


# The HIPAA security guide for cloud communications

The essential HIPAA security, data privacy, and compliance guide for your trusted unified communications platform


3:17



Mike Chen



Clarissa



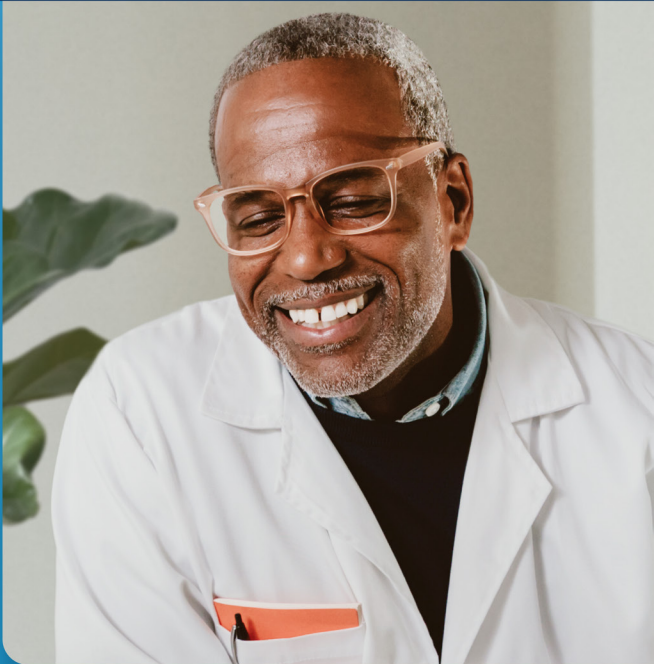
Sentiment 89%



Personal files




Security



Today - Monday, August

8:00 AM Phase 1 Clinical Trial

9:00 AM



+9

Join

# Table of contents

- Introduction ..... 3
- 7 questions to ask a cloud communications vendor about HIPAA ..... 4
- HIPAA 101: The basics ..... 5
- HIPAA security and privacy controls: What to look for from a business associate..... 7
- Cloud communication security essentials: The 3 use cases for a platform you can trust.... 8
- In-depth: Information security protection + data privacy and compliance management. 12
  - Physical Security ..... 12
  - Network Security ..... 12
  - Data Encryption..... 12
  - Toll Fraud Prevention ..... 13
  - Incident response ..... 13
  - Protected Data..... 13
  - Operations Security..... 14
  - Supplier Management ..... 14
  - Data Handling ..... 14
  - Software Development Cycle ..... 14
- In-depth: Global data privacy and security certifications and attestations ..... 14
- In the spotlight: HITRUST CSF certification
- In-depth: Security and administrative policy controls ..... 14
  - Video ..... 14
  - Phone ..... 15
  - Message ..... 15
  - Access and Identity..... 15
  - Encryption ..... 15
  - Unified App ..... 16
  - eFax ..... 17
- Innovation spotlight: End-to-End Encryption for calls, chats, and meetings..... 18

## Introduction

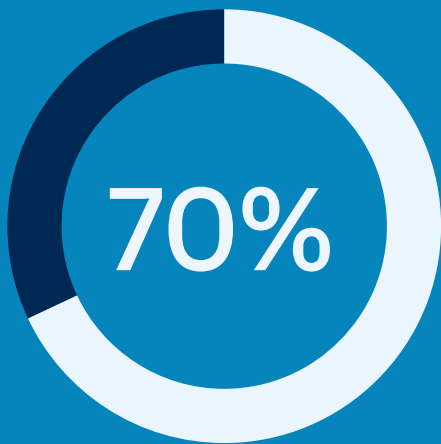
The healthcare industry is often at the forefront of adopting innovative technologies that can improve patient care and streamline operations. However, despite the progress made, there is still much work to be done.

Legacy, on-prem systems that result in regulatory hurdles and security issues pose significant challenges to the journey towards digital transformation. As Gartner reported in 2022, IT spending to transform healthcare business increased from 8% to 11% of total spend (37.5% increase) to address this concern.

To successfully navigate these obstacles, organizations must implement new cloud-native technologies so they can lead the way in advancing digital transformation in healthcare.

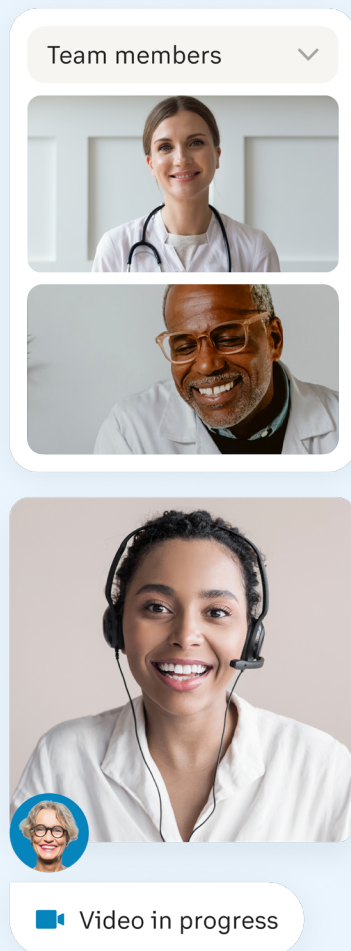
Of the most important aspects of IT transformation for healthcare providers is selecting the right communications vendor to handle employee and patient communications.

Evaluating how a unified cloud communication vendor - one that handles not just internal communications but also external patient communications - will maintain your organization's security and data privacy is an important area of focus, given that according to the U.S. Department of Health and Human Services, approximately 70% of organizations are not "HIPAA compliant."



Approximately 70% of the organizations are not HIPAA compliant

# 7 questions to ask a cloud communications vendor about HIPAA compliance



In 2023, the price of a HIPAA violation increased to adjust for inflation. HIPAA violations are now subject to penalties of up to \$60,226 per violation and up to \$1,919,173 per calendar year. Needless to say, choosing the right cloud communication solution to stay compliant with today's privacy laws is an important decision.

Here are 7 questions to ask a unified communications vendor about HIPAA compliance:

1. Does the vendor keep you HIPAA compliant through security and privacy safeguards and sign a Business Associate Agreement (BAA)?
2. Do they have detailed information about their information security protection capabilities?
3. Are they transparent about their data privacy and compliance management practices?
4. Do they have robust and modern security and administrative policy controls protecting phone, video, messaging collaboration and more?
5. Have they achieved independent, globally recognized 3rd party certifications for their security and privacy processes, such as HITRUST CSF, ISO 27001 and more?
6. Are they innovating by adding HIPAA recommended functionality like end-to-end encryption?
7. Do they have a track record and trusted reputation for delivering scalable and HIPAA compliant cloud communications services for leading healthcare organizations?

RingCentral's cloud communications platform supports HIPAA-compliant communications.

From our industry-leading five 9s in uptime reliability to our comprehensive information security protection, administrative security controls, and adherence to global privacy laws including HIPAA, you don't have to worry about your data being compromised or falling short of regional regulation standards.

## CHAPTER 2

# HIPAA 101: The basics

Understanding HIPAA compliance in today's landscape of cloud communications can be a confusing topic. To make things easier here are a handful of key topics to better understand how it works.

<b>What is HIPAA?</b>	The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of protected health information (PHI).
<b>What PHI is protected under HIPAA?</b>	PHI is individually identifiable health information related to the future or mental condition of an individual. It also includes demographic information such as data collected by a doctor, hospital, clinic, pharmacist, and health plan.
<b>What are PHI indicators?</b>	<ul style="list-style-type: none"><li>• Names and addresses.</li><li>• All elements of dates related to an individual's birth, admission to a healthcare facility, or date of death.</li><li>• Telephone numbers.</li><li>• Fax numbers.</li><li>• Electronic mail addresses.</li><li>• Social Security Number (SSN).</li><li>• Medical record numbers.</li><li>• Health plan beneficiary numbers.</li><li>• Account numbers.</li><li>• Certificate/license numbers.</li><li>• Device identifiers and serial numbers.</li><li>• URLs or IP addresses.</li><li>• Biometric identifiers (including finger and voice prints).</li></ul>
<b>What is ePHI?</b>	Electronic Protected Health Information. ePHI is PHI that has been created, received, maintained or transmitted electronically.

## Who needs to comply with HIPAA?

**Covered entity** - includes healthcare providers, health plans, healthcare clearinghouses. Providers are hospitals, clinics, nursing homes, doctors' offices and entities that are paid for the provision of healthcare.

**Business associates** - A person or organization outside of the covered entity who performs, on behalf of the covered entity, certain defined functions or activities involving PHI. RingCentral is a business associate.

**Business associate subcontractors** - third parties who require access to PHI owned or managed by the business associate, such as billing or accounting firms. These organizations must sign an agreement they will protect PHI per HIPAA guidelines.

## Who needs to comply with HIPAA?

**Covered entity** - includes healthcare providers, health plans, healthcare clearinghouses. Providers are hospitals, clinics, nursing homes, doctors' offices and entities that are paid for the provision of healthcare.

**Business associates** - A person or organization outside of the covered entity who performs, on behalf of the covered entity, certain defined functions or activities involving PHI. RingCentral is a business associate.

**Business associate subcontractors** - third parties who require access to PHI owned or managed by the business associate, such as billing or accounting firms. These organizations must sign an agreement they will protect PHI per HIPAA guidelines.

## What are the three HIPAA rules?

**HIPAA Privacy Rule** - Applies to the use and disclosure of PHI and includes specifications that Covered Entities must follow including notification of privacy practices, providing access to individuals for PHI about themselves, notifying if their data is breached and more.

**HIPAA Security Rule** - National standards for protecting PHI within a healthcare organization from both internal and external threats. The HIPAA Security Rule applies to RingCentral.

**Breach Notification Rule** - Requires healthcare organizations to report breaches in security or confidentiality of PHI.

## What is the difference between a Privacy Rule violation and Security Rule violation?

A Privacy rule violation involves an individual's PHI and a Security rule violation involves ePHI.

## What is a Business Associate Agreement?

HIPAA requires that a Business Associate that provides services to a Covered Entity that includes access to PHI must sign a business associates agreement (BAA). RingCentral makes available a business associate agreement 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.

## CHAPTER 3

# HIPAA security and privacy controls: What to look for from a business associate

RingCentral annually undergoes a third-party audits to certify our services against globally recognized standards.



One of the most recognized standards is the SOC II + HIPAA report, which covers controls around availability, security, and confidentiality of customer data. The SOC II report issued by our third party auditor extensively covers our accordance with the HIPAA Security Rule requirements and outlines in detail our designs, service commitments and system requirements. Among the administrative, technical and physical safeguard practices covered are:

- Security management process
- Risk management
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and related training
- Security incident procedures
- Evaluation
- Facility access controls
- Workstation security
- Device and media controls
- Access control
- Integrity
- Transmission security

# Cloud communication security essentials: The 3 use cases for a HIPAA-compliant platform you can trust

What supported use cases do you absolutely need in order to get security, privacy, and HIPAA-compliance right every time? And to know, consistently, that your platform doesn't present a risk to your brand trust or bottom line?

The essential security formula



**Rigorous information security protection**



**Comprehensive data privacy and compliance management**



**Best practice security and administrative policy controls**

### 1. Information security protection

In addition, reliability and uptime will serve as the underpin for your platform's foundation of trust by assuring your business continuity. When it comes to keeping information assets secure, demonstrating cloud security, and committing to safeguard personal data, ISO/IEC 27001 standards are widely known as leading benchmarks for a vendor's information security.

From the business infrastructure to the design and processes used for the cloud communication platform itself, your vendor must apply airtight security best practices that are always on to provide the peace of mind that your data is safe from compromise.

Your cloud communication vendor must demonstrate that they have applied best-of-breed technologies and stringent operational processes to ensure that your data has rigorous protection at all times.



This should also include details on the security practices of their platform's cloud infrastructure. An approach like this can't be bolted on as an afterthought once a security gap becomes an issue, it must be part of your vendor's DNA that is brought to bear in every aspect of the business.

Your vendor must be ready to demonstrate their strong commitment to data security and provide details across several areas, including the physical security of their environment, data handling policy, and processes for regular security assessments. In addition, you should look for validations from compliance attestations and certifications that help speak to the vendors' commitment to data security, such as: SOC 2 Certification, ISO 27001 Certification, HITRUST CSF and others.

## **2. Data privacy and compliance management**

With the feature-rich capabilities cloud communications platforms provide, there's a high likelihood of sharing confidential items, personally identifiable information (PII), or electronic personal health information (ePHI) over the platform, such as sensitive product plans, customer information, and employee details.

In fact, that's one of the valuable, business-enabling aspects of cloud communication solutions, so it makes sense that your vendor should have a thoughtful data privacy and compliance management policy that is consistently being followed.

Your vendor should employ an exhaustive system to prevent the inadvertent or intentional compromise of protected data, and they should be transparent about how data is collected and used. This is imperative to establish trust in a vendor's data practices and to validate they're respecting your company's data privacy.

Your vendor should have the most stringent data privacy policies, which will ideally be documented in a comprehensive data privacy notice that is made publically available. In addition, review the vendor's transparency practice for regularly communicating the requests they have received about customer data along with details on how they responded to these requests.

These will provide the assurance you need that your vendor is keeping your data and organization free of regulatory concerns.

## **3. Security and administrative policy controls**

From waiting rooms to meeting passwords, cloud communication platforms should include comprehensive security capabilities to protect the platform and user experience. Administrative options, such as requiring authentication for meeting attendees, controls on who can enable screen sharing, and requiring waiting rooms to authorize attendees to join safeguard your organization from data loss and bad actors.

In addition to providing in-depth security and policy controls, your platform should take the guesswork out of which ones to enable by providing best-practice recommendations. This will make it easy to secure your everyday communications.

## RingCentral: a leading approach to trust

RingCentral is leading the way as the market standard in trusted, unified communications for today's digital and modern business by providing secure and safe communications for every user. We've maintained a long-standing commitment to security, built on deep expertise in operating and securing unified communications and SaaS products.

Security is in our DNA. We take a multi-dimensional approach to put the safety of your data first by applying best-in-class technologies and rigorous processes.

### World-class security organization

Built by IT security veterans with over 100 years of experience and a dedicated software development team focused on ensuring platform and data security.



### Best-in class DevSecOps

From our product design to the operations of our business, we employ rigorous security and data best-practices in everything we do. We provide our customers with a robust security platform by integrating security principles into the development process from the get-go.

### Secure-by-design platform

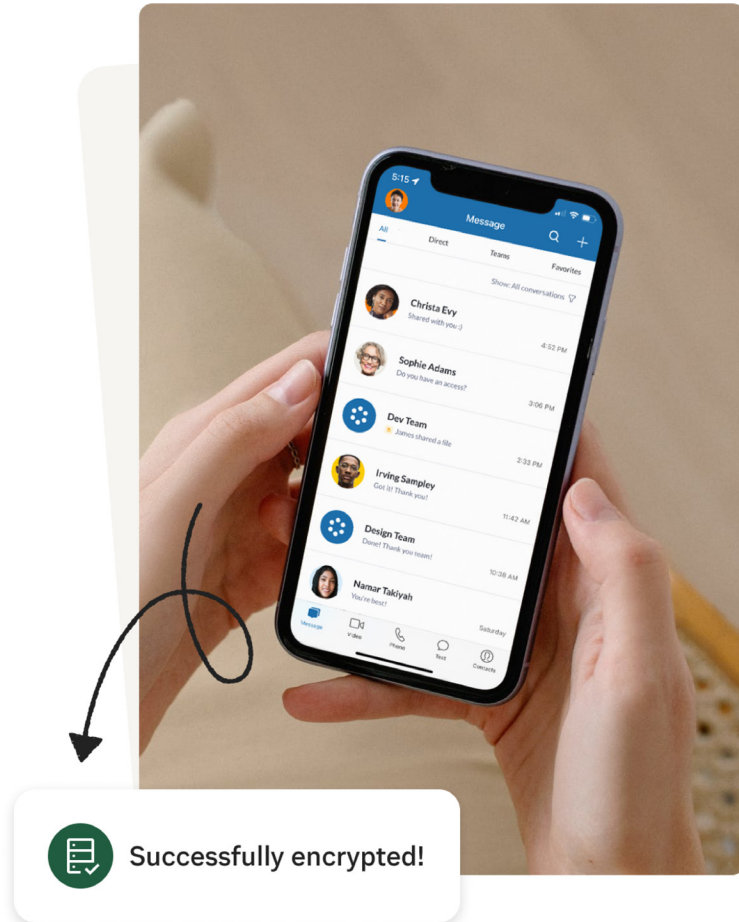
We tirelessly pursue a shared responsibility model where we maintain third-party certifications and attestations that validate our information security policies and practices along with customer controls, so you can directly manage your use case needs.

## High reliability and uptime

Experts are proactively monitoring and optimizing our platform 24/7/365 to ensure the availability of your service remains at the highest level possible.

We stand by this commitment with an industry-leading service level agreement (SLA) of 99.999% uptime offered in over 45+ countries. And we've consistently met that promise for 12 consecutive quarters.

With over 15 geographically dispersed data centers and media points of presence, RingCentral provides a global infrastructure that ensures 24/7 business continuity for your company, from anywhere.



# CHAPTER 5

## In-depth: Information security protection + data privacy and compliance management



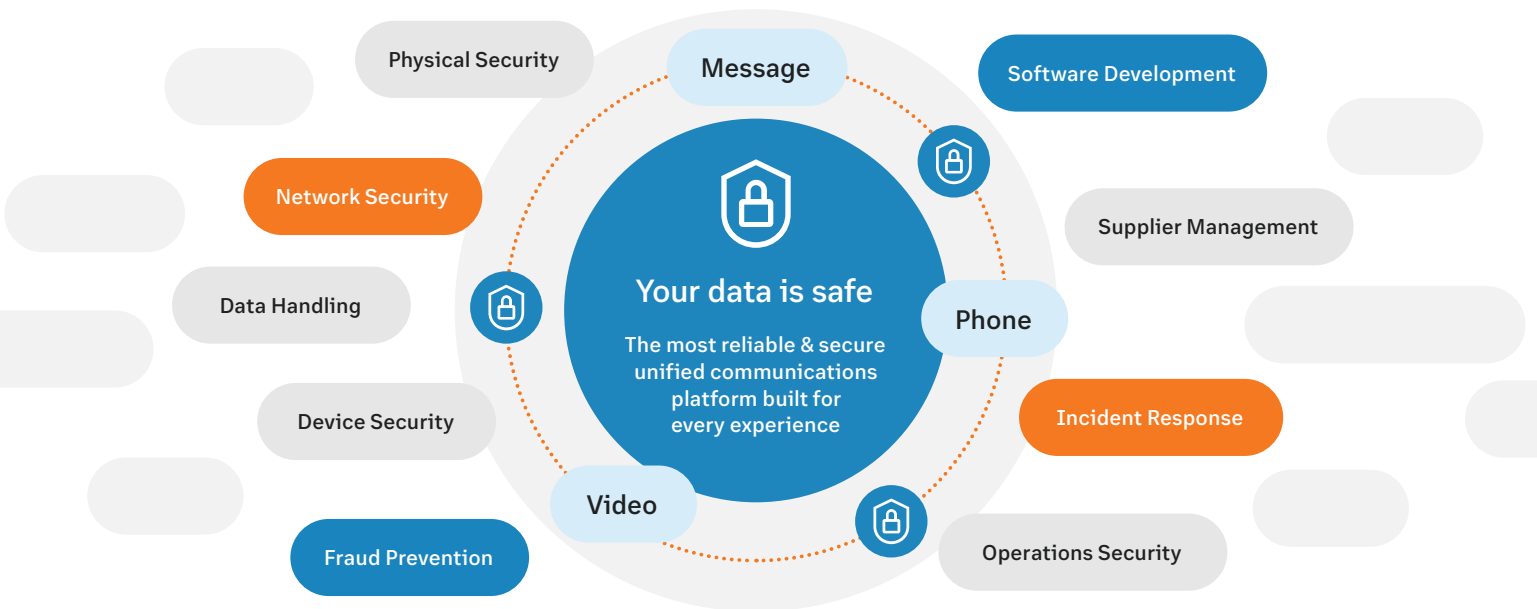
**Always On**  
Information Security, Privacy & Compliance Management



**Customizable / Dynamic Security & Policy Controls**



To give you deeper insight into our stringent practices, let's take a look at the people, process, and technologies we have in place to provide the ultimate customer experience that is safe, compliant, and secure.



# 1. Our secure infrastructure

RingCentral’s security posture consists of numerous controls that reflect the best practices from established information security industry standards. Collectively, these stringent controls allow us to achieve world-class security practices for our customers. Some of these controls include:

## Physical Security

We maintain appropriate physical security controls on a 24-hours-per-day, 7-days-per-week basis, and to the extent that RingCentral operates or uses a data center, we ensure that physical security controls are in alignment with industry standards such as ISO 27001 and SSAE 16 or ISAE 3402.

## Network Security

We maintain a multi-layered network security program that includes industry-standard firewall protection, intrusion detection systems (IDS), intrusion prevention systems (IPS), DDoS attack and other web threat blocking, two-factor authentication for access to RingCentral’s networks, and others. In addition, we run internal and external network vulnerability assessments against our information processing systems at least quarterly to consistently evaluate our network security program.

## Data Encryption

RingCentral encrypts data in transit and at rest, using applicable industry-leading encryption standards and protocols. We apply two, enterprise-grade security protocols to provide additional security for IP phone calls—TLS authentication and SRTP encryption.



In addition, all portals have https access (e.g., service.ringcentral.com); all non-voice data is TLS encrypted; and hard phones use digital certificates to establish secure connections to download their provisioning data.

To address potential vulnerabilities in the VoIP data plane, RingCentral safeguards voice communications with an advanced secure voice technology that prevents call eavesdropping or tampering with audio streams between endpoints.

## Toll Fraud Prevention

Our service abuse and fraud management team is regularly monitoring and on the lookout for fraud. We use a range of tools for detection, which encompass:

- Volume, velocity, historical, and current trends on specific ranges, numbers dialed, and dial-pattern recognition
- Anomalous and or suspicious usage traversing our network
- Unauthorized access of extensions/mailboxes, digital lines, SIP devices, and IVRs

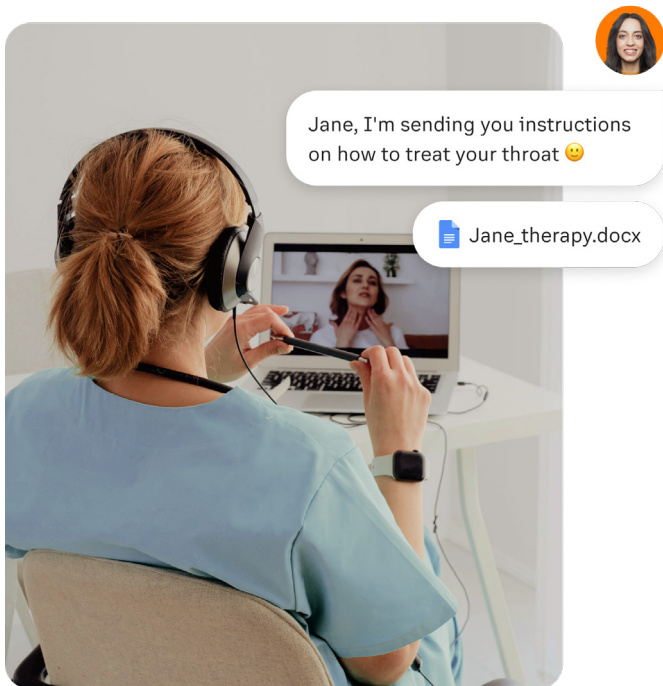
Our team responds to alerts from carriers when there is detected activity of anomalous usage, such as high risk and high cost of international ranges, reports of scams (e.g., a RingCentral customer number has been reported of committing scam, defraud, phishing, etc.), as well as any reports of harassment, unsolicited calls, or call annoyance.

## Incident response

Our incident response capabilities are designed to comply with statutory and regulatory obligations that cover incident response. To deliver on this, we maintain incident response capabilities to respond to events potentially impacting the confidentiality, integrity, or availability of your services or data, including protected data.

## Protected Data

We maintain a written information security program that includes policies for handling protected data in



compliance with the Agreement and with applicable law. In addition, it includes administrative, technical, and physical safeguards that are designed to protect the confidentiality, integrity, and availability of protected data.

## Operations Security

Our rigorous operations security program follows industry best practices across our global organization, including in-depth security measures for asset management, configuration management, malicious code protection, vulnerability and patch management, as well as log monitoring.

## Supplier Management

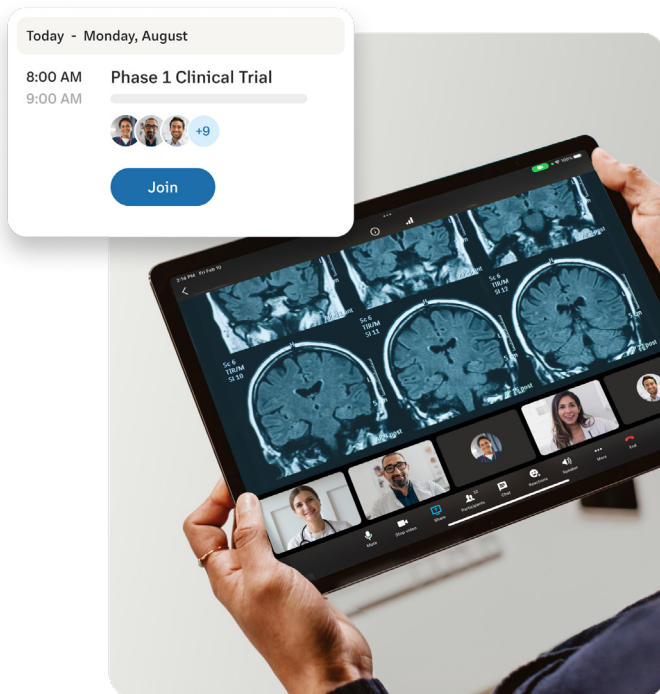
We hold our third-party suppliers to our same high security standards, and we consistently monitor for publicly disclosed vulnerabilities and exposures for impact to our supplier's information systems and products.

## Data Handling

RingCentral maintains data classification standards for both public data (i.e., data that is generally available or expected to be known to the public) and confidential data (i.e., data that is not available to the general public, including protected data).

## Software Development Cycle

We apply secure development lifecycle practices, including during design, development and test cycles, and we ensure that our products are subject to security reviews, including threat considerations and data handling practices.



ALWAYS ON

## 2. In-depth: Global data privacy and security certifications and attestations

Our third-party attestations and certifications speak to our commitment to data security. RingCentral is built on a secure cloud platform with a robust portfolio of security and compliance certifications, including:

- SOC 2 attestation
- SOC 3 attestation
- ISO 27001 and ISO 27017-18 certifications
- STIR/SHAKEN (Spam blocking)
- HITRUST CSF certificate
- HIPAA attestation of compliance
- GDPR
- PCI-certified merchant
- PIPEDA
- FINRA



This means your data is secure, private, and compliant across mobile, video, and phone, making RingCentral the most reliable and secure unified cloud communications platform built for every experience. You can see the full list and learn more about our independent certifications [here](#).



## In the spotlight: HITRUST CSF certification

HITRUST, a healthcare industry-led organization, has developed and maintains the Common Security Framework (CSF), which is a verifiable framework that enables healthcare organizations and providers to demonstrate their security and compliance in a consistent and efficient manner.

The CSF, which is based on the US healthcare laws HIPAA and the HITECH Act, sets out requirements for the use, disclosure, and protection of individually identifiable health information, and enforces non-compliance.

Additionally, the CSF includes healthcare-specific security, privacy, and other regulatory requirements from recognized frameworks like the Payment Card Industry Data Security Standard (PCI-DSS) and the ISO/IEC 27001 information security management standards.

RingCentral MVP has earned Certified status for information security by HITRUST, the highest level of HITRUST certification.

The screenshot shows a RingCentral team chat interface for a group named "Product Team". The interface includes a left-hand navigation pane with options like Mentions, Bookmarks, Show Unread, FAVORITES, and TEAMS. The main chat area displays a conversation with five team members: Rachel DaMario, Will Serra, Hope Lee, Rachel DaMario, and Hope Lee. The messages discuss the status of the Echo Project, a brainstorming session, and a plan. A "Today" separator is visible. At the bottom, a message from Mikaela Sobhani says "Hey Team! Great meeting yesterday, what are the next steps?". The right-hand pane shows team details, including "Private team", "Members (5)", "Guests", and a list of pinned files such as "Product Release V1.pdf", "Product 1.9 view.docx", "Weekly Report.pdf", and "Ico-Font\_mobile.zip".

# 3. In-depth: Security and administrative policy controls

The RingCentral platform provides our customers with leading-edge security and policy controls that ensure a safe and secure experience for your users. Our platform puts a comprehensive set of administrative controls across video, message and phone at your fingertips, such as requiring your meeting attendees to authenticate, limiting who can enable screen sharing, and requiring waiting rooms for your users to approve attendees who can join. These provide you with best-in-class security capabilities to safeguard your organization from data loss and bad actors.

## Video



- Single sign-on (SSO)
- Available via desktop & mobile app, and browser (via WebRTC)
- Require password
- Restrict screen sharing
- Enforce waiting rooms
- Restrict meeting attendance to authenticated users
- Allow user to enable meeting recordings
- Enable moderator turn on/off video for all participants
- Moderator remove participants
- Moderator mute participants
- Virtual background for privacy
- Hide meeting ID
- Control data file sharing

## Phone

- Audit trail to track changes
- End-to-end encrypted meetings
- TLS encryption/SRTP secure voice
- Single sign-on (SSO)
- Block phone numbers
- AI-based spam blocking
- RoboCall mitigation using STIR/SHAKEN standards
- Number masking
- RingOut—calling on third-party devices with your business phone number
- Emergency response locations for E911 calls
- Voicemail routing based on business hours
- Analytics portal
- 99.999% SLA uptime
- End-to-end encrypted calls
- TLS encryption/SRTP secure voice
- Allow/block list—external guest domains
- Allow/block list—webmail accounts
- Clear guest identification within 1:1 and group chats
- Enforce policies
- End-to-end encrypted messages
- SEA FINRA 17a-4 compliant
- Single sign-on (SSO)
- Enforced multi-factor authentication (MFA)
- Device PIN enforcement
- User management
- Data-at-rest
- Data-in-transit
- TLS encryption/SRTP secure voice
- E2EE via Message Layer Security (MLS)



## Message

- Allow/block list—external guest domains
- Allow/block list—webmail accounts
- Clear guest identification within 1:1 and group chats

- Enforce policies
- End-to-end encrypted messages
- SEA FINRA 17a-4 compliant

## Access and Identity

- Single sign-on (SSO)
- Enforced multi-factor authentication (MFA)
- Device PIN enforcement
- User management

## Encryption

- Data-at-rest
- Data-in-transit
- TLS encryption/SRTP secure voice
- E2EE via Message Layer Security (MLS)

## Unified App




- Single sign-on (SSO)
- Available via desktop & mobile app, and browser (via WebRTC)
- Require password
- Restrict to authenticated users
- Session timer to logout inactivity
- Authorized apps manager
- VoIP country blocking
- Centralized IT management of free and paid users
- Audit trail to track changes
- Mobile Application Management via MS Intune
- Archive capabilities through Ringcentral Archiver and 3rd party integrations

## eFax

- Custom fax cover sheets for HIPAA compliant disclaimers

# Innovation spotlight: End-to-End Encryption for calls, chats, and meetings

## Best-in-class encryption:

-  Goes beyond 1:1 calls and supports up to 50 participants
-  Multi-modal and available on any device whether it's desktop or mobile
-  Available whether the conversation is ongoing, scheduled or spontaneous



This scheduled, spontaneous, or ongoing layer of privacy gives your users the same level of privacy that they'd experience in a face-to-face conversation held in a conference room.

RingCentral's end-to-end encryption (E2EE) provides unparalleled security and privacy for privileged conversations, and protection against 3rd-party intrusion and a host of attacks. E2EE removes the need for multiple encryption products, modernizes the user experience and reduces privacy concerns within privileged conversations.

For many organizations, privacy concerns are complex, costly and inadequate. Before RingCentral E2EE, those who wanted private, end-to-end encrypted calls, chat messages and video meetings were stuck using multiple products that lacked sufficient compliance oversight, often forcing them to evade corporate policies and use non-sanctioned apps. Now, organizations can simplify their tech stack by eliminating non-sanctioned apps and enabling RingCentral's native capabilities.

With RingCentral's End-to-End Encryption for calls, chats, and meetings - no third party, not even RingCentral - can access company communication data. E2EE provides intuitive controls to turn everyday conversations into end-to-end encrypted conversations, at the individual and team level. We are the only UCaaS provider with enterprise-ready End-to-End Encryption for all forms of business communications - whether it's a scheduled, spontaneous or ongoing 1:1 conversation or a meeting with up to 50 participants.

## Compliance for chat messages

Company IT admins with the right kind of permissions will be able to access the chat data within the RingCentral admin dashboard. If needed, company IT admins can grant 3rd party auditors the ability to access the data. However, RingCentral will not have access to the data.

For compliance-minded organizations, such as financial services, IT administrators can turn off E2EE at the organizational level. For added peace of mind, RingCentral tightly integrates with Theta Lake for compliance monitoring and supervision requirements for voice, chat, and video calls using RingCentral.

# Conclusion

Cloud communication platforms play a critical role in fostering an organization's collaboration to drive growth. Partnering with a vendor that places a priority on the security, privacy, and maintained HIPAA-compliance of your data will meet your business needs, safely and securely. When you take a close look at buying criteria that assures your continued trusted healthcare customer experiences, you'll get your winning platform with RingCentral.

RingCentral offers a fundamentally different approach to global trust for your unified communications platform. From our industry-leading five 9s in uptime reliability to our comprehensive information security protection and global privacy management, you don't have to worry about your data being compromised or falling short of regional regulation standards.

Our innovations and commitment to security, data privacy, and compliance have earned RingCentral recognition as a trailblazer in the market, including seven consecutive years being named as a Leader in the Gartner Magic Quadrant for Unified Communications as a Service (UCaaS).

Our approach delivers "always-on" information security protection and data privacy management that keeps your data safe and compliant with the law. And our platform provides a comprehensive toolset for your administrators and users with a breadth of dynamic and real-time controls.

To learn more visit the [RingCentral Trust Center](#).

#### Disclaimer:

Please note that the information in this document on legal or technical subject matters is for general awareness only and does not constitute legal or professional advice, or warranty of compliance with applicable laws. The content of this document may be subject to change.

---

For more information, please contact a sales representative. Visit [ringcentral.com](https://ringcentral.com) or call 855-774-2510.

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact center solutions based on its powerful Message Video Phone™ (MVP™) global platform. More flexible and cost effective than legacy on-premises PBX and video conferencing systems that it replaces, RingCentral empowers modern mobile and distributed workforces to communicate, collaborate, and connect via any mode, any device, and any location. RingCentral offers three key products in its portfolio including RingCentral MVP™, a unified communications as a service (UCaaS) platform including team messaging, video meetings, and a cloud phone system; RingCentral Video®, the company's video meetings solution with team messaging that enables Smart Video Meetings™; and RingCentral cloud Contact Center solutions. RingCentral's open platform integrates with leading third-party business applications and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

**RingCentral**

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. [ringcentral.com](https://ringcentral.com)

© 2021 RingCentral, Inc. All rights reserved. RingCentral and the RingCentral logo are registered trademarks of RingCentral, Inc. Other third-party marks and logos displayed in this document are the trademarks of their respective owners.