HIPAA Compliance Datasheet

HIPAA Compliance

The Health Insurance Portability and Accountability Act and supplemental legislation collectively referred to as the HIPAA rules (HIPAA) lay out privacy and security standards that protect the confidentiality of protected health information (PHI). In terms of Krisp systems, the solution and security architecture must comply with the applicable standards, implementation specifications and requirements with respect to electronic PHI of a covered entity.

The general requirements of HIPAA Security Standards state that covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.

4. Ensure compliance by its workforce.

How Krisp Enables HIPAA Compliance

In the course of providing services to healthcare customers, we have put in place multiple measures and procedures to ensure we meet HIPAA requirements. In provisioning and operating the Krisp HIPAA Services, Krisp complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate.

Krisp is responsible for enforcing the administrative, technical and physical safeguards to prevent any unauthorized access to or disclosure of protected health information (PHI) in the Krisp environment.

The following table demonstrates how Krisp supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).

HIPAA Standard	How Krisp Supports the Standard
Access Control	
• Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs. • Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity. • Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency. • Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. • Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	• Data in motion is encrypted minimum with TLS 1.2. • Data at rest is encrypted at the application layer using Advanced Encryption Standard (AES)-256 algorithm. • RBAC with least privilege principle for owner, admin, and members. • Each user has a unique user identification (ID). • Automatic logoff is implemented to terminate a user's session after a predetermined time of inactivity. • Policies and procedures are implemented to protect PHI from improper alteration or destruction. • Audit controls are implemented to record and provide the ability to examine PHI access and processing activity. • Krisp leverages a redundant and distributed architecture to offer a high level of availability and redundancy. • Emergency access procedures are established for obtaining and accessing PHI during an emergency (HIPAA 164.312 Technical Safeguards, 2003)
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.	• Data in motion traverses Krisp's secured and distributed infrastructure. • Platform connections are logged for quality-of-service purposes. • Account admins have secured access to manage individual, group, or organization level management.

HIPAA Standard	How Krisp Supports the Standard
Integrity	
• Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multilayer integration protection is designed to protect both data and service layers. • Controls are in place to protect and encrypt data.
Integrity Mechanism	
• Mechanism to authenticate electronic protected health information. • Implemented methods to corroborate that information has not been destroyed or altered.	• Application executables are digitally signed. • Data connections leverage minimum TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. • Web and application access are protected by verified email address and one-time generated magic code.
Person or Entity Authentication	
• Verify that the person or entity seeking access is the one claimed.	• Application access is protected by verified email and magic code (a random magic code is sent to the user's email every at every login attempt). • Google sign-in (OAuth 2.0). • SAMLv2 based SSO (for team plans). • Krisp backend doesn't store passwords.
Transmission Security	
• Protect electronic health information that is stored on the Krisp platform. • Integrity controls: Ensure that protected health information is not improperly modified without detection. • Encryption: Encrypt protected health information.	• Data in transit is protected with minimum TLS 1.2 (enforced throughout all our services without any exception). • Data at rest (all production databases and customer data) is protected with AES-256 (no exception).

Security & Encryption

Healthcare organizations and account administrators need to have the tools and technology to ensure they're meeting HIPAA standards. Here are just a few safeguards that enable you to ensure the security and privacy of protected health information (PHI).

- Data in motion is encrypted using minimum TLS 1.2 encryption.
- All production databases and customer data are encrypted at rest with AES-256.

HIPAA Certification

Currently, the agencies that certify health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Security Rule), nor accredit independent agencies to do HIPAA certifications. Additionally, the HITECH Act only provides for testing and certification of Electronic Health Records (EHR) programs and modules.

Thus, as Krisp is not an EHR software or module, our type of technology is not certifiable by these unregulated agencies.

Other Security Certification

SOC2: The SOC 2 report provides third-party assurance that the design of Krisp, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.