Trust & Security FAQ

What is XINOVEE

XINOVEE is a security-first healthcare infrastructure focused on audit visibility and identity-based access governance. We help organizations understand how access is granted and used across systems in order to improve accountability, audit readiness, and operational oversight.

Does XINOVEE store or process patient data?

No.

XINOVEE does not store, process, or analyze Protected Health Information (PHI), patient identifiers, or clinical content during pilot engagements.

Does XINOVEE require access to live clinical systems?

No.

Pilot engagements are non-production and do not involve live clinical systems. Pilots are designed to evaluate audit visibility and access governance using limited, non-identifiable data.

What data does XINOVEE accept during a pilot?

XINOVEE accepts only:

- De-identified audit logs
- Aggregated access or event metadata
- System-level or role-based identifiers
- Policy and procedural documentation

Any data not explicitly listed above is not accepted.

What data does XINOVEE explicitly not accept?

XINOVEE does not accept:

- Patient identifiers
- Clinical records or notes
- Diagnostic or treatment data
- Full user credentials
- Live production system access

How is pilot data stored?

Pilot data is stored in restricted, access-controlled environments. Access is limited to authorized XINOVEE personnel and used solely for the defined pilot purpose.

How long is pilot data retained?

Pilot data is retained only for the duration of the pilot engagement and is deleted upon completion unless otherwise agreed in writing.

Does XINOVEE use AI?

Yes, in a limited and controlled way.

AI is used only to assist with:

- Summarizing sanitized outputs
- Highlighting patterns or anomalies
- Supporting reporting and documentation

AI is **not** used to process PHI, patient identifiers, or clinical content.

Does AI replace compliance or security decision-making?

No.

AI does not replace human judgment, operational controls, or compliance decision-making. All findings are reviewed and interpreted by humans.

Is XINOVEE HIPAA compliant?

XINOVEE supports HIPAA Security Rule alignment by strengthening audit visibility and access governance.

XINOVEE does not claim HIPAA certification by default and does not operate as a covered entity during pilot engagements.

Does XINOVEE sign Business Associate Agreements (BAAs)?

Not currently and not during pilot engagements.

Pilot engagements are structured to avoid the handling of PHI and therefore do not require a BAA.

Who is XINOVEE built for?

XINOVEE is designed to support:

- Security teams

- Compliance and risk teams
- IT and identity governance teams

It is not a clinical system and does not replace EHRs, IAM platforms, or SIEMs.

Where is XINOVEE based?

Washington, D.C.

XINOVEE's BAA-Ready Roadmap

XINOVEE is intentionally designed to mature toward BAA-eligible engagements over time, following a phased approach aligned with healthcare industry expectations.

Phase 1: Non-PHI Pilot Infrastructure (Current)

- No PHI ingestion or processing
- Limited-scope pilot engagements
- De-identified audit and access metadata only
- Restricted storage and access controls
- Clear data retention and deletion policies

Phase 2: Hardened Security & Operational Controls

- Formalized security policies and procedures
- Expanded logging and monitoring controls
- Incident response documentation
- Independent security review or assessment

Phase 3: BAA-Eligible Architecture (Future)

- Optional PHI handling pathways (customer-controlled)
- Dedicated environments for PHI workloads
- Formal Business Associate Agreement availability
- Expanded compliance and audit support

Important Clarification

This roadmap is provided for transparency only. It does not represent a commitment, timeline, or contractual obligation.

BAA execution is evaluated on a case-by-case basis and only after XINOVEE determines that the appropriate technical, operational, and legal controls are in place.