes, Pictures & File Attachments
- Forms of communication include
    - Streaming & broadcasting of live video, audio, and patient vitals over the medCLOUD secure platform

- Participant messaging over the built-in medCLOUD secure Instant Messaging engine. **No PHI is ever sent over unsecured email and SMS channels**; unlike other vendors, we don't consider asking end-users to waive their data privacy rights as "compliant" – even if this approach would technically be "HIPAA compliant".
- Recorded video, audio, and patient vitals streamed over the medCLOUD secure platform

- What is NOT captured and stored in the medCLOUD platform
  - The patient's medical record
- Who owns the information?
  - As a SaaS vendor, PriusMED is the custodian of our customers' Data, for the patients that you serve, your end-users, and the hospitals and EMS agencies that we serve.
  - Customers own their Data, defined as
    - any and all text, graphics, images, audio content, audiovisual content, app usage, other materials, and any other information provided on or entered into the software or made available by healthcare providers through the software including all healthcare related information.

How is PHI protected?

- End-User device security
  - No patient information is permanently stored or cached on mobile devices.
  - All communications from the End-User device to the medCLOUD cloud platform are via encrypted TLS 1.3 connections with only the strongest cyphers enabled.

    - End-User devices must be Activated prior to use before they can connect to any medCLOUD services to prevent man-in-the-middle attacks.
    - All traffic is secured with rapidly rotating session tokens with a short expiration window to minimize the attack surface.
    - Automatic user logout after a configurable period of inactivity.
    - Password complexity requirements are enforced following OWASP guidelines.
- Cloud and Network Security
    - Google Cloud Compute Engine (GCE) hosted in SOC 2/3 (**SSAE 18**)-compliant data centers within US borders.
        - GCE Data centers are staffed 24/7 by trained security guards, and access is authorized strictly on a least-privileged basis.
        - See Google's Cloud Data Processing Addendum and Google Cloud Platform HIPAA BAA Addendum documents for more information on the data center / infrastructure.
        - PriusMED follows best practices to maintain security of Data, applications, and networks, in addition to the infrastructure level compliance provided by Google.
    - For each virtual server, all services are off, disabled, or blocked by default, and only certain services are added if and when needed.
    - All ports are locked down at the network (public access) level and at the virtual server (internal access) level by default.
    - Up-to-date security patches are deployed periodically and with each medCLOUD platform release.
    - TLS 1.3 with the most secure cyphers is strictly required for all client applications for both the public Internet traffic and for all internal GCE traffic

  - GCE infrastructure can only be accessed from a PriusMED-owned IP address enforced by: posture assessment, firewall rules, and using public/private key authentication.
  - GCE's Andromeda (external traffic) and Cloud Armor Level 7 (internal traffic) provide always-on Distributed Denial of Service (DDoS) and volumetric network/protocol attacks (SYN floods, UDP floods) protection for the medCLOUD platform.
- Privacy and Encryption
  - All PHI and end-user data is always encrypted in transit and at rest.
  - Secure TLS 1.3 connection using SHA 256 with 2048 bit key and the strongest cipher suite.
  - Database backups are encrypted using AES 256.
- Role-Based Access Control and Restrictions
  - A restricted number of PriusMED engineers, based on role, can access production servers.
  - Access to the production environment is only allowed if it originates from an approved PriusMED IP address
  - Any access to the administration of GCE environments requires a device that passes posture assessment for encryption and anti-virus
- Disaster Recovery and Data Backup
  - Available per SLA, the use of multiple Availability Zones with automatic failover allows customers to remain resilient in the face of most failure modes, including natural disasters or system failures.
  - Media files are stored in a secure, encrypted GCE bucket and can be automatically replicated to another GCE geographic region per SLA.
  - medCLOUD utilizes CGE intra-day persistent disk snapshots that are available for 14 days, and daily database backups available for 24

months. Backups are stored in Google backup vaults with vault status locked "Compliance Mode" and are immutable. All backups are encrypted to industry standard levels.

- Available per SLA, medCLOUD can maintain a warm, stand-by stack in a separate GCE geographic region where we can transfer production operations in the event of a Production region outage.

Isolated Environments

- Completely separate, distinct environments for each of the development lifecycle phases.
- Each environment has its own completely independent load-balancer and firewall.
- All environments are provisioned by code, version control, change management, and peer review to ensure consistency between environments.
- PHI data is only stored in the production environment and in data backups of the production environment. PHI is never stored in development or test environments.

Scalability & Reliability

Available per SLA, medCLOUD makes use of GCE Regions to provide high scalability with automatic addition of compute resources, reliability with automatic failover between GCE Regions if an entire GCE Region goes down.