Privacy & security

Trust is the most important currency at Abridge. We hold ourselves accountable to a HIPAA-compliant data storage and processing protocol for all data captured and shared through our platform.

1. Internal personnel security
   - Security starts with our people. All Abridge employees are required to:
     - Undergo background checks before being hired.
     - Complete annual security awareness training, HIPAA training, privacy training, and information classification training.

2. Compliance
   - Abridge conducts regular risk assessments to ensure policies remain up-to-date and relevant.
   - Abridge is HIPAA compliant.

3. Secure Software Development Lifecycle (SSDLC)
   - Abridge’s Secure Software Development Lifecycle (SSDLC) ensures the confidentiality, integrity, and availability of your data.
   - All software changes are reviewed, subjected to automated testing, and deployed via automated tools.
   - Our enterprise-grade infrastructure is managed using the same secure software development practices used for application development.
   - All engineers complete secure development practices training, which covers application and development security risks such as the OWASP Top 10.

For more information, please contact us at privacy@abridge.com
Cloud hosting and availability

- All data is stored and processed within HIPAA-compliant and secure cloud data centers in the U.S.
- Abridge leverages high-availability infrastructure to scale up with workload and ensure your data is always accessible.

Confidentiality and data encryption

- All data is encrypted at-rest and in-transit using FIPS 140-2 Validated encryption.
- Abridge practices the principle of least-privilege access. We invest in tooling and automation so that employees do not need to access customer data during normal duties.

Monitoring and alerting

- Abridge uses automated systems to detect and report unusual or suspicious activity.
  Incidents are escalated and resolved through a documented process to find and remediate systemic issues.
- Abridge conducts weekly vulnerability scans and regular penetration tests of critical systems using third-party security firms. We maintain a dedicated channel for reporting security issues.

Vendor management

- Vendors are required to sign a BAA whenever appropriate to safeguard data and operations.
- Abridge regularly reviews vendor security practices to ensure continued high standards.

For more information, please contact us at privacy@abridge.com