Data Security & Privacy

Levi Malott
Chief Technology Officer

Weave is an AI-native, life sciences company that provides a cloud-based platform to support the regulatory lifecycle. As a SaaS solution provider, Weave maintains policies with the highest level of commitment to data security and privacy. This includes, but is not limited to:

- **Zero Data Retention**: The Weave platform is supported by OpenAI models under a formal Zero Data Retention (ZDR) policy.
- **No Machine Learning on User Data**: Both Weave and our vendors refrain from using user data for machine learning purposes.
- **Top-Tier Data Protection**: User data remains secure and private, adhering to industry-standard best practices within each unique client account.

If you have questions not answered in this policy overview, please contact our security team by email at security@weave.bio.

What data do we collect?

User Data: When organizations license our platform, we collect authorized user names and corporate email addresses for account creation.

Usage Data: We use Posthog and Pendo to collect product usage statistics, specifically feature and functionality use and browser confirmation. This information helps our support teams manage the Weave platform to maintain uptime, address infrequent bugs or errors and understand product usage to inform product improvements and new developments.

Who can access customer data?

All files uploaded to the Weave platform are considered customer data, and we follow industry best practices to protect all customer data. This includes encryption in transit (TLS 1.2+) and at rest (AES-256). Standard operating procedures include segregation of customer data within the product, controlled access to the production systems and customer data, system monitoring, and strict policies around data access and control.

Weave uses multi-factor authentication and role-based access controls for Weave systems. Users of the platform can configure (1) single-sign with their identity providers as long as they are SAML compatible or use (2) user/password login.

Authorized users have access to only their specific data in the Weave platform. Authorized users include:

- Contracted customers and partners working on unique projects in the system.
- Approved consultants and partners provisioned at the request of a contracted customer.

Only provisioned Weave employees have access to the platform and customer data. Access to data is given on a strict, need-to-know basis when required to support product and customer operations. Access is removed immediately if it is no longer needed. We will request explicit permission if we have an interest in using your data for any other purpose.

Regarding our infrastructure partners, we utilize OpenAI as our LLM provider and AWS Textract for content extraction of customer files. We maintain a ZDR policy with OpenAI (see OpenAI Trust), and Textract does not retain any customer data (see AWS Data Privacy).

How do we protect customer data?

Once an account for your organization is created on our platform, you have complete control over access and permission levels. All data related to your organization is logically partitioned to ensure customer data remains separate. At any time, you can delete your data and remove user access.

Customer data is encrypted both in transit using SSL/TLS and at rest with AES-256 encryption. We maintain rolling backups on a 14-day window and have hot-standby databases available in case of a server outage. Customer data (e.g. uploaded files and generated content) deletion occurs within 30-days of a given contract termination/end.

Our application relies on OpenAI models, and we will only use providers where we have a ZDR policy in place. Currently, this is GPT4o and text-embedding-3-small. We pin to specific models and only update model versions after we have (1) vetted that the new version(s) improve our system and (2) ensure the new version(s) pass our standard suite of regressions tests.

Additionally, Weave engages a contracted security team that conducts regular audits of our corporate, application and infrastructure security. This team also provides continuous monitoring of our infrastructure and platform to detect anomalous behavior.

What if there is a security-related incident?

In the event of a data breach or security incident, Weave will adhere to our policy and promptly implement measures to immediately secure impacted systems. We will alert impacted customers within 24 hours, outlining the scope and significance of the breach. Comprehensive details will be provided within 72 hours after the investigation concludes. We are engaged with a security contractor to assist in root cause analysis and providing remediation recommendations. Throughout the process, we are committed to maintaining transparent and proactive communication with our customers.