The Weave Platform

Data Security & Privacy

At Weave Bio, we help life sciences teams connect data, people, and process across regulatory workflows. We take data security and privacy seriously. The Weave Platform and our policies are designed to protect your information at every step.

Zero Data Retention: The platform operates on OpenAI models under a formal Zero Data Retention (ZDR) policy. Your data is never stored or used to train models.

No Machine Learning on User Data: Neither Weave nor our vendors use customer data to train or improve AI models.

Top-Tier Data Protection: User information is safeguarded through industry best practices, ensuring that each client's data remains secure, private, and contained within its own environment.

The Information You Share With Us

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 gather feature usage and browser data to maintain platform performance, resolve issues, and inform product development.

Who Sees Your Data (and Why)

All files uploaded to the platform are considered customer data, and Weave follows industry best practices to protect this information. 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 production systems and customer data, continuous system monitoring, and strict policies around data access and control.

Weave uses multi-factor authentication (MFA) and role-based access controls across all Weave systems. Users of the platform can configure either: ① Single sign-on (SSO) with their identity providers, provided they are SAML compatible, or ② Username and password login with Multi-Factor Authentication.

security@weave.bio

Who Sees Your Data (and Why)

(Continued)

Authorized users have access only to their specific data within the platform. These users include:

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

Only provisioned Weave team members have access to the platform and customer data. Access is granted on a need-to-know basis to support product operations and customer success, and it is removed as soon as it's no longer required. If Weave ever needs to use customer data for another purpose, we will request explicit permission.

Regarding infrastructure partners, Weave uses OpenAI as its large language model (LLM) provider and AWS Bedrock for content extraction from customer files. Our platform operates under a Zero Data Retention (ZDR) policy with OpenAI (see OpenAI Trust), and AWS Bedrock does not retain customer data (see AWS Data Privacy).

How We Keep Your Information Safe

All files uploaded to the platform are considered customer data, and Weave follows industry best practices to protect this information. 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 production systems and customer data, continuous system monitoring, and strict policies around data access and control.

Weave uses OpenAI models under a Zero Data Retention (ZDR) policy, currently GPT-4.1 and text-embedding-3-small. Model updates occur only after verification of performance improvements and successful regression testing.

A contracted security team performs regular audits and provides continuous monitoring of Weave's corporate, application, and infrastructure environments to detect and address anomalous activity.

Incident Response

In the event of a data breach or security incident, Weave will follow its incident response policy and take immediate action to secure affected systems. Impacted customers will be notified within 24 hours, including the scope and significance of the event. Comprehensive details will be shared within 72 hours after the investigation concludes.

Weave works with a dedicated security contractor to assist in root cause analysis and provide remediation recommendations. Throughout the process, we remain committed to transparent and proactive communication with our customers.

© 2025 Weave. All rights reserved.