# HIPAA Compliance

## How We Comply with HIPAA

As part of the process of providing services to healthcare customers, CAPTIV8 Share telemedicine does not access PHI (Personal Health Information). Rather, for purposes of compliance with HIPAA, we model our compliance under the “conduit exception” which applies to entities that transmit PHI but do not have access to the transmitted information. That said, to avoid any doubt we offer all our customers in the United States with a Business Associate Agreement (BAA) which downloaded within the app.

The CAPTIV8 Share App applies specific criteria to healthcare in order to eliminate a customer’s ability to transmit PHI. We do not have access to identifiable PHI and we protect and encrypt all audio, video, and screen sharing data. All multimedia (audio and video data) is sent Peer-to-Peer i.e. from the Customers device directly to the Patient in an encrypted stream so that only the sender and receiver can read what is sent.

Authentication processes have been implemented to ensure meeting requests are coming from the correct sources and not from a malicious 3rd party using TLS encryption and HTTPS URLs to validate meetings with HMAC-SHA1 authentication token signatures.

## Security & Encryption

Telemedicine consultations can only be initiated by the account owner. Only one account owner is permitted per account. The account owner may invite only one individual and virtual meetings are locked to only allow 2 people in any given meeting. The account owner (or host) can screen share and the host has complete control of the meeting with features such as mute/unmute and end meeting.

Optimed

August 2020

CAPTIV8 Share telemedicine utilises Peer-to-Peer WebRTC (real-time communication) with industry-standard Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings. As a result of the Peer-to-Peer protocol, recordings of virtual consultations are not possible, therefore, there is no storage of the consultation within the CAPTIV8 Share platform.

## Screen Sharing

Screen Sharing allows healthcare professionals to display other apps and data on their device to the Receiver (normally the patient). Screen sharing data is also transmitted Peer-to-Peer and encrypted. There is no facility to record screen sharing or consultations.

The following itemised list demonstrates how CAPTIV8 Share telemedicine 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 | CAPTIV8 Share Telemedicine Standard |
|---|---|
| Access Control:<br>• 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.<br>• Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.<br>• Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency.<br>• Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.<br>• Encryption and Decryption: Implement a mechanism to encrypt and decrypt | • Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 256-bit key generated and securely distributed to all both participants at the start of each session.<br>• Access control for the account owner, only one user per account.<br>• Application access is protected by verified email address and password.<br>• Telemedicine consultations are not listed publicly and cannot be scheduled at a future date/time.<br>• CAPTIV8 Share telemedicine architecture offers a high level of availability and redundancy.<br>• Meeting host can terminate meeting sessions. |

| | |
|---|---|
| electronic protected health information. | • Host can conduct telemedicine consultations with a single person.<br>• Meetings end automatically after 30 minutes. |
| Audit Controls:<br>• 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 are connected on a Peer-to-Peer network. Audio and video data do not enter the CAPTIV8 Share infrastructure or the infrastructure of any Partners.<br>• Account owners have secured access to meeting management. |
| Integrity:<br>• Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | • Media is encrypted end-to-end (E2E) using WebRTC security protocols.<br>• There is no facility to edit or delete PHI |
| Integrity Mechanism:<br>• Mechanism to authenticate electronic protected health information.<br>• Implemented methods to corroborate that information has not been destroyed of altered. | • Application executables are digitally signed.<br>• WebRTC uses Secure Real-Time Transport Protocol (SRTP) to encrypt, authenticate, and protect your data and conversations. |
| Transmission Security:<br>• Protect electronic health information that is being transmitted over a network.<br>• Integrity controls: Ensure that protected health information is not improperly modified without detection.<br>• Encryption: Encrypt protected health information. | • Data encryption protects against passive and active attacks on confidentiality.<br>• WebRTC uses Secure Real-Time Transport Protocol (SRTP) to encrypt, authenticate, and protect your data and conversations.<br>• TLS encryption and HTTPS URLs are used to validate meetings with HMAC-SHA1 authentication token signatures to ensure meeting requests are coming from the correct sources and not from a malicious 3rd party. |
| Person or Entity Authentication:<br>• Verify that the person or entity seeking access is the one claimed. | • Web and application access are protected by verified email and password.<br>• Meeting host must log in to CAPTIV8 Share app using a unique email address and account password.<br>• Only the Host can control screen sharing. |