8x8 Jitsi as a Service (JaaS)

HIPAA and Privacy Law Compliant Usage Guide

Obligation of Customers Operating Under a Business Associate Agreement or Data Processing Agreement with 8x8

Version 1.0 | Effective Upon Execution of BAA or DPA

IMPORTANT: This Usage Guide sets forth the mandatory and recommended security settings and features that customers must implement when using 8x8 JaaS for sessions involving Protected Health Information (PHI) or personal data. Compliance with this Guide is a condition of 8x8's Business Associate Agreement (BAA) and Data Processing Agreement (DPA) with you. Execution of the BAA or DPA alone does not render a JaaS deployment compliant; proper configuration is required.

1. Introduction

8x8 Jitsi as a Service (JaaS) is a cloud-based video conferencing platform. Organizations using JaaS for sessions in which personal data or PHI may be discussed or displayed — including telehealth consultations, legal or financial advisory sessions, HR meetings, and any other interaction involving identifiable individuals — must configure and operate JaaS in a manner consistent with applicable privacy and data protection law. This Guide identifies the specific JaaS settings and features that are required or recommended to meet that standard.

JaaS meeting security is built on a layered model. JWT-based room authorization is the foundational control: it is the cryptographic front door that governs whether a participant can join a room at all. Room naming practices, the waiting room, and meeting passwords are additional defense-in-depth layers on top of that foundation. This layered structure is reflected in the requirements below.

This Guide applies to customers on two tracks, both of which are subject to the same meeting security requirements. The technical controls that protect personal data and PHI in a JaaS session are identical regardless of which legal framework applies.

	HIPAA Track	Privacy Law Track
Who it applies to	Covered entities and business associates using JaaS for communications involving PHI, operating under an 8x8 BAA	All customers using JaaS for sessions in which personal data may be discussed or displayed, operating under an 8x8 DPA, regardless of jurisdiction

	HIPAA Track	Privacy Law Track
Governing legal framework	HIPAA Security Rule, Privacy Rule, and Breach Notification Rule	Applicable privacy and data protection laws including GDPR, CCPA/CPRA, and equivalent US state and international privacy laws
Reference data category	Protected Health Information (PHI)	Personal data, with heightened requirements for sensitive data
8x8 agreement	Business Associate Agreement (BAA)	Data Processing Agreement (DPA)

A valid, executed BAA or DPA with 8x8 (as applicable) must be in place before JaaS is used for any session that may involve PHI or personal data.

Throughout this Guide, requirements are marked as follows:

MUST	Mandatory. Non-compliance is a breach of the applicable BAA or DPA obligation.
SHOULD	Strongly recommended best practice. Customers who do not implement a SHOULD requirement must document the reason in their risk analysis.

2. Meeting Security Configuration

JaaS meeting security uses a layered model. JWT room authorization is the foundational access control — no participant can join without a valid signed token. The sections below describe that foundational control first, followed by the additional layers that provide defense in depth.

2.1 JWT-Based Room Authorization (Foundational Control)

JWT room authorization is the primary security mechanism for JaaS. It operates at the infrastructure level: a participant cannot join a room at all without presenting a valid JSON Web Token signed by the customer's backend. This cryptographic gate is the front door to every JaaS session and is the foundation on which all other meeting security controls rest.

- **MUST** issue a signed JWT from the customer's server-side application for each participant in each session. JaaS validates the token before permitting the participant to join. Unsigned or missing tokens are rejected at the infrastructure level.
- **MUST NOT** issue JWTs from client-side code or embed long-lived tokens in applications. All token issuance must occur server-side to prevent token theft or reuse.
- **MUST** bind each JWT to the specific room name for that session. A token issued for one room must not be usable to join a different room.
- **MUST** set short token expiration times appropriate to the session duration (e.g., 60–90 minutes). Expired tokens must not be accepted.

- **MUST** integrate JWT issuance with the customer's participant identity verification flow — for example, issuing the token only after a patient has authenticated through a patient portal login or equivalent mechanism.
- **MUST** treat JWT secret compromise as a security incident: invalidate the affected tokens and rotate the signing secret immediately.

2.2 Meeting Room URLs

Even with JWT authorization in place, room naming practices provide an important additional layer of protection. A predictable room name reduces the entropy of the overall system and may assist an attacker in targeting a specific session for token theft or social engineering.

- **MUST NOT** use static, predictable, or publicly advertised room names for sessions involving personal data or PHI. A room name that incorporates the host's name, organization, or professional identity is guessable by anyone aware of that identity.
- **MUST** generate a unique, unpredictable room identifier for each session. Acceptable approaches include UUIDs or randomly generated alphanumeric strings of at least 12 characters. Do not incorporate any personal data into the room name.
- **MUST** communicate session-specific room links to participants through a secure channel (e.g., encrypted portal message or authenticated scheduling system notification). Transmission via unencrypted email is not recommended.

2.3 Waiting Room / Lobby

The waiting room is a recommended host-level verification layer that complements JWT authorization. Because JWT is the foundational access control, any participant who reaches the waiting room has already presented a valid, server-signed token. The waiting room gives the host an additional opportunity to visually confirm who is joining before admitting them, and provides a practical safeguard against token sharing in deployments where JWT issuance is not tightly integrated with a strong upstream identity verification system.

- **SHOULD** enable the JaaS waiting room (lobby) for sessions involving personal data or PHI, particularly where JWT issuance is not integrated with a strong upstream identity verification system such as an authenticated patient portal or SSO.
- **SHOULD** verify each participant's identity (by name displayed in the waiting room) before admission, and not admit any participant whose identity cannot be confirmed.
- **SHOULD** ensure the host is present before any participant is admitted, and remove any participant who cannot be identified after joining.

2.4 Meeting Passwords

Meeting passwords provide an additional factor of protection on top of JWT authorization and unpredictable room names. Given the strength of the JWT control, passwords are a recommended enhancement rather than a mandatory requirement.

- **SHOULD** protect every JaaS session involving personal data or PHI with a meeting password.
- **SHOULD** use a password that is unique to each session and at least 8 characters long, mixing letters and numbers. Do not reuse the same password across sessions and do not use a password derived from personal data.

- **SHOULD** communicate the password to participants through a channel separate from the meeting link where feasible.

2.5 In-Session Participant Controls

- **MUST** limit screen-sharing permissions to authorized participants. Disable screen-sharing for guests or other participants unless operationally necessary.
- **MUST NOT** enable anonymous or guest participation for sessions involving personal data or PHI.
- **SHOULD** transfer host privileges to another authorized participant before the host leaves if the session has not concluded.

3. Encryption

3.1 Transport Encryption (Provided by Default)

JaaS encrypts all audio, video, and data streams in transit using DTLS-SRTP for media and TLS 1.2+ for signaling. This is provided by 8x8 by default and requires no customer configuration. Customers MUST NOT use any proxy or network architecture that terminates TLS/SRTP encryption before media reaches the intended endpoint.

3.2 End-to-End Encryption (E2EE)

- **SHOULD** enable E2EE for sessions involving sensitive data or PHI where technically feasible. When E2EE is active, media is encrypted on the sender's device and decrypted only on the recipient's device, preventing access by any intermediate infrastructure.

E2EE Trade-offs to Evaluate Before Enabling
• E2EE is not compatible with JaaS cloud recording, AI transcription, or certain moderation features — evaluate functional impact before enabling
• E2EE requires all participants to use a compatible, up-to-date browser or client
• When E2EE is not used, JaaS transport encryption and 8x8's contractual safeguards under the BAA or DPA provide a legally adequate baseline
• The decision to use or forgo E2EE must be documented in the customer's risk analysis

4. Key Definitions

Term	Definition
BAA	Business Associate Agreement — a contract governing 8x8's use and disclosure of PHI on behalf of a HIPAA covered entity or business associate customer.
DPA	Data Processing Agreement — a contract governing 8x8's processing of personal data on behalf of a customer, as required by GDPR Article 28, CCPA, and equivalent privacy laws.

Term	Definition
E2EE	End-to-end encryption — media encrypted on the sender's device and decrypted only on the recipient's device.
JaaS	Jitsi as a Service — 8x8's hosted video conferencing platform based on Jitsi Meet technology.
JWT	JSON Web Token — a signed token issued by the customer's backend and validated by JaaS to cryptographically authorize room access. Required for a participant to join any JaaS session.
Personal Data	Any information relating to an identified or identifiable natural person. Includes PHI and all categories of personal information regulated under applicable privacy laws.
PHI	Protected Health Information — individually identifiable health information held or transmitted by a HIPAA covered entity or business associate.
Sensitive Data	A subset of personal data warranting heightened protection, including: health and medical information; biometric data; financial account information; precise geolocation; racial or ethnic origin; sexual orientation or gender identity; immigration status; government-issued identifiers; and information about children.
Waiting Room	A JaaS feature that holds joining participants until the host explicitly admits them.

This document is a contractual obligation under the applicable 8x8 Business Associate Agreement or Data Processing Agreement. For questions, contact your 8x8 Customer Success Manager or privacy@8x8.com.