HIPAA Compliance

Nemus Insights LLC

Document version: 2026-11-09

Status: Draft pending counsel review

Nemus Insights is built so protected health information stays in a HIPAA-eligible backend and never leaks through the AI that people talk to. Data lives in Xano. Every research and customer-facing conversation agent is secured through Microsoft Azure.

That split is the core of our posture: Xano is the system of record for PHI. Azure is the controlled environment where agents reason. Together they keep personal health information inside the platform instead of sending it to public consumer AI tools.

How we secure the platform

Three layers work together so a chat, a research question, or an internal analysis cannot expose someone's health records.

1. **Xano holds the data.** Claims, eligibility, plan documents, and conversation history live in Xano — a HIPAA-eligible backend with encryption and role-based APIs.
2. **Azure hosts the agents.** Research and customer-facing conversation agents run inside Microsoft Azure. They are not public consumer chat products. Azure provides the HIPAA-eligible environment and enterprise controls around those models.
3. **Xano decides what an agent sees.** Each request is authenticated in Xano first. Only the signed-in person's allowed context is passed to the matching Azure agent. Research mode receives none of that personal health information.

Xano: a HIPAA-eligible backend

All platform data — medical and pharmacy claims, eligibility rosters, plan documents, and chat history — is stored and authorized in Xano. Xano provides HIPAA-eligible infrastructure so we can handle PHI the way HIPAA expects: encrypted and access-controlled.

- **HIPAA-compliant backend.** Xano is audited for HIPAA and offers a HIPAA hosting plan with a Business Associate Agreement (BAA). Protected health information (PHI) is stored and served from that environment — not from the browser or from a public AI service.
- **Access is role-scoped.** Members can only retrieve their own benefits and claims. Employers see population analytics, not an employee's private chat. Brokers and admins are limited to the companies they are authorized to serve.
- **Encryption and access controls.** Data is encrypted in transit and at rest by our infrastructure vendors. Every API request is authenticated and role-scoped, environments are separated, and

request history is retained. Application logs record who viewed a member record: the actor, the subject id, and the endpoint. They do not store claim contents.

- **Least-privilege APIs.** The application never sends a raw database to an agent. Xano builds a narrow, purpose-built payload for that turn — and omits PHI entirely when the member is in research mode.

Azure: secured agents for research and chat

The agents members, brokers, and our operations team use are hosted in Microsoft Azure — not on a public chatbot. Azure is a HIPAA-eligible cloud with its own BAA, identity, networking, and logging. That is how we keep every conversation inside a controlled backend instead of leaking PHI to the open internet.

- **Customer-facing personal chat.** The member health advocate that answers questions about deductibles or claim cost runs on Azure. It only receives that member's plan and claims context after Xano has authenticated the session.
- **Research chat — no personal data.** A separate research agent answers general medical and benefits questions. It has no access to claims, identifiers, or other PHI.
- **Broker and operations agents.** Research and analysis agents used by brokers, plus internal helpers that summarize policies or classify claims, also run on Azure. Azure runs the model; Xano supplies only the data that agent is allowed to use.

Personal chat vs. research chat

Employees get two conversation modes on purpose. One can see their own record. The other cannot. That separation is enforced in Xano before anything reaches Azure.

HIPAA-aligned personal chat

For questions about a person's own coverage, claims, and programs. The Azure agent only receives that authenticated member's context. Employers do not see individual chat transcripts.

- Signed-in session required
- Context limited to the member (or a dependent they are allowed to view)
- Processed by an Azure-hosted agent, not a public consumer model

Research chat — no PHI

For general medical and benefits questions. This agent is not given claims, names, or other identifiers. It can look up public medical sources and return references without touching a personal record.

- Zero access to claims or health metrics
- Knowledge used for research is non-PHI content
- If the question is about a specific plan or claim, we point the user to personal mode

How this prevents PHI leakage

- **No public consumer AI.** Research and customer-facing chats do not go to an unmanaged public chatbot. They run on Azure under enterprise controls.
- **PHI stays in Xano.** The database of record is the HIPAA-eligible backend. Agents receive a scoped snapshot for one turn, not an open connection to every table.
- **Research never sees the record.** General research agents are isolated from claims and identifiers so a curiosity question cannot pull someone's health history.
- **Business Associate Agreements.** We use HIPAA-eligible vendors (Xano, Microsoft Azure) and execute Business Associate Agreements where PHI is processed as agreements are put in place.

Disclaimer

This document describes how Nemus Insights is designed and operated. It is not legal advice and does not replace a signed BAA or your organization's own compliance program. HIPAA is a shared responsibility: our infrastructure and application controls are built for it, and customers remain responsible for how they use the platform.