Interpreter HIPAA security and compliance overview

Overview

Interpreter provides a real-time transcription and translation platform designed for over-the-phone interpreters. The platform converts spoken audio into text across 60+ languages with low latency and delivers live translations during interpreting sessions.

Interpreter is designed so that Protected Health Information (PHI) never reaches Interpreter's servers. Audio streams directly from the user's browser to the speech recognition provider and is not stored. Transcripts are rendered in the user's browser and are not sent to or retained by Interpreter.

The only data Interpreter stores is basic account information (email, name) and session duration for billing purposes.

When customers require a Business Associate Agreement (BAA), one is available upon request.

HIPAA alignment

Interpreter's architecture eliminates PHI from Interpreter's infrastructure by design. Audio and transcript data are processed outside of Interpreter's servers, and only minimal account data is stored.

Interpreter maintains security practices aligned with the HIPAA Security Rule across the following categories:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

Administrative safeguards

Interpreter implements administrative safeguards to manage systems and account data securely:

Access management

- Role-based access control
- Authentication via Google OAuth 2.0
- Session-based access with automatic expiry
- Users can access only their own account data

Vendor management

- Security assessment of third-party service providers
- Speech recognition provider holds SOC 2 Type II and ISO/IEC 27001 certifications
- Payment processing handled by PCI-compliant provider (Dodo Payments)
- Contractual data protection obligations with subprocessors

Incident response

- Incident response procedures
- Automated detection and termination of inactive sessions
- Webhook signature verification for payment events

Technical safeguards

Interpreter applies technical safeguards to protect account data and platform infrastructure.

Encryption

- Encryption in transit: all data transmitted to and from the platform is encrypted using TLS
- Database connections use encrypted protocols
- Secrets and API keys managed through Infisical and never stored in source code

Access control

- Strong authentication requirements via Google OAuth
- Secure session cookies (HttpOnly, Secure, SameSite)
- Rate limiting on all API endpoints

Audit controls

- Logging of system activity and access events
- Monitoring for unauthorized access or anomalous activity
- Automated session lifecycle management

Transmission security

- Secure API access using encrypted connections (HTTPS)
- WebSocket connections encrypted via WSS
- Authentication mechanisms to protect API endpoints
- CORS policy restricting access to authorized origins

Physical safeguards

Interpreter leverages cloud infrastructure providers that maintain industry-standard physical security controls for their data centers, including:

- Controlled facility access
- Environmental protections
- Redundant power and network connectivity
- 24/7 monitoring and surveillance

Data handling and storage

Interpreter does not store audio or transcripts. Audio streams directly from the user's browser to the speech recognition provider, is processed transiently, and is discarded. Transcripts are generated by the speech engine and rendered in the user's browser only.

Key data handling principles:

- Audio is never transmitted to or stored on Interpreter's servers
- Transcripts are never transmitted to or stored on Interpreter's servers
- The only data stored is account information (email, name) and session duration
- Payment card data is handled entirely by the payment processor (Dodo Payments) and is never stored by Interpreter
- Users can delete their account and all associated data at any time

Business Associate Agreement (BAA)

Although Interpreter does not store or process PHI, a BAA is available upon request for customers who require one for their compliance programs.

The speech recognition provider also offers BAAs separately.

Customers can request a BAA by contacting the Interpreter compliance team.

Certifications and security program

Interpreter's speech recognition provider maintains a comprehensive security program with independent certifications:

- SOC 2 Type II
- ISO/IEC 27001:2022
- HIPAA BAA available

Shared responsibility

Interpreter secures the platform infrastructure and ensures that audio and transcript data never reach its servers. Customers are responsible for:

- Managing access to their accounts
- Complying with applicable healthcare regulations in their jurisdiction
- Determining whether their specific workflow requires a BAA

Contact

For HIPAA-related questions or to request a BAA, contact:

Interpreter Security and Compliance security@useinterpreter.com