Calvient

Security and Privacy at Calvient

Security is at the heart of what we do. Helping our customers improve their security and compliance posture starts with our own. We build, operate, and maintain our platform with security woven into every layer.

Generated on: October 31, 2026 12:12 PM UTC

Governance

Calvient's Security and Compliance teams establish policies and controls, monitor compliance with those controls, and demonstrate our security posture to third-party auditors. Access is limited to those with a legitimate business need and granted on the principle of least privilege. We implement and layer controls according to defense-in-depth and apply them consistently across the enterprise. Our approach is iterative: we continuously mature controls to improve effectiveness, auditability, and ease of use.

Security & Compliance

Calvient maintains industry-recognized compliance certifications and aligns with leading security frameworks to protect our customers' healthcare data.

HIPAA **SOC 2 Type II** **NIST AI RMF**

Our SOC 2 Type II certification was achieved in April 2026 and addresses the Trust Services Criteria for Security, with optional criteria (e.g., Confidentiality, Availability) as documented in our Trust Center. Our AI practices are assessed internally against NIST AI RMF 1.0; documentation is available in our Trust Center.

Detailed compliance documentation and audit reports are available in our Trust Center.

How We Align with HIPAA

HIPAA compliance for healthcare software is governed by three primary rules. Calvient's practices align with each as follows:

Privacy Rule (45 CFR Part 164, Subpart E)

We use and disclose protected health information (PHI) only as permitted by our agreements and policies. Access to PHI is limited to the minimum necessary required for the purpose — whether supporting your workflows, operating

our platform, or responding to your requests.

Security Rule (45 CFR Part 164, Subpart C)

We implement administrative, physical, and technical safeguards for electronic PHI (ePHI) as described throughout this document — including encryption, access controls, audit logging, risk assessments, and incident response. Our controls are designed to meet or exceed the Security Rule's requirements.

Breach Notification Rule (45 CFR Part 164, Subpart D)

In the event of a breach of unsecured PHI, we follow documented procedures to notify affected individuals and, where required, the Secretary of HHS within 60 days of discovery. We also activate our incident response process within 72 hours of identifying a security incident, in line with evolving regulatory expectations.

Evolving regulatory expectations

We track and align with evolving HIPAA Security Rule expectations, including stronger encryption and transport security, required MFA for ePHI access, structured patch management, continuous monitoring, annual risk assessment, and timely incident response and documentation retention. Detailed evidence of our controls is available in our Trust Center.

Data Protection

Data at Rest

All datastores containing customer data are encrypted at rest using AES-256 or equivalent industry-standard algorithms. Sensitive data is additionally protected with field-level encryption — meaning data is encrypted before it reaches the database so that neither physical access nor logical access to the database is enough to read the most sensitive information.

Data in Transit

Calvient uses TLS 1.2 or higher (TLS 1.3 where supported) everywhere data is transmitted over potentially insecure networks. We also enforce HSTS (HTTP Strict Transport Security) to maximize the security of data in transit. Server TLS keys and certificates are managed by our cloud provider and deployed via secure load balancers.

Secret Management

Encryption keys are managed via cloud-based key management services with hardware security module (HSM) backing, preventing direct access by any individuals. Key rotation is performed in accordance with our key management policy. Application secrets are encrypted and stored securely, with access strictly limited to authorized services and personnel.

Audit Logging & Accountability

Access to ePHI and other sensitive data is logged with sufficient detail to support accountability and investigation — including who accessed what, when, and from where. Where applicable, we maintain tamper-evident, append-only audit trails and retain logs for at least six years in line with HIPAA documentation expectations. We monitor and alert on suspicious or inappropriate access patterns so that issues can be addressed promptly.

Hosting & Infrastructure

Calvient operates in a HIPAA-eligible cloud environment. Customer data is logically isolated by tenant: access controls, data storage, and processing are scoped so that each customer's data is segregated from other customers' data and accessible only according to that tenant's authorization and our contractual and policy commitments.

Product Security

Penetration Testing

Calvient engages leading external penetration testing firms at least annually. All areas of our product and cloud infrastructure are in scope for these assessments, with source code fully available to testers to maximize effectiveness and coverage.

Vulnerability Scanning

At key stages of our Secure Development Lifecycle we run static analysis (SAST) during code review, software composition analysis (SCA) for supply chain risks, and dynamic analysis (DAST) against running applications. We also scan dependencies for known vulnerabilities and malicious packages so that we can address issues before they reach production. We remediate vulnerabilities according to risk-based timelines, with critical and high-severity issues prioritized; specific remediation targets are documented in our Trust Center.

Secure Development & Test Data

Development and test environments do not use production PHI. We use only synthetic or properly de-identified data in non-production environments. Credentials and secrets are not stored in source code; they are managed through secure pipelines and secret stores. Application and support logs are designed to avoid inclusion of PHI; where identifiers are necessary for troubleshooting, they are handled through audited, access-controlled channels.

Administrative Safeguards

Calvient maintains administrative policies and procedures that support our security and compliance posture. We conduct an annual risk analysis, maintain a risk management plan, and retain related documentation for at least six years. Our contingency and disaster recovery plans are documented and include defined recovery time and recovery point objectives (RTO/RPO); backups are performed at a frequency set in those plans, and we run periodic recovery tests to verify we can restore. A documented incident response plan guides our response to security incidents, which we activate within 72 hours of identification. Designated Security and Privacy Officers (or equivalents) lead our programs; further detail is available in our Trust Center.

Enterprise Security

Endpoint Protection

All corporate devices are centrally managed and equipped with mobile device management (MDM) software and anti-malware protection. We use MDM to enforce secure configurations including disk encryption, screen lock policies, and timely software updates. Endpoint security alerts are monitored continuously.

Identity & Access Management

Calvient enforces strong identity and access management practices. We require multi-factor authentication and utilize phishing-resistant authentication factors wherever possible. Employee access is role-based, granted according to the principle of least privilege, and automatically deprovisioned upon termination. We conduct periodic access reviews and apply separation of duties for sensitive access where appropriate.

Vendor Security

Calvient uses a risk-based approach to vendor security. Factors influencing a vendor's risk rating include access to customer and corporate data, integration with production environments, and potential impact to our customers. Each vendor's security posture is evaluated to determine a residual risk rating before approval.

Business Associate Agreements (BAAs)

We maintain Business Associate Agreements (BAAs) with all vendors that create, receive, maintain, or transmit PHI on our behalf — including infrastructure providers, support tools, and subprocessors. Our BAA with customers is available upon request and through our Trust Center.

Security Education

Calvient provides comprehensive security training to all employees upon onboarding and annually. All new engineers attend mandatory onboarding sessions focused on secure coding principles and practices. Our security team shares regular threat briefings with employees to inform them of important security updates requiring action.

Incident Response & Breach Notification

We maintain a documented incident response plan. For security incidents, we activate response within 72 hours and follow procedures for containment, investigation, and notification. In the event of a breach of unsecured PHI, we notify

affected individuals and, where required, the Secretary of HHS within 60 days of discovery, in accordance with HIPAA's Breach Notification Rule.

AI Risk Management

As an AI-powered healthcare platform, Calvient is committed to building safe, transparent, and responsible AI systems. We conduct an internal assessment aligned to the NIST AI Risk Management Framework (NIST AI RMF 1.0); documentation of our AI risk management practices is available in our Trust Center. We maintain clear documentation of how our AI models are trained, what data they process, and how decisions are made so that customers understand the technology working on their behalf. Our AI is designed to augment human decision-making, not replace it; critical clinical and operational decisions always keep a human in the loop. We proactively test for and mitigate bias to support equitable outcomes across diverse patient populations and healthcare settings, and we continuously monitor our AI for performance, accuracy, and safety with feedback loops that help us identify and address anomalies quickly.

Data Privacy

At Calvient, data privacy is a first-class priority. We strive to be trustworthy stewards of all sensitive data — especially the protected health information (PHI) entrusted to us by our healthcare partners.

Data lifecycle at contract end. Upon contract termination or at the end of the agreed retention period, we support data return or export in an agreed format upon request. Data we retain is securely deleted in accordance with our data retention and deletion policies and our agreements with you. Further details are set out in our contracts and available in our Trust Center.

For our Privacy Policy, Terms of Use, and Customer Trust commitments, visit **calvient.com**.

Trust Center

For detailed security documentation, compliance certifications, penetration test summaries, and audit reports, visit our comprehensive Trust Center.