— HIPAA & SECURITY OVERVIEW

HIPAA at Axis

A plain-language overview of our Business Associate workflow

Axis HQ, Inc. ("Axis") is a Business Associate under HIPAA. This document summarizes, in plain language, how we handle Protected Health Information (PHI) on behalf of the dental and primary-care practices that use our services. The complete legal terms live in the Business Associate Agreement (BAA), which we sign with every practice before onboarding. This one-pager is intended to help your compliance officer, privacy officer, and leadership understand our workflows quickly.

BAA	ENCRYPTION	BREACH NOTICE	NO MODEL TRAINING
Signed before any PHI is processed	**AES-256 at rest · TLS 1.3 in transit**	**Within 48 hours of discovery**	**PHI is never used to train public AI**

[01] Our role as a Business Associate

Your practice is the Covered Entity under HIPAA. You hold the patient relationship and the legal duty to protect their information. Axis operates as a Business Associate: we perform specific administrative functions on your behalf — answering calls, booking appointments, collecting intake, verifying insurance — and in the course of doing so, we receive and process PHI. Every obligation we take on is memorialized in the BAA.

[02] What we treat as PHI

From the moment a patient-related signal enters our systems until it is cryptographically destroyed under your retention policy, the following is treated as PHI:

- Audio of patient phone calls and the transcripts we generate from them.
- Patient names, dates of birth, addresses, phone numbers, and email addresses.
- Insurance carrier, member ID, group number, and eligibility results.
- Reason for visit, triage notes, and appointment outcomes.
- SMS and other messages exchanged between the practice and its patients.
- Any other identifying information the patient shares on a call or message.

[03] How we protect PHI

HIPAA requires administrative, technical, and physical safeguards. Axis implements all three in layers. A vulnerability in any single layer does not expose patient data.

— SAFEGUARD

Administrative

- Workforce security training on hire and annually
- Access governed by least-privilege policy
- Written vendor agreements and BAAs with every subprocessor that touches PHI
- Documented incident-response runbooks

— SAFEGUARD

Technical

- AES-256 encryption at rest across audio, transcripts, and derived data
- TLS 1.3 for all data in transit
- Multi-factor authentication for all Axis personnel
- Centralized audit logging retained for 6+ years

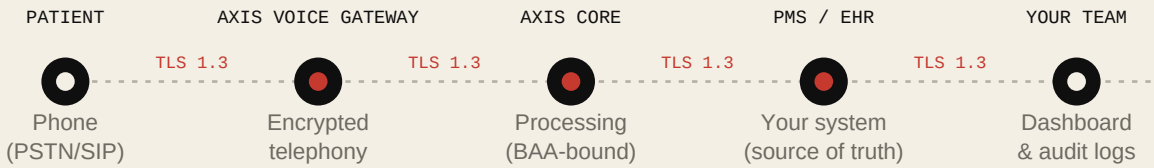
— SAFEGUARD

Physical

- Cloud-hosted in SOC 2-audited U.S.-only data centers
- No on-premise servers at Axis offices
- Hardware asset tracking and secure media disposal
- Segregated production and corporate networks

[04] How patient data flows

The diagram below shows the path a piece of PHI takes from a patient's phone to your practice management system. Every leg is encrypted. Every system that touches PHI is covered by a written agreement with Axis.



[05] Minimum necessary

Axis processes only the PHI required to perform the service you have authorized. The voice agent does not read clinical notes or treatment plans. The AI does not diagnose, prescribe, or make treatment decisions. PHI is partitioned from our business and marketing systems and is never mixed with non-PHI data.

[06] Breach notification

If Axis becomes aware of a breach of unsecured PHI, we will notify the affected practice in writing within 48 hours of discovery. Our notice will describe what happened, when, what categories of PHI were involved, the number of patient records affected, the containment and remediation steps taken, and our plan to prevent recurrence. We will cooperate fully with your own breach-notification obligations to patients and to HHS.

[07] What we will not do with PHI

- **Train public AI models.** Your patient audio, transcripts, and derived data are never used to train or fine-tune publicly available language models or AI systems.
- **Sell or share your data.** We do not sell, share, or license PHI or practice data to third parties for marketing, analytics, or any other commercial purpose.
- **Market to your patients.** Axis does not use PHI to market our own services, and we do not market the practice's services to your patients except where you direct us to.
- **Aggregate across practices.** We do not build cross-practice benchmarks or industry reports using your identifiable data. Any aggregate insights we publish rely on data that has been de-identified under HIPAA Safe Harbor or Expert Determination.

[08] Your role as the Covered Entity

HIPAA assigns specific duties to the Covered Entity that Axis cannot perform on your behalf. These remain your responsibility:

- Obtaining patient authorizations where required (including any required consents for automated SMS and voice calls).
- Responding to patient requests for access, amendment, and accounting of disclosures.
- Maintaining your own Notice of Privacy Practices.
- Training your workforce on your internal PHI handling procedures.
- Configuring Axis appropriately for the jurisdictions you serve.

[09] Requesting the BAA

We sign a Business Associate Agreement with every practice before onboarding — not after a sales conversation, not as a separate transaction. To request the BAA and a tailored security questionnaire response, email sebastian@useaxis.app with your practice name, point of contact, and practice management system. We respond within one business day.

— DOCUMENT INFO

Issued by: Axis HQ, Inc.
Effective: 2026-04-24 · Review cycle: every 12 months
For BAA and compliance questions: sebastian@useaxis.app
Mailing address: 2261 Market Street STE 62976, San Francisco, CA 94114