Jump



OCTOBER 2026

Compliance Resource Guide.

A reference for customers evaluating Jump's practices against their regulatory and compliance obligations.

DOCUMENT
Compliance Resource Guide

TRUST CENTER
security.jump.ai

OVERVIEW

Jump is the AI meeting platform built specifically for financial professionals.

Jump helps customers capture, transcribe, and act on client conversations while meeting the rigorous security and compliance expectations of the financial services industry. This document is a compliance reference resource designed to help customers, their compliance officers, legal counsel, and risk managers evaluate Jump's practices in the context of their regulatory obligations. It is organized around the topics most commonly raised by regulated firms when adopting an AI meeting platform.

IMPORTANT DISCLAIMER

This document is provided for general informational purposes only. Jump does not provide legal, regulatory, or compliance advice. Each customer is solely responsible for determining its own applicable regulatory obligations and for ensuring that its use of Jump meets those obligations. Regulatory requirements vary by jurisdiction and are subject to change. Customers should work with qualified legal and compliance counsel to evaluate their specific obligations.

The descriptions of Jump's practices in this document are accurate as of the date noted and subject to change; customers should consult Jump's Trust Center at security.jump.ai for current documentation.

CONTENTS

01 **Customer controls** 03
Summary of customer-configurable policies and settings.

02 **Recording, disclosure, & consent** 04
Automated disclosures, verbal consent detection, summary-only mode

03 **Books, records, & data retention** 05
Configurable retention, archiving, audit logs, attestation

04 **AI governance & human oversight** 06
Human-in-the-loop, no model training, transparency, bias review

05 **HIPAA & PHI** 07
Business Associate Agreements, third-party security, incident notification

06 **Data security & privacy** 08
Ownership, encryption, data residency

A **Appendix — regulatory mapping summary** 09
Jump's practices mapped to key regulatory areas

© 2026 JUMP

C

CUSTOMER CONTROLS

Customer controls

Jump gives customers granular controls to support their compliance posture. The following configuration options are available to administrators.

Access & authentication

- **SSO & SCIM** — any SAML 2.0 and SCIM provider (e.g., Okta, Azure AD, Google Workspace).
- **MFA & IP allowlisting** — enforceable through the customer's Identity Provider (IdP).
- **Role-based access control (RBAC)** — granular permission levels managed through the customer's IdP via SCIM, or directly within the Jump application.
- **Session inactivity timeout** — configurable and enforceable upon request, available to enterprise customers.

Data controls

- **NPI/PII redaction** — configurable automated redaction of sensitive data types (e.g., SSNs, account numbers) from transcripts and downstream content.
- **Data retention policies** — customer-configurable retention periods per meeting asset type (audio/video, transcript, AI summary), including zero-retention.

Disclosure & consent

- **Automated recording disclosures** — configurable visual and audible disclosures for virtual, phone, and in-person meetings.
- **Verbal consent detection** — automatically detects and logs consent language from transcripts.
- **Custom disclosures on AI notes** — configurable firm-specified, non-editable disclosure language appended to AI-generated outputs.

Monitoring & oversight

- **Audit logs & SIEM integration** — immutable audit logs covering user logon/logoff, screens viewed, and all data changes and deletions are exportable to a customer's SIEM.

Mobile

- **Mobile MDM support** — Microsoft Intune MAM/APP policies supported for iOS and Android.

© 2026 JUMP

01

SECTION ONE

Recording, disclosure, & consent

Jump captures client meetings through an AI notetaker that joins virtual, phone, or in-person meetings. This involves processing audio to generate meeting transcripts and related, AI-generated assets like meeting summaries. Customers operating in regulated industries may have disclosure and consent obligations when recording or capturing client communications.

WHAT JUMP PROVIDES

- **Automated recording disclosures** across meeting platforms (e.g., Zoom, Microsoft Teams, Google Meet, phone, in-person), with configurable visual and audible disclosure options.
- **Custom disclosure messages** configurable to align with firm policy and applicable law.
- **Consent monitoring** is a configurable setting. Account owners may select from: automatic detection only, self-attestation only, automatic detection and self-attestation, or off. Verbal consent detection automatically identifies and logs consent language from meeting transcripts, providing an accessible record.
- **Custom, non-editable disclosures** appended to AI-generated notes, which advisors cannot remove or modify.
- **Summary-only mode** processes live audio without saving audio or video recordings, generating AI-generated notes, summaries, and tasks as outputs without creating audio or video recordings. A transcript is generated as a temporary back-end artifact to power AI processing and can also optionally be configured for automatic deletion. This is suitable for customers who wish to minimize recorded media.

CUSTOMER RESPONSIBILITY

Customers are responsible for determining the disclosure and consent requirements applicable to their business and jurisdiction, implementing those requirements for their clients, and ensuring that their deployment of Jump's meeting capture capabilities meets applicable recording law.

© 2026 JUMP

02

SECTION TWO

Books, records, & data retention

Regulated firms commonly have obligations to retain business records — including client communications, documentation of investment advice, and meeting-related records — for defined periods. How AI meeting platform outputs are classified under applicable recordkeeping rules is a determination each firm must make in consultation with its legal and compliance team.

Jump supports a range of data retention configurations, allowing customers to align Jump's behavior with their chosen recordkeeping approach. For customers whose use of Jump involves Protected Health Information, the zero-retention and summary-only options are mechanisms for limiting retention of PHI consistent with the HIPAA minimum-necessary standard (45 CFR 164.502(b)).

WHAT JUMP PROVIDES

- **Customer-configurable retention periods** per meeting asset type (e.g., audio/video recordings, transcripts). Once a configured retention period lapses, Jump automatically and permanently hard-deletes the data, meaning deletion is permanent and it is not recoverable.
- **Zero-retention option** — customers may configure immediate deletion of meeting assets, effectively maintaining no persistent storage of raw meeting data in Jump.
- **Summary-only mode** generates AI outputs without storing the meeting audio or video recording files, reducing the scope of what must be managed as a record.
- **Archiving** — AI-generated summaries and notes can be automatically routed to a designated email address or integrated into a customer's third-party archiving solution for long-term recordkeeping.
- **Audit logs & SIEM integration** — comprehensive, immutable audit logs covering user activity, data changes, and access events, are exportable to a customer's SIEM.
- **Sync confirmation & attestation** — administrators can require advisors to confirm review of AI-generated content before any of the following actions: syncing notes to a CRM, syncing financial planning data, syncing tasks, drafting follow-up emails, copying notes, or exporting notes as a PDF. This control also supports supervisory oversight of AI-assisted workflows.
- **Attestation report** — for accounts with attestation enabled, Jump generates a downloadable audit log (exportable as CSV) recording each attestation event, including the user who attested, the action attested to, and the timestamp.

CUSTOMER RESPONSIBILITY

Customers are responsible for determining which Jump outputs constitute records subject to their applicable retention requirements, establishing and enforcing appropriate retention policies, and ensuring outputs are preserved through their own recordkeeping and archiving systems where required.

© 2026 JUMP

03

SECTION THREE

AI governance & human oversight

Regulators and industry bodies have emphasized the importance of human oversight of AI-generated outputs, governance structures around AI tool adoption, and controls to manage risks such as inaccuracy, bias, and unauthorized autonomous action. Below is a summary of Jump's AI governance practices.

HUMAN-IN-THE-LOOP DESIGN

Jump is designed as a human-in-the-loop system. AI may draft or propose content (e.g., follow-up emails, CRM updates), but no AI-generated content is sent to clients or written to external systems until an end user explicitly reviews and approves it. Jump does not take autonomous action on behalf of advisors.

No model training on customer data

Jump does not use any customer data to train, fine-tune, or improve any AI model. All customers are opted out of model training by default. Jump has enforced zero-data-retention and no-training clauses with all third-party LLM providers.

AI model transparency

Jump uses enterprise API deployments of third-party Large Language Models (LLMs) and does not build or host its own LLMs. Jump's current AI model providers are identified in its sub-processor list, available in the Trust Center.

AI performance monitoring & model versioning

Jump monitors AI model performance using structured evaluation sets to benchmark precision, recall, and F1 scores across model versions. These metrics are tracked before and after production deployments to detect performance drift, regression, or safety degradation. Jump maintains model versioning and the ability to roll back to a prior stable version if a deployed model exhibits unexpected behavior.

Bias review

Before any model is promoted to production, it is assessed for disparate performance across relevant demographic, use-case, and input-type dimensions. Findings are documented, reviewed, and factored into model selection, configuration, and prompt design decisions.

AI security testing

Jump conducts adversarial security testing specific to AI systems, including automated red-teaming for direct and indirect prompt injection across key AI workflows (using NVIDIA GARAK).

EU AI Act classification

Jump's AI governance practices align with the EU AI Act as a Minimal Risk AI system provider (Regulation (EU) 2024/1689). As a Minimal Risk system, Jump is not subject to mandatory regulatory obligations under the Act beyond applicable transparency norms, and has voluntarily aligned its AI governance practices with the Act's principles.

CUSTOMER RESPONSIBILITY

Customers are responsible for reviewing and approving all AI-generated outputs before use, establishing internal governance policies around AI tool adoption, and ensuring that their supervisory and oversight processes are designed to appropriately govern AI-assisted workflows.

© 2026 JUMP

04

SECTION FOUR

HIPAA & PHI

Jump is purpose-built for financial advisors and is not marketed as a healthcare platform. However, some customers (e.g., benefits consultants, insurance advisors, and firms whose clients discuss health-related financial matters (e.g., health savings accounts, long-term care insurance, disability insurance, or Medicare planning)) may capture Protected Health Information (PHI) incidental to a client meeting.

Business Associate Agreement

Jump offers a Business Associate Agreement (BAA) to customers who require one to cover PHI processed through the platform. Customers who anticipate that their use of Jump will involve PHI should contact their Jump account team to execute a BAA before processing PHI in Jump.

Third-party security

Jump's service relies on third-party providers, including cloud infrastructure and AI model providers. Jump maintains a formal vendor management program to assess and monitor these providers. Jump assesses all third parties prior to contract signature and on an ongoing basis thereafter. Vendor agreements include appropriate confidentiality, security, and privacy obligations. Jump also executes a BAA with all applicable business associates. For customers whose use of Jump involves PHI, these due diligence and contractual requirements align with the Business Associate flow-down obligations for vendors under 45 CFR 164.314(a)(2)(iii) and 164.502(e).

Incident response & notification

Jump maintains a documented Incident Response Policy and Plan tested at least annually. Jump will notify impacted customers within 72 hours upon confirmation of a security incident. For customers whose use of Jump involves PHI, this 72-hour notification commitment exceeds the 60-calendar-day outer limit for business associate breach notification required by 45 CFR 164.410(b).

CUSTOMER RESPONSIBILITY

Customers are responsible for determining whether their use of Jump involves PHI subject to HIPAA, for executing a BAA with Jump before processing PHI on the platform, and for configuring Jump's configurable policies and settings in a manner consistent with their obligations as a covered entity or business associate.

© 2026 JUMP

05

SECTION FIVE

Data security & privacy

Jump is purpose-built for financial professionals and handles sensitive client data, including personal and financial information discussed in client meetings. Jump's security program is designed to protect this data throughout its lifecycle and for operational resilience. Please reference Jump's Security whitepaper, Security FAQ, and our SOC2 report (available in our Trust Center) for more information about our data security practices.

Customer data is owned by the customer. Jump does not use customer data for advertising, sell it, or share it with third parties except as necessary to provide the contracted services. Customer data, including backups, is encrypted at rest and in transit, and is stored in the region designated by the customer. Jump supports US, Canada, and EU hosting regions. Please reference Jump's Privacy whitepaper for more information about our data privacy practices.

© 2026 JUMP

A

APPENDIX

Regulatory mapping summary

The table below provides a high-level summary of Jump's practices mapped to key regulatory areas that our customers may be subject to. It is not exhaustive. Customers should consult the relevant sections of this document and their own legal counsel for a complete assessment.

TOPIC	RELEVANT REGULATIONS	JUMP'S PRACTICE
Recording disclosure & consent	Federal & state recording laws; FINRA Rule 3110 (supervision framework)	Automated disclosures (visual + audible), verbal consent detection (configurable), summary-only mode.
Books & records retention	FINRA Rule 4511; SEC Rules 17a-4 & 204-2	Configurable retention per asset type; email archiving output; immutable audit logs.
Human oversight of AI	FINRA 2026 GenAI Guidance; SEC Reg BI; EU AI Act	Human-in-the-loop: no AI output sent or written without explicit advisor approval.
AI model training on customer data	FINRA 2026 Guidance; GDPR; GLBA	No training on customer data. DPAs with all AI providers with zero-retention and no-training clauses.
AI model version tracking	FINRA 2026 GenAI Guidance	Model versioning with rollback capability. Providers listed in sub-processor list.
AI bias review	SEC Reg BI; FINRA 2026 Guidance	Pre-production bias assessment across demographic and use-case dimensions.
NPI / PII protection	GLBA; Reg S-P; GDPR; CCPA	Configurable NPI/PII redaction. No data monetization.
Data encryption	DORA Art. 9/13; Reg S-P; GDPR	AES-256 at rest, TLS 1.2+ in transit.
Incident notification	DORA Art. 17-19; GDPR Art. 33; Reg S-P §248.30(a)(5); HIPAA Breach Notification Rule (45 CFR 164.400-414)	Jump's standard 72-hour notification satisfies Reg S-P §248.30(a)(5) and GDPR Art. 33, and exceeds the 60-calendar-day outer limit required by 45 CFR 164.410(b).
Business continuity	DORA Art. 11–12/24	Multi-zone GCP, automated failover, daily backups, annual BCP/DR testing.
Vendor risk	DORA Art. 29/30; FINRA 2026 Guidance; HIPAA Business Associate requirements (45 CFR 164.314(a), 164.502(e))	Formal vendor management program, including contractual requirements for sub-processors and business associates.
EU AI Act classification	EU AI Act (Reg. (EU) 2024/1689)	Minimal Risk AI system provider.
Independent security audit	DORA Art. 28; FINRA 2026 Guidance	SOC 2 Type II (continuous 12-month window).
Privacy framework compliance	GDPR; CCPA; GLBA; HIPAA Privacy Rule (45 CFR 164.500 et seq)	DPA; privacy by design; data minimization; deletion within 30 days of request; SCCs for cross-border transfers.
PHI protection	HIPAA Security Rule (45 CFR 164.312)	Encryption; SSO, MFA, and RBAC; configurable session inactivity timeout; audit logs with SIEM export; configurable NPI/PII redaction; configurable data retention. BAA available upon request.

© 2026 JUMP