RP1Cloud

Polycom POWERED

HIPAA Compliance

HIPAA and RP1Cloud

Pragmatic's RP1Cloud service is HIPAA compliant, and we sign the HIPAA Business Associate Agreement (BAA) for our healthcare customers. The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting the confidentiality of sensitive patient data. The RP1Cloud service does not have access to identifiable protected health information under HIPAA, but we do ensure that all the required physical, network, privacy and security measures are in place and followed as applicable to our service. Your patient information is secure with end-to-end encryption of video, audio, and screen sharing data.

Protecting Private Health Info

Here's what we do to make sure we're in full compliance with the law's extensive guidelines:

Workforce compliance

Our employees are trained on the key privacy, security and breach notification policies and procedures concerning HIPAA, and detailed records of all training initiatives are logged. HIPAA training encompasses new hire onboarding, offboarding and ongoing training and awareness.

Meeting Access Control

- Meeting access is protected by unique personal authenticators – email, conference ID and multi-tiered passwords, even when RP1Cloud is in emergency mode.
- Meetings are private by default, and require an invitation and the above info to get in.
- The host can lock meetings so that no one else can join, mute attendees and remove attendees.
- There's an auto-logoff if meetings haven't been properly ended, and meeting hosts can terminate sessions in progress.
- Only meeting hosts can start and stop recording a meeting and all presented content.

Data in motion

- All data transmitted on a call – including audio, video, and collaboration tools – are encrypted using AES 128-bit as well as SIP TLS/SRTP SIP encryption. We also use HTTPS tunneling (with H.323/SIP and browser plug-in) via Polycom's RealPresence Access Director. The ePHI is never duplicated, altered or destroyed in any unauthorized way. Participants joining via PSTN telephone may or may not be able to join a meeting based on encryption settings.
- The screen share function is an encrypted real-time screen capture with mouse and keyboard strokes only, not a transmission of the data file itself. RP1Cloud does not collect or distribute the actual patient data.

1.844.204.0023
www.rp1cloud.com
sales@rp1cloud.com

Data at rest

Here's what RP1Cloud holds on to: recordings made by meeting hosts, and the login data including time-stamps for meeting attendees.

- All of this information is stored, with full redundancy and security, at an automated SAS 70 II cloud datacenter.
- We use role-based Access Control mechanisms that restrict access to specific objects containing ePHI.
- During a call, RP1Cloud does not record any part of the meeting itself. The only time a meeting is recorded is when the meeting host uses the recording feature. That recording is encrypted and held in our secure datacenter. It is ONLY available for download (no streaming) after the proper authentication procedure.

General Security

We've got HIPAA security covered with:

- UC industry best practice security standards including NIST 800-53, SP 800-53, ISO 27001, PCI DSS and COBIT
- Pragmatic's RP1Cloud service being powered by Polycom, which has the Polycom Solutions Security Office overseeing all security in all products at Polycom and conducting yearly reviews to address the most challenging security concerns
- H.460 network firewall traversal
- Application firewalls
- Vulnerability scanning
- Patch management
- Breach testing
- DOS protection

Keep in Mind...

We've done our part to protect ePHI, but it's important to recognize that while RP1Cloud is a HIPAA compliant service, we look at it as being part of a shared responsibility with Covered Entities and sub-Business Associates. We are part of your overall HIPAA compliance solution, including core components such as Data at Rest, Data in Motion and Meeting Access Control. Our employees do not interface with patients or identifiable ePHI directly. Individuals, such as employees of a Covered Entity, using the RP1Cloud service must exercise their own due diligence for the ePHI they share and how they share it.