RingCentral

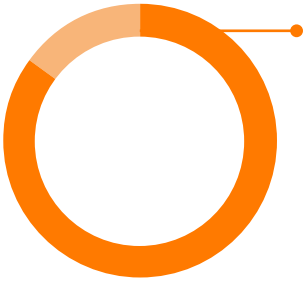
US

The HIPAA security guide for cloud communications

Table of contents

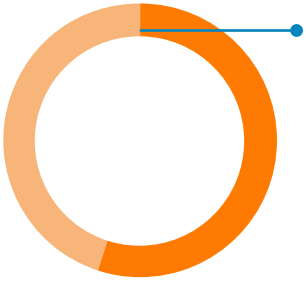
Introduction

The healthcare industry is at the forefront of innovation, striving to adopt technologies that will improve patient care and streamline operations. Today's innovators are aggressively moving to the cloud, gaining efficiency, agility, and scalability along the way.



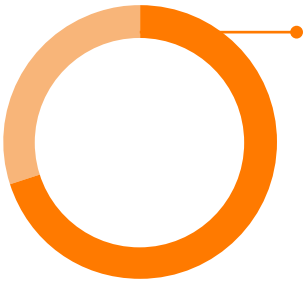
85%

of health systems are increasing their IT budgets



55%

with cybersecurity as a top investment priority for 55% of respondents.



70%

approximately 70% of organizations are not HIPAA compliant.

Legacy, on-premises systems are often plagued by regulatory hurdles and security issues, creating significant challenges along the path toward digital transformation. According to the 2024 Health System Digital and Investment Trends Report, more than 85% of health systems are increasing their IT budgets, with cybersecurity as a top investment priority for 55% of respondents.

Organizations must implement new cloud-based technologies to navigate these obstacles and successfully advance digital transformation in healthcare.

One of the most essential aspects of IT transformation for healthcare providers is selecting the right communications vendor to handle employee and patient communications. This is especially important in the context of omnichannel services, the increasing digitization of interactions, and rising consumer expectations. Integrated Unified Communications as a Service (UCaaS) and Contact Center as a Service (CCaaS) solutions offer a fast track to efficiency, productivity, and stakeholder satisfaction.

Evaluating how a unified cloud communication vendor protects internal communications and external patient communications to maintain your organization's security and data privacy is an essential area of focus. According to the US Department of Health and Human Services, approximately 70% of organizations are not "HIPAA compliant."

CHAPTER 1

7 questions to ask a cloud communications vendor about HIPAA compliance

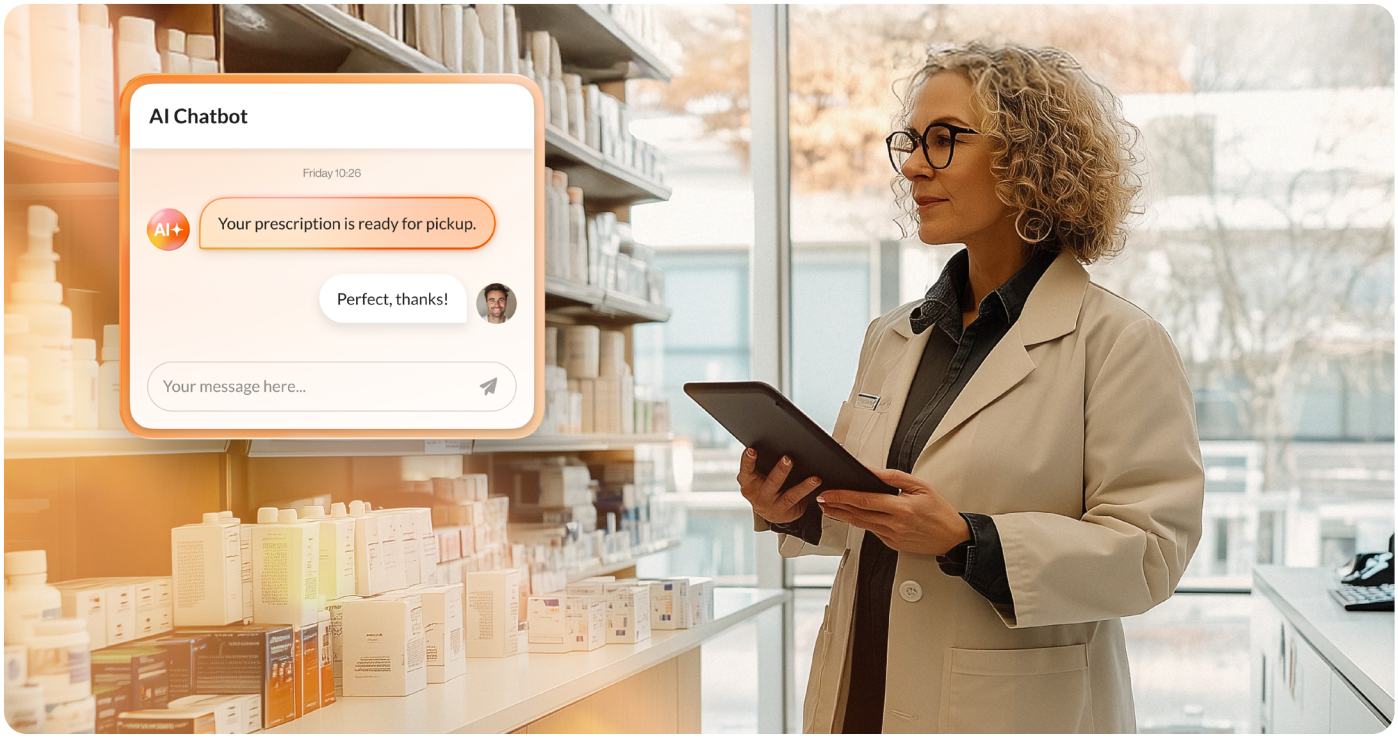
In 2023, the price of a HIPAA violation increased to adjust for inflation. HIPAA violations are now subject to penalties of up to $60,226 per violation and up to $1,919,173 per calendar year. Needless to say, choosing the right cloud communication solution to stay compliant with today's privacy laws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

Here are seven questions to ask a cloud 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, modern security and administrative policy controls protecting phone, video, and messaging collaboration?
5. Have they achieved independent, globally recognized third-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 99.999% 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.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of protected health information (PHI).

What PHI is protected under HIPAA?

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.

What are PHI indicators?

- Names and addresses
- All elements of dates related to an individual's birth, admission to a healthcare facility, or date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security number (SSN)
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Device identifiers and serial numbers
- URLs or IP addresses
- Biometric identifiers (including finger and voice prints)

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 associate 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.

What is ePHI?

ePHI is "Electronic Protected Health Information." ePHI is PHI created, received, maintained, or transmitted electronically.

Who needs to comply with HIPAA?

Covered entities: This category includes healthcare providers, health plans, and healthcare clearinghouses. Providers are hospitals, clinics, nursing homes, doctors' offices, and entities that are paid to provide healthcare.

Business associates: A person or organization outside of the covered entity who performs certain defined functions or activities involving PHI on behalf of the covered entity. 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 certifying that 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 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.

CHAPTER 3

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

RingCentral annually undergoes third-party audits to certify that our services conform to globally recognized standards for privacy and security.

One of the most recognized standards is the SOC 2 + HIPAA report, which covers controls around the availability, security, and confidentiality of customer data. The SOC 2 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

CHAPTER 4

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

What supported use cases do you absolutely need for uncompromising security, privacy, and HIPAA compliance? And how can you know with certainty that your platform doesn't present a risk to your brand trust or bottom line?

Here's the essential security formula:

1. Rigorous information security protection
2. Comprehensive data privacy and compliance management
3. Best practice security and administrative policy controls

1. Information security protection

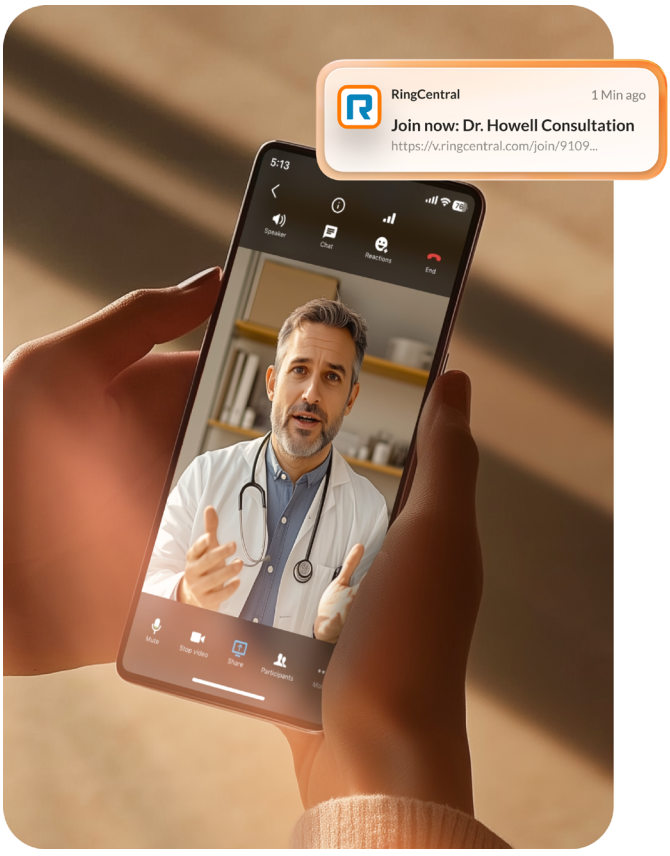
Reliability and uptime will serve as the linchpin for your platform's foundation of trust, assuring your business continuity. Regarding keeping information assets secure, demonstrating cloud security, and committing to safeguard personal data, ISO/IEC 27001 standards are widely known as leading benchmarks 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 they have applied best-of-breed technologies and stringent operational processes to ensure your data is always rigorously protected.

This should also include details on the security practices of the 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 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, 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 followed.

Your vendor should employ an exhaustive system to prevent the inadvertent or intentional compromising of protected data. Moreover, 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 that they respect your company's data privacy.

Your vendor should enforce stringent data privacy policies, documented in a comprehensive data privacy notice and made publicly 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 communications 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.

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 from the very beginning of our development processes.

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 proactively monitor and optimize 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. We have 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 and data privacy and compliance management

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.

ALWAYS ON

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.

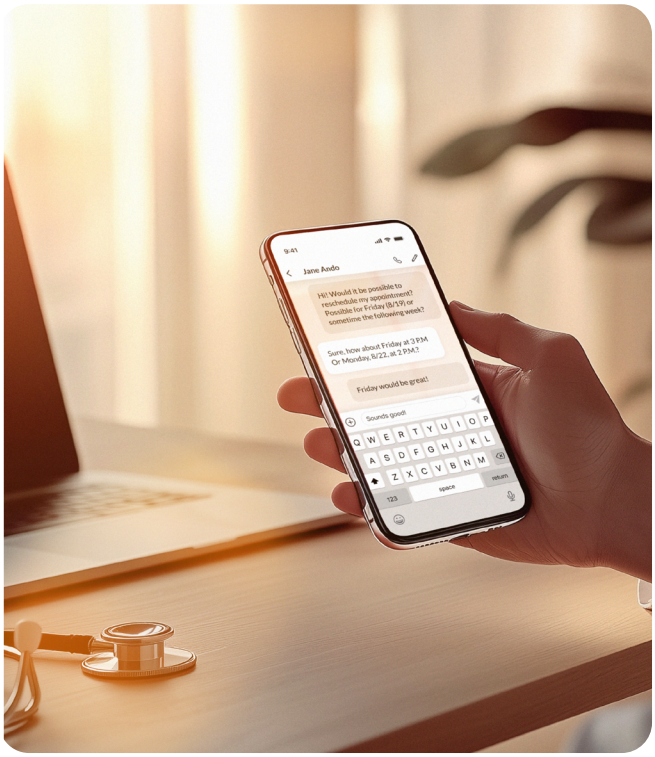
In addition, we run internal and external network vulnerability assessments against our information processing systems at least quarterly to consistently evaluate our network security program.

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 routinely monitors traffic and is always 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 applicable law. It also includes administrative, technical, and physical safeguards 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. It includes in-depth security measures for asset management, configuration management, malicious code protection, vulnerability and patch management, and 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 generally available or expected to be known to the public) and confidential data (i.e., data 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). This verifiable framework enables healthcare organizations and providers to demonstrate their security and compliance consistently and efficiently.

Based on the US healthcare laws HIPAA and the HITECH Act, the CSF sets out requirements for the use, disclosure, and protection of individually identifiable health information and enforces compliance.

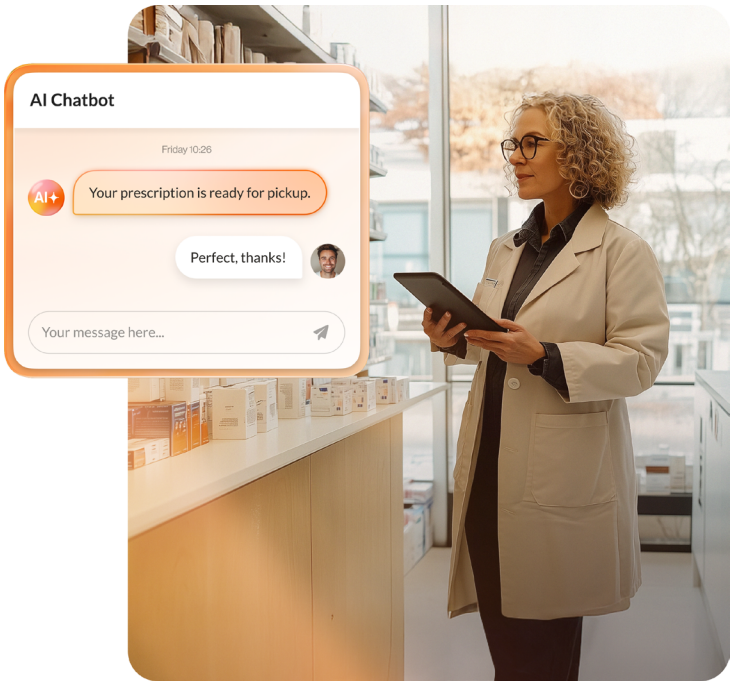
Additionally, the CSF includes healthcare-specific security, privacy, and other regulatory requirements from recognized frameworks like the Payment Card Industry Data Security Standard (PCI-DSS) and the ISO/IEC 27001 information security management standards.

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

CUSTOMIZABLE / DYNAMIC

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
- 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
- Authorized apps manager
- VoIP country blocking
- Centralized IT management of free and paid users
- Audit trail to track changes
- Mobile Application Management vis 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

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, while typical solutions are 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 (including RingCentral) can access your 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.

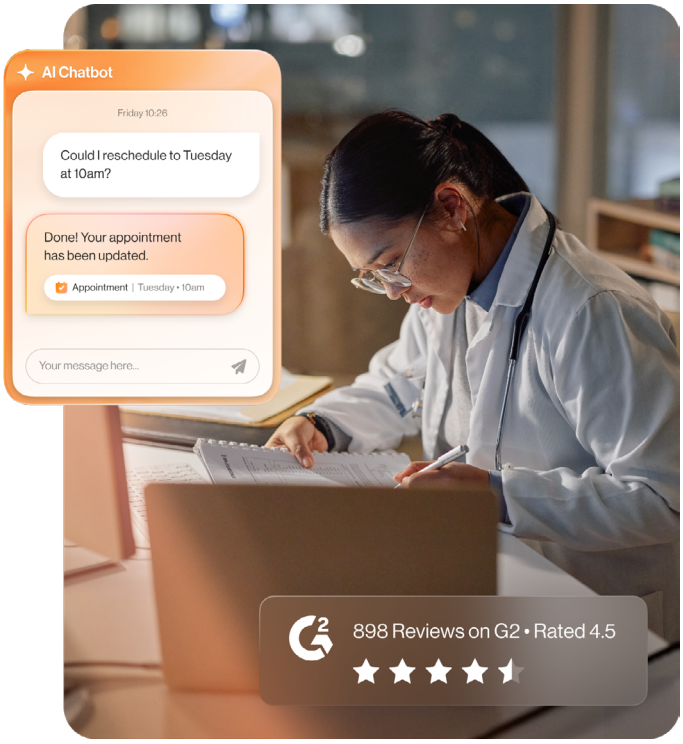
Compliance for chat messages

Company IT admins with the right kind of permissions can access chat data within the RingCentral admin dashboard. If needed, company IT admins can grant third party auditors the ability to access the data. Even so, RingCentral will never gain access to your company's message 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 the buying criteria for trusted healthcare customer experiences, you'll find winning platforms with RingEX, our unified communications solution, and RingCX, our cloud contact center.

RingCentral offers a fundamentally different approach to global trust for your unified communications and contact center platforms. From our industry-leading five 9s in comprehensive information security protection and uptime reliability to HIPAA-compliance to our comprehensive information security 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 ten consecutive years being named as a Leader in the Gartner Magic Quadrant for UCaaS.

Our approach delivers "always-on" information security protection and data privacy management that keeps your data safe and compliant with the law. 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.

About RingCentral

RingCentral Inc. (NYSE: RNG) is a leading provider of AI-driven cloud business communications, contact center, video and hybrid event solutions. RingCentral empowers businesses with conversation intelligence, and unlocks rich customer and employee interactions to provide insights and improved business outcomes. With decades of expertise in reliable and secure cloud communications, RingCentral has earned the trust of millions of customers and thousands of partners worldwide. RingCentral is headquartered in Belmont, California, and has offices around the world.

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com

03/2025