HIPAA COMPLIANCE GUIDE

OHMNILABS

HOW OHMNILABS ENABLES **HIPAA COMPLIANCE**

We sign the HIPAA Business Associate Agreement (BAA) for our healthcare customer, 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 and video data.

The following table demonstrates how OhmniLabs 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).

ACCESS CONTROL

HIPAA STANDARD	HOW WE SUPPORT THE STANDARD
• 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.	• All user and device data are stored in a redundant infrastructure that maintains periodic backups. • User and device data are only available to OhmniLabs administrators through a password-enabled data portal on a private VPN network. • Users receive different levels of permission that determine operations they are allowed to perform when using the system. • Users are identified by unique user IDs, usernames and email addresses. • Passwords are hashed using Bcrypt. • All data is protected using hard disk encryption. • Inactivity on the user dashboard will result in automatic logoff of the system after 48 hours of inactivity. • All streaming and data transfers are protected by TLS 1.2, DTLS and SRTP security protocols using AES 256 encryption cipher.

© 2021 OhmniLabs Inc.

AUDIT **CONTROLS**

HIPAA STANDARD

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

HOW WE SUPPORT THE STANDARD

Device connections, statuses and user activities are logged for review by account administrators and OhmniLabs administrators.

INTEGRITY

HIPAA STANDARD

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

HOW WE SUPPORT THE STANDARD

Access to data is protected through VPN private networks, password and certificate protected systems. Authorization from OhmniLabs administrators is required to access any data.

INTEGRITY **MECHANISM**

HIPAA STANDARD

- Mechanism to authenticate electronic protected health information.
- Implement methods to corroborate that information has not been destroyed or altered.

HOW WE SUPPORT THE STANDARD

- Application binaries and device firmware are digitally signed to prevent tampering.
- Data transmitted are encrypted using DTLS and SRTP security protocols using AES 256 encryption cipher.

PERSON OR ENTITY AUTHENTICATION

HIPAA STANDARD

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

HOW WE SUPPORT THE STANDARD

User logins are protected by unique usernames and password combinations or Single-Sign-On systems with added integration.

© 2021 OhmniLabs Inc.

TRANSMISSION **SECURITY**

HIPAA STANDARD

- Protect electronic health information that is being transmitted over a network.
- Integrity controls: Ensure that protected health information is not improperly modified without detection.
- Encryption: Encrypt protected health information.

HOW WE SUPPORT THE STANDARD

- Streaming data like video, audio and robotic controls are protected by DTLS 1.2 and SRTP security protocols.
- Access to user dashboards and OhmniLabs website are protected by TLS 1.2 security protocol.
- All data is signed by AES 256 encryption cipher.

SECURITY AND **ENCRYPTION**

Each user needs to be granted access to Ohmni® robot(s) by the administrators to be able to dial into and control the robot(s). Only one user can control a robot at a time. The user has complete control of the robot(s) and can change the settings, take snapshots (only available on Ohmni Supercam), invite others, and end call.
OhmniLabs employs industry-standard, end-to-end Advanced Encryption Standard (AES) encryption using 256 encryption cipher to protect calls. OhmniLabs fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.
Medical professionals and authorized healthcare partners can use Ohmni to meet with patients and other healthcare professionals to discuss health information and other resources.
OhmniLabs does not distribute the actual patient data. OhmniLabs further protects data confidentiality through a combination of encryption, strong access control, and other protection methods.

ABOUT **OHMNILABS**

We are changing the way people communicate by providing demand-driven robotics solutions. Ohmni® is an award-winning telepresence robot that transforms how people connect with co-workers, family members, teachers and friends.

QUESTIONS

CONTACT@OHMNILABS.COM | OHMNILABS.COM

© 2021 OhmniLabs Inc.