Veeting Rooms and HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) calls for privacy and security standards that protect the confidentiality and integrity of patient health information. Specifically, if you are transmitting patient data across the internet during an online meeting or video conference, your online meeting solution and security architecture must provide end-to-end encryption and meeting access control so the data cannot be intercepted by anyone other than the invited participants.

Veeting Rooms is an online web conferencing solution that can help your company or office meet these guidelines. The following matrix demonstrates how Veeting Rooms can support HIPAA compliance and is based upon the HIPAA Security Standards rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule). The United States Department of Health and Human Services provides the HIPAA Security Standards on its website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

Technical Safeguards § 164.312

Standards Covered Entities Must Implement	Implementation Specifications R=Required A=Addressable		Key Factors	Support in Veeting Rooms
(a) (1) Access Control		R	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow	• Meeting access is protected by a unique meeting code and optional strong password

Standards Covered Entities Must Implement	Implementation Specifications R=Required A=Addressable		Key Factors	Support in Veeting Rooms
			access only to authorized persons or software programs.	authentication. • Meetings are not listed publicly, and access is restricted to invited participants.
	Unique User Identification	R	Assign a unique name and/or number for identifying and tracking user identity.	• Meeting organizers and account administrators use their unique email address as their login name; they must also enter a unique account password.
	Emergency Access Procedure	R	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	• One-click meetings provide rapid, secure access to an online meeting from virtually anywhere, which may be used as a supplementary method for providing emergency access to healthcare information.
	Automatic Logoff	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	• Website inactivity time-out automatically logs users out of their Veeting Rooms accounts.
	Encryption and Decryption	A	Implement a mechanism to encrypt and decrypt electronic protected health information.	• All sensitive chat, session and control data transmitted across the network is protected using 256 bit

Standards Covered Entities Must Implement	Implementation Specifications R=Required A=Addressable		Key Factors	Support in Veeting Rooms
				SSL/TLS encryption • All audio and video conversations are encrypted with the DTLS-SRTP encryption standard
(b) Audit Controls		R	Implement hardware, software and/ or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• All connection and session activity in Veeting Rooms is logged for security and quality-of-service purposes.
(c)(1) Integrity		A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Only meeting organizers can delete uploaded documents. Uploaded documents cannot be altered after the meeting has ended.
(c)(1) Integrity Mechanism	Mechanism to authenticate electronic protected health information.	A	Implement methods to corroborate that information has not been destroyed or altered.	• All transmitted data is protected by SSL/TLS to ensure the integrity of the data sent between the browser and the server.
(d) Person or Entity Authentication		R	Verify that the person or entity seeking access is the one claimed.	• Meeting organizers must log in to Veeting Rooms using a unique email address and account password. • Meeting access is protected by a unique code. Only invited

Standards Covered Entities Must Implement	Implementation Specifications R=Required A=Addressable		Key Factors	Support in Veeting Rooms
				participants may view shared meeting data.
(e)(1) Transmission Security		R	Protect electronic health information that is being transmitted over a network.	• Veeting Rooms provides true end-to-end data security that addresses both passive and active attacks against confidentiality.
	Integrity Controls	A	Ensure that protected health information is not improperly modified without detection.	• SSL/TLS encrypted HTTP communication ensures data integrity
	Encryption	A	Encrypt protected health information whenever deemed appropriate.	• All sensitive chat, session, video, audio, and control data transmitted across the network is protected using 256 bit SSL/TLS encryption.