# HIPAA compliance

The Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations restrict KrispCall's abilities to use and disclose protected health information.

As per the requirement of HIPAA standards, the Covered Entities must:

- Ensure the confidentiality, integrity, and availability of all electronic personal health information (ePHI) that the Covered Entity creates, receives, maintains, or transmits.
- Protect yourself against any reasonably anticipated threat or danger to the security or integrity of this information.
- Protect yourself against any reasonably anticipated use or disclosure of this information that is not permitted or required by privacy regulations.
- Ensure Compliance with your staff.

KrispCall is HIPAA compliant and follows all the practices to meet HIPAA criteria, which includes;

## Authentication

Each agent is assigned a specific role so that they are required to use their own unique account to access the services of KrispCall.

## Encryption

Transport Layer Security (TLS), virtual private networks (VPN), and other encryption technologies are used to protect data.

## Call Logs

KrispCall records all call data, including metadata and administrative functions performed during calls.

## Business Associate Agreement

Business Associates are VoIP providers that store ePHI. They need to sign a Business Associate Agreement (BAA) with covered entities to ensure that associates comply with the HIPAA rule. *Note: Qualifying customers who require a contractual agreement regarding safeguards on PHI can apply to enroll in a Business Associate Agreements (BAA) program as well.*

Besides the security practices mandated by HIPAA, such as encryption of data at rest, KrispCall enables its users to protect Protected Health Information (PHI) in faxes, voicemails, and call recordings via HIPAA setting. All voicemails, faxes, and call recordings are deleted within 30 days with the setting in place.