RingCentral

# RingEX and HIPAA

April 2024

## Introduction

The United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its amendments set forth requirements for HIPAA Covered Entities including vendor entities that process protected health information (PHI). PHI includes electronic protected health information (ePHI).

This document provides customers with information regarding HIPAA and how RingCentral, as a business associate, enables customers' HIPAA compliance.

## RingCentral as a Business Associate

RingCentral does not require customers to provide PHI in order to provide the services but customers may use the RingCentral products to process PHI. RingCentral customers subject to HIPAA ("Covered Entities"), who utilize RingCentral's services to create, collect, transmit, or maintain PHI, may consider RingCentral a business associate. Business associates are organizations that have routine access (reviewing, managing, handling) to PHI when providing their core services.

## How RingCentral complies with HIPAA

RingCentral is aware of its responsibilities as a business associate and offers certain controls for Covered Entities to determine how the PHI is managed, handled, and accessed.

**We offer contractual terms in line with HIPAA**

RingCentral makes available a business associate agreement (BAA) for our paying Covered Entity customers in alignment with HIPAA requirements. Furthermore, RingCentral has flowed down the same BAA requirements to our subcontractor business associates that may process PHI. The RingCentral BAA covers the PHI that the RingCentral services[1] may process and it covers our obligations with respect to our subcontractor business associates that may process PHI on our behalf.

**Our security is certified**

RingEX and the RingCentral App have earned Certified status for information security by HITRUST. HITRUST CSF Certified status indicates that these RingCentral applications have met industry-defined security requirements and are appropriately managing risk. RingCentral is part of an elite group of global organizations that have earned this certification. HITRUST CSF helps organizations address cybersecurity challenges through a comprehensive framework and scalable security controls by including federal and state regulations, standards, and frameworks. HITRUST CSF Certification sets the highest standard for compliance of security requirements and has become the benchmark that organizations apply to safeguard ePHI data.

Additionally, RingCentral annually undergoes a third-party SOC 2+ audit, which includes an assessment of controls mapped to the HIPAA Security Rule requirements, demonstrating the implementation of the security safeguards and requirements outlined in the HIPAA Security Rule.

**We protect the data of patients and other third parties communicating with RingCentral**

When a Covered Entity uses RingEX or the RingCentral App to communicate with their patients or with other third party individuals not employed by the Covered Entity and the patient or third party individuals are required to either download RingCentral Video Pro App or use the RingCentral Pro web version, the RingCentral communication occurring between the Covered Entity and the patient or third party is protected by the security standards required under HIPAA both for RingCentral Video Pro for end user consumers as for RingEX/RingCentral App, even though RingCentral does not enter into a Business Associate Agreement with such patients or third parties.

**We encrypt e-mail notifications to a Customer's preferred email platform**

RingEX may offer customers the option to send voicemail messages and the transcriptions of those messages to a user's email address as a notification. Even though the email provider is a third-party provider, the email will be sent over the RingCentral network to the user's email server using SMTP/TLS encryption.

---

[1] The following services are covered by the RingCentral BAA: RingEX, Avaya Cloud Office, Unify Cloud Office, Rainbow Cloud Office, RingCentral Contact Center, RingCentral Video Pro, Unify Video, RingCentral Engage Voice, RingCentral Engage Digital (third party channel communications excluded).

**How RingCentral aligns with HIPAA Security Requirements**

We have mapped certain HIPAA security requirements below to enable customers to assess HIPAA obligations and requirements[2]. These requirements have been audited by our SOC2+ audit report. Our security commitments to our customers can be found in the RingCentral Security Addendum.

| HIPAA Requirement | RingCentral Response |
|---|---|
| Administrative Safeguards | |
| Security management process | • RingCentral maintains a written information security program that includes documented policies or standards appropriate to govern the handling of protected data in compliance with the agreement with the customer and with applicable law.<br>• RingCentral employees acknowledge a code of conduct, which includes a sanctions policy for personnel who violate the code. |
| Risk management | • RingCentral performs regular cybersecurity risk assessments in accordance with a risk assessment policy to identify threats to its business or operations. |
| Assigned security responsibility | RingCentral implements:<br>• Defined organizational roles and responsibilities which are made available to RingCentral personnel.<br>• Oversight by senior employees responsible for implementing RingCentral's written information security program. |
| Workforce security and information access management | RingCentral employs access control mechanisms designed to:<br>• Limit access to protected data to only those personnel who have a reasonable need to access said data;<br>• Prevent unauthorized access to protected data;<br>• Perform a regular review of access controls for all RingCentral's systems that transmit, |

[2] Customers that are subject to HIPAA regulations are ultimately responsible for complying with its requirements.

| | |
|---|---|
| | process, or store protected data.<br><br>• RingCentral maintains a documented user management lifecycle management process that includes manual and/or automated processes for approved account creation, account removal and account modification for all information resources and across all environments. |
| Security awareness and related training | • RingCentral ensures that all employees including contractors, complete annual training for security and privacy requirements, including cybersecurity awareness, GDPR, and CCPA. |
| Security incident procedures | • RingCentral maintains an incident response capability to respond to events potentially impacting the confidentiality, integrity and/or availability of services, and/or data (including protected data). |
| Evaluation | • RingCentral runs regular internal and external network vulnerability scans against information processing systems. |
| Physical Safeguards | |
| Facility access controls | • All physical areas where RingCentral services process protected data are monitored, controlled, and access to them is restricted to authorized individuals. |
| Workstation security | • RingCentral employees either use RingCentral owned and managed devices in the performance of their duties or use devices under the bring your own device (BYOD) program, all of which are enrolled in the RingCentral managed device program. |
| Device and media controls | • RingCentral maintains an accurate and current asset register covering hardware and software assets used for the delivery of services. RingCentral also maintains |

| | |
|---|---|
| | processes to wipe or physically destroy physical assets prior to their disposal. |
| Technical Safeguards | |
| Access control | • RingCentral user password requirements align with current NIST guidance.<br>• RingCentral leverages role-based security to limit and control access within the production network. Production access is controlled using least privilege principles. |
| Integrity | • Access is limited to users who have a business need to know. The principle of least privilege is followed, allowing access to only the information and resources that are necessary.<br>• All systems, devices or applications associated with the access, processing, storage, communication and/or transmission of protected data, generate audit logs, which include sufficient detail that they can be used to detect significant unauthorized activity. |
| Transmission security | • RingCentral ensures encryption of protected data in electronic form in transit over all public wired networks (e.g., internet) and wireless networks (excluding communication over public switched telephone networks). |
| More resources | RingCentral Trust Center |
| Contact us | privacy@ringcentral.com |