TeleSensi HIPAA Compliance

TeleSensi is a web application streaming stethoscope data from a patient to a specialist consultant over a secure network, enabling the specialist to diagnose possible heart, lung and internal defects.

The Health Insurance Portability and Accountability Act (HIPAA) lays out privacy and security standards that protect the confidentiality of patient health information. In terms of stethoscope streaming, the solution and security architecture must provide end-to-end encryption and meet access controls so data in transit cannot be intercepted.

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

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information 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.

TeleSensi Enables HIPAA Compliance

We sign the HIPAA Business Associate Agreement (BAA) for our healthcare customers, meaning we are responsible for keeping your patient information secure and reporting security breaches involving personal healthcare information. We do not have access to identifiable health information and we protect and encrypt all audio sharing data.

How Tele-Sensi Enables HIPAA Compliance.

TeleSensi has several characteristics that make it easy to protect the confidentiality of protected health information:

1. **Peer-to-Peer Sessions**: TeleSensi uses a managed peer-to-peer architecture, where stethoscope audio is directly streamed from endpoint to endpoint. Information is never stored on any TeleSensi server or intercepted in any way. The TeleSensi managed server is only used for connection brokering and user administration.
2. **Encryption**: Encryption adds an additional layer of security. Datagram Transport Layer Security (DTLS) is used to secure all TeleSensi communication channels.

The following table demonstrates how TeleSensi 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).

TeleSensi HIPAA Support Matrix

HIPAA Requirements	TeleSensi Implementation
Technical Safeguards (§164.312)	
Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. **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 protected health information during an emergency. **Automatic Logoff**: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. **Encryption & Decryption**: a mechanism to encrypt and decrypt electronic protected health information.	• Multi-layered access control for owner, admin, and members. • Web and application access are protected by verified email address and password. • Meeting access is protected by password. • Meetings are not listed publicly. • Meeting host can easily disconnect attendees or terminate sessions in progress. • Meeting data transmitted across the network is protected using Datagram Transport Layer Security. Generated encryption keys are distributed to all participants start of each session. • Meeting ends automatically with timeouts.
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.	• Meeting connections traverse TeleSensi's secured and distributed infrastructure. • Meeting connections are logged for audio and quality-of-service purposes. • Account admins have secured access to meeting management and reports.
Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multi-layer integrity protection is designed to protect both data and service layers. • Controls are in place and protect data in motion and at-rest.
Mechanism to authenticate electronic protected health information: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	• The web server application installed on the local computer is not able to connect to the internet, all data is passed to the web portal. • An SSL/TLS certificate is used to protect communication with the web service.

Person or entity authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	• Web and application access are protected by verified email and password. • Meeting host must log into TeleSensi using a unique email address and account password. • Data sharing is under the host's control.
Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. **Integrity controls**: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. **Encryption**. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	End-to-end data security protects passive and active attacks against confidentiality. All media streams sent using the Telesensi web application are securely encrypted. The encryption protocol used depends on the data being sent. Chat messages are encrypted using Datagram Transport Layer Security (DTLS) and the audio data stream is encrypted using Secure Real-time Transport Protocol (SRTP)

Security and Encryption

Only members registered by account administrators can get access to a TeleSensi streaming session by means of an unique ID and password. Each meeting can only have one host and consultant. The host has complete control of creating a consultation room and inviting a consultant. A unique room ID is created that is share with a participant through an own communication channel of choice. Both the host and consultant can terminate a meeting or mute/unmute the audio streaming. This host is able to connect or disconnect the electronic stethoscope at choice.

All media streams sent using the Telesensi web application are securely encrypted. The encryption protocol used depends on the data being sent. Chat messages are encrypted using Datagram Transport Layer Security (DTLS) and the audio data stream is encrypted using Secure Real-time Transport Protocol (SRTP).

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