TrueConf HIPAA-Compliance Statement

What is HIPAA?

HIPAA, the Health Insurance Portability and Accountability Act, is a law protecting patient data. Any company that is connected with electronic protected health information (ePHI) must guarantee that all the necessary security measures are thoroughly followed.

The subjects of HIPAA compliance are **covered entities (CE)**, namely the companies and institutions providing health care assistance, and **business associates (BA)**, the companies supporting medical treatment or consultations and having access to patient personal data.

HIPAA generally provides two rules of compliance: **Privacy Rule** and **Security Rule**. Privacy Rule is designed to ensure that the private patient data, whether electronic, written, or oral, is safely protected. Security Rule, on the other hand, protects electronic information exclusively. Security Rule binds covered entities and business associates to follow the requirements and protect ePHI. Under Security Rule, the entities should protect ePHI against any threats, hazards, or disclosures; guarantee confidentiality, integrity, and availability of ePHI.

Is TrueConf HIPAA-compliant?

TrueConf video conferencing products, both cloud and on-premises software, support HIPAA security standards and are HIPAA-compliant**.** TrueConf guarantees that patient data will not be passed to any third parties.

How does TrueConf support HIPAA standards?

Data access and security

TrueConf Server operates in private networks monitored by our customers and ensures secure connection via SSL/TLS encryption protocols. Data streams (video, audio, and content) are additionally protected using AES-256. Application access is constantly secured by login name and password verification. During video conferencing sessions, hosts can easily disconnect participants or even terminate current session. The system is protected against cyber attacks as the server is located within client's local network or VPN.

Authentication

TrueConf Server and client applications requires to verify login name and password to access the application. Login names are verified to be unique and defined by system administrator who manages the server.

Auditing

TrueConf Server provides audit trails of usage along with extensive log files. Access to meetings management, recordings and reports is secured.

Integrity

Transmitted data and service itself are secured in an integrated manner by means of TrueConf proprietary communication protocol based on TCP and use of SSL/TLS-based connectivity and AES-256 encryption between server and endpoints.

Revision v2, 1st of April 2017.