8x8 AI Studio

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 controls that customers must implement when using 8x8 AI Studio to build or operate AI agents that process 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 an AI Studio deployment compliant; proper agent design and configuration are required.

1. Introduction

8x8 AI Studio is a platform that enables customers to build AI-driven agent workflows across voice and digital channels. Customers using AI Studio to build agents that interact with individuals — or that retrieve, transmit, or display personal data or PHI — must design and configure those agents in a manner consistent with applicable privacy and data protection law.

8x8 secures the underlying AI Studio infrastructure and commits to appropriate technical and organizational measures in its BAA and DPA. Customers are responsible for the design, configuration, and operation of the agents they build on that platform. A misconfigured agent — one that discloses personal data to an unverified user, retrieves more data than the interaction requires, or processes data for purposes beyond those for which it was collected — can constitute a violation of applicable law regardless of the security measures 8x8 applies at the platform level. The requirements in this Guide are designed to prevent those outcomes.

This Guide applies to customers on two tracks, both of which are subject to the same agent design requirements. Where a requirement has a specific legal basis under one track only, that is noted. Otherwise all requirements apply to both tracks.

	HIPAA Track	Privacy Law Track
Who it applies to	Covered entities and business associates using AI Studio to process Protected Health Information (PHI), operating under an 8x8 BAA	All customers using AI Studio to process personal data, 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 any AI Studio agent that may process PHI or personal data is deployed to a production environment.

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.
MUST NOT	Prohibited. Deploying an agent with this configuration constitutes a violation of your obligations under the applicable BAA or DPA and may constitute a reportable breach or incident.

2. Agent Design Requirements

The following requirements apply to any AI Studio agent that may access, retrieve, transmit, display, or disclose personal data or PHI. They address the design decisions that are within the customer's control and that directly determine whether the agent processes data in a compliant manner.

2.1 Identity Verification Before Disclosure of Personal Data

The most critical design requirement for agents that disclose personal data is ensuring that data is only disclosed to the person authorized to receive it. The required level of verification is risk-based: it must be appropriate to the sensitivity of the data being disclosed and the risk profile of the interaction. For agents processing sensitive data or PHI, a higher standard of verification is warranted. Customers must document their verification approach in their risk analysis.

- **MUST** implement identity verification within the agent workflow before any personal data is disclosed to a caller or user. The verification method must be appropriate to the sensitivity of the data involved and the channel through which the interaction occurs.
- **SHOULD** use multi-factor verification for interactions involving sensitive data or PHI — such as health information, financial records, precise geolocation, government identifiers, or

biometric data. For lower-sensitivity interactions, a single strong factor may be sufficient, subject to the customer's risk analysis.

- **MUST NOT** use ANI/CLI (Automatic Number Identification / Caller Line Identification) as the sole verification factor for voice channel agents. Phone numbers can be spoofed and ANI/CLI alone provides no meaningful identity assurance. ANI/CLI may be used as one layer within a broader verification workflow.
- **MUST** implement OTP verification or integration with an authenticated session (e.g., customer portal SSO or OAuth) for digital channel agents before any personal data is disclosed. Agents deployed in publicly accessible digital channels must never disclose personal data to an unauthenticated user.
- **MUST** ensure that authentication failure does not itself disclose personal data — error messages and fallback handling must not confirm or reveal information about the individual.

Acceptable Verification Factors
• Something the individual knows: date of birth, account number, last four digits of a government identifier, or a previously established PIN
• Something the individual has: a one-time passcode (OTP) sent to a phone number or email address on file
• Authenticated session: SSO or OAuth verification against an existing authenticated customer or patient portal session (recommended for digital channels)
• Call metadata: ANI/CLI matched against a registered number on file — as a supplementary layer only, never as the sole factor

2.2 Data Minimization

Agent workflows must be designed to retrieve and disclose only the personal data required to fulfill the specific purpose of the interaction. This principle — known as data minimization under privacy law and the minimum necessary standard under HIPAA — applies equally under both tracks.

- **MUST** configure backend integrations to return scoped data sets rather than full individual records. Each data field returned must be justified by the specific interaction purpose.
- **MUST NOT** design agents that retrieve or disclose an individual's full record in response to a standard query. An appointment confirmation agent should retrieve appointment date, time, and provider name — not the individual's full history.
- **SHOULD** use separate agent workflows for distinct use cases (e.g., appointment scheduling, account balance inquiry, billing) rather than a single agent with broad access to all data types, to minimize the data footprint of any individual agent.

2.3 Purpose Limitation

Agents must be configured and operated in a manner consistent with the specific, defined purposes for which the underlying personal data was collected. Purpose limitation is a core requirement of applicable privacy laws and reflects the expectation of individuals whose data is being processed.

- **MUST** define a specific processing purpose for each AI Studio agent before deployment. The agent's design, data access, and workflow logic must be scoped to that purpose.

- **MUST NOT** repurpose an existing agent to process personal data for a materially different purpose without first reviewing whether the new use is compatible with the original collection purpose, updating any required privacy notices, and ensuring the applicable DPA or BAA covers the new processing activity.
- **MUST NOT** design agents that collect personal data beyond what is necessary for the defined purpose, including through open-ended free-text fields or unscoped data queries that may capture incidental sensitive data.
- **SHOULD** document the defined processing purpose for each PHI- or personal data-handling agent and maintain that documentation as part of the customer's records of processing activities (required under GDPR Article 30 and consistent with HIPAA risk analysis obligations).

2.4 Audit Logging of Personal Data Access

AI Studio generates call log records and interaction transcripts for voice and digital sessions, which provide a foundation for audit purposes. However, AI Studio does not automatically capture the additional fields required for legally adequate audit records — specifically, authentication outcomes and categories of personal data accessed or disclosed. Customers must design their agent workflows to generate and route those records to a retention-compliant logging system.

- **MUST** design agent workflows to log each interaction involving personal data or PHI, capturing: timestamp; channel (voice, chat, SMS); caller/user identifier; agent name or identifier; authentication outcome (pass/fail); and category of personal data accessed or disclosed.
- **MUST** route interaction logs to a system that retains them for a period consistent with applicable law. HIPAA requires a minimum of six years from the date of creation. Privacy law customers should apply the retention period required under their applicable law and organizational policy.
- **MUST NOT** forward interaction transcripts or logs containing personal data or PHI to any system — including email, collaboration tools, or analytics platforms — that is not covered by the applicable DPA or BAA and that does not meet the security requirements of applicable law.
- **SHOULD** implement automated monitoring of logs for anomalies such as repeated authentication failures, unusual query volumes, or queries returning significantly more data than typical, each of which may indicate misconfiguration or unauthorized access attempts.

2.5 Session Termination and Inactivity Timeouts

AI Studio provides idle session termination natively for digital channel agents. Sessions that are inactive for 25 minutes receive an automatic warning; sessions that remain inactive for a further 5 minutes are terminated, giving a total idle timeout of 30 minutes. Customers do not need to build session termination logic into their agent workflows to satisfy this requirement. Voice channel sessions are inherently bounded by the call itself and terminate when the caller disconnects.

- **SHOULD** implement a shorter idle timeout at the application layer if your organization's security policy specifies a period shorter than 30 minutes for sessions involving sensitive data or PHI.
- **SHOULD** clear or obscure any personal data or PHI displayed in a chat interface upon session termination, where technically feasible.

2.6 Encryption of Data in Transit

AI Studio's platform-level communications are encrypted by 8x8. This includes all AI Studio integration surfaces — user tools, Apps/Webhooks, Flows, and MCP Connectors — where 8x8 enforces TLS on its side of every connection. The customer's obligation is to ensure that the endpoint on their own backend infrastructure likewise requires TLS. The requirements below govern those customer-controlled connections to backend systems containing personal data or PHI.

- **MUST** use TLS 1.2 or higher for all API connections between AI Studio agents and any integrated backend system that stores or returns personal data or PHI.
- **MUST NOT** configure integrations that permit fallback to unencrypted protocols.

2.7 Agent Configuration and Testing Integrity

- **MUST NOT** embed real personal data or PHI in agent instructions, system prompts, or configuration fields. Agent instructions and configuration data may be stored, logged, or accessed in ways not covered by the security measures applicable to personal data. All personal data must come from secured, integrated backend systems at runtime.
- **MUST** test agents using de-identified or synthetic data only. Real personal data or PHI must not be used in non-production testing or development environments unless those environments are equivalently secured and covered by the applicable BAA or DPA.
- **MUST** require a compliance review before any new personal data- or PHI-handling agent is deployed to production and before any material change is made to an existing such agent.
- **SHOULD** test authentication bypass vulnerabilities explicitly during QA — verify that the agent cannot be manipulated into disclosing personal data by malformed inputs, prompt injection attempts, or edge-case session states.

3. Excluded Subprocessors

3.1 ElevenLabs

- **MUST NOT** be used as an AI Model for HIPAA applications. 8x8 does not have a flow down BAA in place for ElevenLabs.

3.2 SpaceXAI (Grok)

- **MUST NOT** be used as an AI Model for HIPAA applications. 8x8 does not have a flow down BAA in place for SpaceXAI.

3.3 TeleSign

- **MUST NOT** be used for HIPAA applications or Privacy use cases under the 8x8 DPA. AI Studio customers can use TeleSign to perform a fraud check on a telephone number that is placing a call into an 8x8 AI Studio agent. TeleSign would process this telephone number, which could be personal data or PHI. Currently, 8x8 does not a flow down DPA or BAA in place for TeleSign.

4. Key Definitions

Term	Definition
ANI / CLI	Automatic Number Identification / Caller Line Identification — the telephone number transmitted by the calling party's network. Can be spoofed and is not a reliable sole authentication factor.
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.
Data Minimization	The principle, required under applicable privacy laws and the HIPAA Privacy Rule minimum necessary standard, that personal data collected and processed must be limited to what is necessary for the specified purpose.
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.
OTP	One-Time Passcode — a time-limited code sent to a verified phone number or email address, used as an authentication factor.
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.
Purpose Limitation	The principle, required under applicable privacy laws, that personal data may only be processed for the specific, defined purposes for which it was collected and must not be used for incompatible purposes without a fresh legal basis.
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. Corresponds to PHI under HIPAA and special category data under GDPR Article 9, and to equivalent categories under applicable US state privacy laws.
SSO / OAuth	Single Sign-On / Open Authorization — authentication protocols that allow an AI Studio agent to verify a user's identity against an existing authenticated session.
TLS	Transport Layer Security — the encryption protocol used to secure data in transit between AI Studio and integrated backend systems.

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.