Sysevo · Published website snapshot · Captured 21 November 2026
Source: https://www.sysevo.io/security
Engagement-specific signed terms remain governed by their agreements.

Security

Security, privacy and compliance.

Read about our approach to data protection, the current status of our compliance work and the documents available to your organisation.

View compliance & public documents

How your data is handled today

Transport and storage safeguards

Public Sysevo services use HTTPS/TLS. Healthcare readiness also requires review of encryption, storage, backups and key controls across the specific services proposed for PHI processing.

Tenant isolation & access control

We use database row-level policies and account-scoped access controls to protect access to business records. Privileged service credentials are kept server-side. Healthcare approval requires additional validation across the enabled features and integrations.

Authentication & session security

Platform sign-in and user sessions use managed authentication and account permissions. Healthcare access requirements, including privileged access and MFA, must be reviewed as part of the approved service scope.

Card payment processing

Card payment details are collected through Stripe payment flows. Our Privacy Policy explains how billing and payment metadata is used.

Backup and recovery review

Backup coverage and recovery procedures form part of our security programme. Healthcare approval requires verified coverage and tested recovery for the approved processing scope.

Infrastructure responsibilities

We use cloud providers and also operate service components ourselves. Provider responsibilities, Sysevo configuration and service operations all need to be covered by a healthcare review.

GDPR & UK GDPR documentation

Our published documents describe data handling and the responsibilities of Sysevo and our customers. Read our Data Processing Agreement and Privacy Policy.

Public Data Processing Agreement

Our published DPA describes processing responsibilities, subprocessor terms and international transfer arrangements. Healthcare PHI use requires a separately approved service scope and BAA.

Privacy rights and requests

Our Privacy Policy describes applicable rights, how to make a request and how to contact us. Requests are subject to identity verification and applicable legal requirements.

Documented sub-processors

Our DPA sets out subprocessor terms and how changes are handled. Any healthcare use requires a review of the exact providers, services and processing arrangements involved.

Lawful international transfers

Where a sub-processor operates outside the UK/EEA, we rely on appropriate safeguards, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or the SCCs, with additional safeguards where needed.

Consent-gated analytics

Analytics cookies only load after you actively accept them in our cookie banner. Reject them and we simply don't load them: no dark patterns, no pre-ticked boxes.

Compliance status and independent assurance

These programmes have different requirements. HIPAA does not provide an official government certification for software. Our public documents hub records the current status and available materials.

Report not yet available

SOC 2 Type II

Sysevo does not currently hold a SOC 2 Type II report. Any future report will be listed in our documents hub after it is issued and approved for release.

Service-specific approval

HIPAA and healthcare

Healthcare engagements are defined by a service-specific scope, Business Associate Agreement and operating schedules. Review the statement and customer BAA template, then confirm the services, providers and safeguards required for your organisation.

Read the healthcare statement
Not yet certified

ISO 27001

Not pursued yet. If this is a hard requirement for your procurement process, get in touch, it helps us prioritise.

Found a security issue?

We don't have a formal bug bounty program yet. If you find a vulnerability, email us directly and we'll respond as a priority; we won't pursue legal action against good-faith, non-destructive security research.

security@sysevo.io

Also see: Compliance & documents · Privacy Policy · DPA · Terms