AI, Security & Data Governance Frequently Asked Questions

This FAQ is designed for Health System CIOs, Legal Counsel, and IT Compliance teams to detail how Elora protects sensitive data while leveraging AI to improve social care coordination. It covers key aspects of compliance, federated privacy, and AI safety, highlighting Elora's commitment to secure, responsible, and equitable AI in healthcare. For further information, please contact info@elorahq.com.

Regulatory Compliance & Administrative Safeguards

Q: Is Elora HIPAA compliant?
Yes. Elora operates as a HIPAA Business Associate. We provide a secure platform for handling Protected Health Information (PHI) in strict accordance with all applicable federal and state privacy regulations. We execute Business Associate Agreements (BAAs) with all covered-entity customers and with every third-party vendor that may process PHI on our behalf—including our cloud infrastructure provider, transcription service, and any other downstream processors.

Q: What is Elora's security certification status?
Elora is actively pursuing SOC 2 Type II certification. Our audit is ongoing, and we maintain rigorous internal controls in the interim—including continuous monitoring, Third-Party Risk Management (TPRM) reviews, and regular internal security assessments to identify and mitigate threats in real time. We will share our SOC 2 Type II report with customers upon completion.

Q: How long are audit logs and data maintained?
Audit logs are retained for a minimum of 6 years, consistent with HIPAA requirements. Upon written request from a customer, Elora will delete customer data within 30 days of receiving the request. Customers are responsible for ensuring that deletion requests comply with their own applicable retention obligations under state and federal law. End-client data requests should be directed to the covered entity.

Q: What is your breach notification protocol?
In the event of a confirmed or suspected security incident, Elora will notify affected customers within 72 hours of discovery—meeting or exceeding HIPAA's Breach Notification Rule requirements. Our team conducts annual simulated breach drills to test and refine our investigation, containment, and documentation procedures. A full incident report is provided to customers following any investigation.

Q: How do you support data auditability?
Elora provides real-time auditability through an automated Audit Logging System that captures all access events, API requests, data exports, and disposal records. Full audit logs are available to customers within 72 hours of request. Logs are immutable and tamper-evident, ensuring a reliable chain of custody for compliance reviews or investigations.

Technical Infrastructure & Data Security

Q: How is data protected at Rest and In Transit?
All data is encrypted using TLS 1.2+ in transit and AES-256 at rest. Data is never transmitted across the public internet in an unencrypted state. Our encryption standards meet or exceed HIPAA technical safeguard requirements.

Q: Are your databases multi-tenant?
Elora uses a tiered storage architecture designed to match the sensitivity of each data type:

- Transcriptions and raw session data: Stored in dedicated per-customer storage (Amazon S3), isolated by design. No other customer's data shares the same storage namespace.
- PHI and clinical data: Stored in a logically isolated database with strict row-level tenant separation. Application and database-level controls ensure that no customer can access another customer's records.
- User authentication and operational data: Managed through shared infrastructure with logical separation enforced at the access control layer.

Q: How do you manage user access?
Elora enforces Role-Based Access Control (RBAC), ensuring staff members can only access the data and functions relevant to their role. Multi-Factor Authentication (MFA) is required for all users. Access logs are reviewed at least annually by Elora's designated HIPAA Compliance Officer, and access rights are reviewed and recertified on a regular cadence. Customers can also configure organization-level access policies and review their own team's access logs on request.

Q: Does Elora support EHR integration?
Our 2026 roadmap includes integration options via Redox middleware, as well as HL7 and FHIR write-back support. This will enable automated population of structured fields such as Z-codes and Social History—reducing duplicate data entry for care coordinators. We will provide customers with advance notice and documentation before any integration features are enabled.

Q: How does Elora protect client or patient privacy?
Elora's architecture enables controlled data exchange across a partner network without compromising individual privacy. The system applies the Minimum Necessary Principle: each entity—whether a clinic, food bank, or community organization—can only send or receive the specific data elements they are explicitly authorized to handle. No agency in the network can view another agency's PHI.

Q: What is Elora's "Federated Privacy Framework"?
Elora's Federated Privacy Framework is our architectural commitment to data sovereignty and privacy-by-design as we scale across partner networks. The core principles are:

- Data isolation: Each customer's PHI is stored in a dedicated single-tenant environment, never co-mingled with other organizations' data.
- Minimum Necessary exchange: When data flows across a partner network, only the minimum necessary information is shared — and only with entities explicitly authorized to receive it.
- De-identification before aggregation: Any cross-network insights (such as population-level analytics or resource matching signals) are derived from de-identified data only. Raw PHI never crosses organizational boundaries.

As Elora's platform matures, this framework will evolve to support more sophisticated federated capabilities — including localized processing within customer-controlled environments for organizations that require it. Today, the framework is expressed primarily through our data isolation architecture, access controls, and BAA structure.

Q: How is PHI isolated from the rest of the system?
Elora uses a dual-gateway architecture:

- PHI API Gateway: Handles all requests involving sensitive patient information, with additional authentication and logging requirements.
- Non-PHI API Gateway: Manages general application traffic and operational data, completely separated from PHI flows.
- Storage: Client PHI and raw transcriptions are stored in dedicated single-tenant environments, isolated from all multi-tenant operational databases.

This separation ensures that a vulnerability or anomaly in one part of the system cannot propagate to sensitive data stores.

Q: Does Elora use "Secure Aggregation"?
Yes. When insights are shared across a partner network, only de-identified, aggregated patterns are exchanged—never individual PHI. For example, population-level trends used to improve resource matching are derived from anonymized data, ensuring no agency can identify a specific individual from network-shared information.

Responsible AI, Safety, and Health Equity

Q: Does Elora use my patient data to train its AI models?
No. Customer data is used exclusively to deliver services to that customer. We do not use PHI, client records, session content, or any proprietary organizational data to train our AI models. Any internal model development uses only de-identified data that has been processed through our De-identification Protocol—which applies HIPAA Safe Harbor and Expert Determination standards to remove all 18 PHI identifiers before any use outside of direct service delivery.

Q: What does Elora do with audio and transcriptions?
Elora handles data with a minimal-retention approach:

- Audio: Converted to text using AWS Transcribe, a HIPAA-eligible service covered under our AWS BAA. Raw audio is not retained after transcription.
- Transcriptions: PHI within transcripts is automatically redacted according to our De-identification Protocol. Customers may request immediate disposal of raw transcriptions after processing—this can be configured at the organizational level.
- No secondary use: Transcription content is never used for advertising, shared with third parties outside our BAA relationships, or used to train models.

Q. How does Elora treat sensitive demographic data?
Elora's data schema is designed for **privacy-by-default.** We adhere to a strict Data Minimization Policy and do not collect, process, or store certain highly sensitive demographic attributes—specifically immigration status and sexual orientation—unless explicitly enabled by a customer to meet specific clinical or social needs (HRSN) documentation requirements. These fields are never activated by default and require deliberate administrative configuration.

Q: What if AI makes a mistake? Is there an expert or "Human-in-the-Loop"?
Yes. Elora is a decision-support tool, not an autonomous system. Care managers review, edit, and co-create all care documentation with their clients. AI-generated summaries, suggested pathways, and recommended resources are always presented as drafts for human review—a professional must validate and approve all content before it is finalized or shared with a patient. Staff remain in full control of every clinical and social care decision.

Q: What does Elora do to mitigate bias and ensure health equity?
Elora takes a multi-layered approach to bias mitigation:

- Representative Validation: Our models are validated across diverse demographic groups to identify and address data generalizability issues before deployment.
- No Cost-as-Proxy: We do not use spending or cost data as a proxy for need—a documented source of bias in healthcare AI. Instead, we use structured Z-code and Community Health Index (CHI) documentation to map to actual clinical and social requirements.
- Equity Dashboards: Supervisor-level dashboards allow administrators to monitor caseload composition, intervention velocity, and outcome distribution across insurance types, demographics, and populations—enabling active auditing for disparate impact.
- Subpopulation Analysis: Real-time monitoring of individual, cohort, and population-level metrics helps organizations ensure care coordination quality is consistent across all groups served.

AI Use, Controls & Staff Concerns

Q: What AI functions does Elora use, and where?

- **Session Documentation**: The primary AI function. Elora can transcribe a care coordination session and generate a draft case note or care summary, which the staff member reviews and edits before saving.
- **Pathway Suggestions**: Based on documented needs and structured SDOH assessments, Elora may suggest relevant care pathways or resources. These are suggestions only—staff must actively select, modify, or dismiss them.
- **Resource Matching**: Elora can surface relevant community resources based on a client's documented needs. This is a search-assist function, not an automated referral.
- **Supervisor Analytics**: Aggregate, de-identified AI-assisted analysis to support population health monitoring and equity auditing.

AI is **NOT used** to make autonomous clinical decisions, generate communications sent directly to clients, or take any action without staff review and approval.

Q: Can staff disable AI features individually?
Yes. Staff members can disable the case note generation and pathway suggestion features on a per-session basis. If a staff member prefers to document a session manually, they can do so within the same platform—Elora supports both AI-assisted and fully manual documentation workflows. No staff member is required to use AI-generated content.

Q: Can our organization administratively disable AI features for all staff?
Yes. Organization administrators can configure Elora at the account level to disable AI-assisted documentation features by default for all users within their organization. This means staff do not need to opt out individually each session—the setting applies platform-wide. Specific AI features can be toggled on or off independently (e.g., disabling case note generation while retaining resource matching), giving administrators granular control. Please contact your Elora account manager to configure these settings.

Q: Will Elora open care pathways automatically based on things a client mentions in passing?
No. Elora does not automatically open, assign, or act on care pathways. If a client mentions something in conversation—for example, considering and then deciding against a medical appointment—that information may appear in a draft summary, but no pathway is created or triggered without deliberate action by the care manager. Staff review all AI-generated content and must actively choose to create or assign any pathway. The care manager's judgment governs what is documented and acted upon.

AI, Security & Data Governance (continued)

Q: What about client confidentiality—is information less safe because AI is involved?
No. The use of AI features does not change Elora's underlying data security posture or HIPAA compliance obligations. All PHI protections described in this document—encryption, single-tenant storage, BAAs, access controls, audit logging—apply equally whether a staff member is using AI-assisted documentation or not. The AI processing itself occurs within our HIPAA-compliant infrastructure under the same BAA that governs all PHI handling. Client information is not shared with external AI services outside of our BAA relationships, and is never used for advertising or model training.

Q: What about the environmental impact of AI?
We take environment safety and sustainability seriously. Elora's AI features run on AWS infrastructure, which has committed to powering its operations with 100% renewable energy by 2025 and is one of the largest corporate purchasers of renewable energy globally. We are deliberate about model efficiency—using purpose-built, lightweight models for specific tasks rather than large general-purpose models where possible—which reduces compute and energy consumption per session. We are also actively evaluating energy usage metrics as part of our broader sustainability commitments and will share more specifics as our measurement practices mature.

Q: Could reliance on Elora's AI erode staff skills over time?
Elora is designed to support staff, not replace their judgment or skill. The case note generation feature produces a draft that staff must read, correct, and approve—a process that still requires professional knowledge, clinical reasoning, and understanding of the client's situation. Staff who prefer to write notes manually can do so. For organizations with specific concerns, we recommend establishing internal norms around how AI-generated drafts are reviewed—treating them as a starting point that staff actively engage with, rather than a finished product to be rubber-stamped. We're happy to work with your leadership team on change management guidance if that would be helpful.

Q: Are there concerns about using AI with clients who have technology-related fears?
Yes, and we appreciate that partner organizations are thinking carefully about this. A few things worth knowing:

- **Disclosure is in your control.** Elora does not require you to explain the platform's technical architecture to clients. Your organization determines how and whether to discuss documentation tools with clients, consistent with your own consent and transparency practices.
- **Staff can work without AI features.** For specific clients where AI-assisted documentation would create rapport or trust concerns, individual staff members can disable AI features for that session and document manually.
- **No client-facing AI.** Elora does not interact with clients directly—there is no chatbot, no automated client communication, and no AI system that clients encounter. The AI functions are tools for staff use only, invisible to the client.

We recommend that organizations develop a simple, plain-language description of how documentation works—one that is accurate, reassuring, and appropriate for the populations you serve. We can help draft that language if useful.

Last updated: March 2026. For questions not addressed here, contact your Elora account manager or reach out to info@elorahq.com.