GoTo Connect

COMPLIANCE GUIDE

HIPAA Guide

This guide provides an overview of GoTo Connect's security features and operational practices designed to support healthcare use cases subject to HIPAA. It outlines the respective responsibilities of GoTo and its customers when using the platform in environments where customer-provided content may include electronic protected health information (ePHI). This guide is intended for informational purposes only and does not constitute legal advice.

HIPAA establishes national standards in the U.S. for protecting protected health information (PHI) and applies to covered entities, such as healthcare providers, health plans, and clearinghouses, as well as their business associates. The HIPAA Security Rule focuses on safeguarding ePHI by ensuring its confidentiality, integrity, and availability, protecting against reasonably anticipated threats, and requiring appropriate administrative, physical, and technical safeguards.

GoTo Connect platform

GoTo Connect is an all-in-one, cloud communications platform that includes a cloud phone system, meetings, contact center and customer experience (CX) capabilities, and AI-assisted features such as AI Receptionist and call summaries. GoTo Connect is used by organizations across many industries, including healthcare, and may process customer-provided content that can include ePHI when configured and used by HIPAA-regulated customers. The platform also supports integrations with common business and healthcare-adjacent tools.

Shared responsibility model

HIPAA compliance is a shared responsibility between GoTo and our customers. When GoTo Connect is used by HIPAA-regulated customers under a Business Associate Agreement (BAA), GoTo is responsible for implementing and maintaining appropriate platform safeguards, while customers are responsible for configuration, access governance, and appropriate use.

Customer responsibilities typically include:

- Determining whether PHI is permitted within specific communication channels.
- Implementing internal policies and procedures for workforce access and training.
- Configuring access controls, authentication policies, and user permissions.
- Managing endpoint security (devices, networks, and local storage).
- Establishing retention and deletion policies aligned to organizational requirements.

How GoTo Connect supports HIPAA Security Rule safeguards

GoTo Connect supports safeguards relevant to the HIPAA Security Rule through layered access controls, encryption, audit logging, and secure platform operations. The platform provides technical capabilities that help covered entities and business associates address applicable Security Rule requirements, subject to appropriate customer configuration and use.

GoTo Connect provides the following platform-level capabilities:

- Access controls and authentication to ensure only authorized users can access communications features and data.
- Encryption in transit and at rest to protect ePHI across networks and within the service platform.
- Audit logging to track administrative changes, access activity, and configuration updates.
- Integrity safeguards for stored communications data (e.g., voicemail, recordings, transcripts) and system components.
- Availability measures supporting operational continuity and emergency access procedures.

HIPAA Technical Safeguards mapping (GoTo Connect)

The following table summarizes GoTo Connect capabilities that support HIPAA Technical Safeguards under 45 CFR §164.312.

Requirement	Description	GoTo Connect support
Access control		
Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.	Each user is assigned a unique user account and a unique extension. User access is authenticated using unique credentials directly associated with the user account.
Authentication	Require user authentication prior to access.	Users must authenticate before accessing GoTo applications and administrative interfaces.
Access management	Limit access to authorized persons or programs.	Administrative controls allow customers to assign roles, restrict features, and manage access to calling features and call data in accordance with least-privilege principles.
Emergency access procedure	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. an	GoTo is designed to support service availability and operational continuity. Customers are responsible for defining and implementing emergency access procedures, including the assignment of appropriate administrative privileges. Authorized administrators can update permissions as needed.
Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	GoTo applications support automatic logoff.
Encryption and decryption	Implement a mechanism to encrypt and decrypt electronic protected health information.	Customer content is encrypted in transit and at rest within the GoTo Connect platform.

Requirement	Description	GoTo Connect support
	Audit Controls	
Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	GoTo Connect can generate audit logs for administrative and configuration-related activities, including changes to user roles, permissions, and system settings. Product infrastructure logging is in place.
	Integrity	
Integrity	Implement policies and procedures to protect ePHI from improper alteration or destruction.	GoTo Connect incorporates access controls and system-level protections designed to help prevent unauthorized alteration or deletion of stored communications data, such as voicemail, recordings, transcripts, and messages. Platform policies and operational procedures support the integrity of underlying infrastructure and services.
Integrity mechanism	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	GoTo employs integrity mechanisms at the infrastructure and platform level. All executables are digitally signed. Immutable audit logs record access and changes with timestamps to detect unauthorized alteration or destruction.
	Person or Entity Authentication	
Authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	GoTo Connect requires users to authenticate using a unique user account and associated credentials before accessing GoTo Connect applications and administrative interfaces.

Requirement	Description	GoTo Connect support
Transmission Security		
Transmission security	Protect ePHI transmitted over a network.	GoTo Connect employs network security controls and secure communication protocols designed to protect customer-provided content transmitted between client devices, service components, and supporting infrastructure. Secure connections are used for applicable APIs and service-to-service communications.
Integrity controls	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Policies and procedures protect the integrity of APIs, secure connections, and network infrastructure.
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Customer-provided content, including content that may contain ePHI, is protected in transit using industry-standard encryption protocols, consistent with GoTo's information security standards and risk management practices.

Recommended customer configuration checklist

The following configuration practices are recommended to help customers use GoTo Connect in a manner consistent with HIPAA Security Rule expectations. Customers should assess and implement configurations based on their own risk assessments, policies, and regulatory obligations.

- Enforce strong authentication policies and unique user credentials.
- Restrict administrative privileges to minimum necessary personnel.
- Configure calling permissions and access to sensitive groups.
- Review audit logs for access changes and administrative actions.
- Define organizational rules for recordings, transcripts, voicemail, and SMS use.
- Apply endpoint security (device encryption, OS updates, antivirus/EDR).
- Establish incident response and breach notification procedures.

Feature recommendations for HIPAA-aligned use

The following guidance is intended to help customers configure and use specific GoTo Connect features in a HIPAA-aligned manner. Customers should apply the minimum-necessary standard and align use with internal policies and risk assessments.

- Voice: Limit access to call recordings and voicemail to authorized staff; use least-privilege roles and review access regularly. Avoid sharing PHI over speakerphone, in public, or in unsecured environments.
- Faxing: Use faxing only when required by policy; verify recipient numbers before sending. Restrict access to inbound and outbound fax logs; use coversheets that do not contain PHI; and apply retention policies for stored fax content.
- Messaging: Share PHI via messaging only when permitted by your organization's policies. Limit recipients to authorized users and avoid sending PHI to external parties unless approved.
- AI usage: Apply AI features (e.g., summaries or insights) only when approved by and when used in accordance with your organization's policy. Restrict access to AI-generated outputs, validate accuracy before using in clinical workflows, and retain or delete AI artifacts per your retention policy.
- Integrations: Enable only the integrations required for your workflows (e.g., contact sync, text reminders, call log) and restrict access to integrated data to authorized staff. Before enabling integrations such as contact sync or text reminders, assess whether the use of PHI is appropriate and aligns with your organization's policies, as these features may involve storing or transmitting patient-related information. Review third-party integration configurations to confirm they align with your BAA obligations, and apply retention and deletion policies to any PHI surfaced through connected workflows.

Business Associate Agreements (BAA)

Our standard terms of service incorporate a BAA that applies where GoTo processes PHI for your organization. You can review our BAA here.

Certification and Attestations

GoTo undergoes regular independent audits and maintains certifications and attestations to support its security and privacy programs and to align with industry standards, customer commitments, and applicable laws. GoTo Connect provides platform-level safeguards designed to support HIPAA-regulated use cases, however customers remain responsible for ensuring their own HIPAA compliance obligations are met.

In addition to ongoing security and privacy audits, GoTo has engaged an independent third party to assess and attest to the implementation of HIPAA Security Rule safeguards for select products, including GoTo Connect related HIPAA obligations are addressed through a shared responsibility model, with Privacy Rule requirements governed by contractual and policy controls and Breach Notification Rule obligations fulfilled by notifying affected customers in accordance with applicable law and contractual commitments.. This assessment evaluates the design and operating effectiveness of applicable administrative, physical, and technical safeguards and provides an external validation of GoTo's HIPAA controls. GoTo follows trusted frameworks and maintains certifications across three areas:

Privacy & Data Protection

- TRUSTe Enterprise Privacy & Data Governance

Security & Compliance

- AICPA SOC 2 Type II and SOC 3 Type II
- BSI C5 (Cloud Computing Compliance Criteria Catalogue)

Regulatory & Financial Controls

- Internal controls assessment under PCAOB annual audit
- HIPAA assessed for select products

In addition, GoTo supports lawful international data transfers through the following frameworks:

- EU-U.S. Data Privacy Framework (DPF), UK Extension to the DPF, and Swiss-U.S. DPF
- EU Standard Contractual Clauses (EU SCCs) and UK Addendum
- Brazilian Standard Contractual Clauses (CD/ANPD No. 19)
- Global Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications
- APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications

GoTo partners with reputable independent third-party vendors to conduct annual penetration testing, ensuring the identification and remediation of potential vulnerabilities. For inquiries regarding certifications, attestations, or audit reports, customers may visit GoTo's Trust Center or contact GoTo directly through formal channels. Support and additional resources:

- GoTo Connect overview
- HIPAA Security Rule
- GoTo Trust Center