Sysevo

HIPAA & HEALTHCARE DATA PROTECTION

HIPAA and Healthcare Data Protection Statement

Version 2.0 | Updated 21 November 2026

A detailed framework for healthcare service scope, protected information, safeguards and the responsibilities shared by Sysevo, customers and approved providers.

Contents

1. Purpose, scope and contractual framework

2. HIPAA roles and accountable responsibilities

3. Information categories and healthcare workflows

4. Permitted purposes, instructions and minimum necessary use

5. Governance, risk management and workforce safeguards

6. Identity, authorisation and support access

7. Technical safeguards and tenant boundaries

8. Physical safeguards and workforce devices

9. AI, voice, transcription and recordings

10. Subcontractors, integrations and processing locations

11. Audit records, monitoring and operational logging

12. Retention, return, destruction and offboarding

13. Individual access, amendments and disclosure accountings

14. Security incidents and breach response

15. Availability, backup and recovery arrangements

16. Customer configuration and day-to-day responsibilities

17. Assurance, evidence review and material changes

18. Documents, interpretation and enquiries

Regulatory references

Current online statement: www.sysevo.io/compliance/hipaa

1. Purpose, scope and contractual framework

This statement explains the data-handling requirements and responsibilities for a Sysevo healthcare engagement involving protected health information (PHI). It is intended for healthcare organisations, procurement teams, privacy and security reviewers, and administrators responsible for configuring and operating the service.

The applicable Services Agreement, Business Associate Agreement (BAA) and completed service schedules define the legal entities, authorised workflows, permitted information, processing locations and obligations for each engagement. Where a PHI-processing term conflicts, the executed BAA governs that subject to the extent consistent with applicable law.

Healthcare PHI processing requires explicit written service approval and an executed BAA before it begins. A subscription, demonstration, integration connection or access to a platform feature does not extend the agreed healthcare scope. This public statement describes the engagement framework; customer-specific evidence and terms are supplied through the confidential review process.

2. HIPAA roles and accountable responsibilities

The customer identifies whether it is acting as a covered entity or an upstream business associate. Sysevo acts as a business associate or subcontractor business associate for the activities assigned to it in the agreed scope. Each party retains the duties imposed directly on it by HIPAA and other applicable law.

The engagement identifies accountable security and privacy contacts, operational owners, customer administrators and deputies. Responsibilities for authorising access, approving changes, handling individual requests and coordinating incidents must be clear, including where more than one organisation participates in a workflow.

- The customer determines lawful purposes and instructions, applicable patient notices or permissions, its authorised users and any restrictions that affect the service.

- Sysevo’s assigned responsibilities are documented in the BAA and service schedules, including relevant safeguards, assistance, supplier obligations and reporting.

- Clinical assessment, diagnosis, treatment decisions and emergency response remain with appropriately qualified healthcare professionals and the customer’s designated clinical process.

3. Information categories and healthcare workflows

PHI can include information that links a person to healthcare provision or payment, even where no diagnosis is discussed. Appointment details, callback requests, caller identities and administrative conversations may therefore need the same handling protections as more obviously clinical content.

The service inventory must describe information created, received, maintained or transmitted through the approved workflow. It covers source material and derived records rather than treating a recording, transcript or summary as an isolated object.

- Contact details, patient or customer identifiers, appointments, reminders, booking records and permitted administrative communications.

- Voice audio, call metadata, recordings, transcripts, meeting content and any approved attachments or message content.

- AI inputs and outputs, summaries, extracted fields, caller-memory records, search indexes, embeddings and workflow history where enabled.

- Exports, support access, audit events, operational traces, temporary processing, supplier-held copies and backups relevant to the engagement.

4. Permitted purposes, instructions and minimum necessary use

PHI may be handled only for the services and purposes authorised in the BAA and scope, to perform the agreement, or as required by law. Access and disclosure are limited to the information and recipients appropriate to the authorised task, applying the minimum-necessary standard where applicable.

The customer BAA template excludes PHI use for advertising, sale, unrelated product development and general-purpose model training. Additional management, administration, aggregation or other permissions require express written agreement consistent with HIPAA; they are not implied by general product terms.

An instruction that introduces a new data category, recipient, purpose or integration must be reviewed before processing changes. Questions about authority, restrictions or conflicting instructions are escalated to the designated privacy and customer contacts.

5. Governance, risk management and workforce safeguards

The healthcare service review considers confidentiality, integrity and availability across the complete workflow. The assessment identifies threats, vulnerabilities, existing controls, likelihood, impact, treatment owners and residual risk, with evidence supporting the approval decision.

Operating requirements include documented policy ownership, role-appropriate workforce training, access reviews, incident reporting routes, change control and corrective-action tracking. Material changes, significant incidents and new supplier or model dependencies require reassessment.

Where a HIPAA implementation specification is addressable, the responsible reviewer records the reasonable and appropriate measure or a justified alternative under the applicable rule. A risk acceptance cannot waive a legal duty or an agreed customer restriction.

6. Identity, authorisation and support access

Access requirements are defined for workforce members, customer users, service accounts and support operators. They include individual identities, approved roles, tenant scope, least privilege, authentication, privileged-access controls, session handling and timely removal of access when responsibilities change.

Customer and patient-facing workflows require checks appropriate to the information being disclosed. Possession of a telephone number, caller ID, a remembered conversation or an unverified message is not, by itself, sufficient authority to release patient-specific information.

Support and emergency access require an authorised purpose, attributable operator, limited scope and duration, and a reviewable record. Emergency procedures must address revocation and retrospective review. They do not create an unrestricted route around normal protections.

7. Technical safeguards and tenant boundaries

The approved technical design must address access to data through the application, APIs, integrations, storage, background tasks and privileged service operations. Tenant boundaries must be evaluated using both permitted actions and attempts to access another customer’s records.

Transmission and storage protections, key access, secret handling and recovery dependencies are reviewed for the specific systems involved. Any agreed encryption specifications, regions or key-management responsibilities belong in the service schedule and supporting assurance evidence rather than being assumed from a platform or supplier name.

Public pages, demonstrations, widgets, sharing links and download routes require separate consideration. Where a capability link is authorised, its recipient, object scope, expiry, revocation, access record and caching behaviour must be appropriate to the information shared.

8. Physical safeguards and workforce devices

The scope review includes physical access to relevant hosting facilities and workforce equipment, taking account of the division of responsibilities with infrastructure providers. Supplier evidence must relate to the actual facility or service used.

Device and workstation requirements address authorised use, screen locking, supported software, patching, endpoint protection, encryption where appropriate, and secure return, reuse or disposal. Remote work and local downloads are included in the access and device review.

PHI must not be copied to personal storage, unmanaged devices or unapproved collaboration services simply to complete a support or operational task. Any approved exception requires a documented purpose, protective measures, expiry and accountable review.

9. AI, voice, transcription and recordings

AI and telephony review covers the entire processing chain: call transport, realtime inference, speech recognition and synthesis, tools, recording, transcription, post-call analysis, caller memory and subsequent use by assistants or integrations. A covered voice service does not automatically cover a separate analysis or meeting provider.

The approved configuration identifies the exact service, model, endpoint, account or workspace, processing location, retention setting and applicable agreement. Provider training-use settings, troubleshooting access and tracing are examined alongside normal request handling.

Recording and transcription are separate processing choices. Their purpose, permissions, retention and recipients must be agreed. Turning off one output does not prove that audio, temporary copies, diagnostics or another derived record is absent.

Fallbacks, retries, tools and new models must follow the same approval boundaries. AI output requires review appropriate to its intended use; it must not be treated as an independently verified clinical decision.

10. Subcontractors, integrations and processing locations

The supplier schedule identifies legal entities and the precise services that create, receive, maintain or transmit PHI on the engagement's behalf. Where required, written downstream BAAs must impose the applicable restrictions, conditions and safeguards before that processing begins.

Due diligence considers service exclusions, subprocessors, support access, processing regions, security evidence, incident escalation, individual-rights assistance, retention, return and destruction. A vendor badge, a general enterprise plan or a different product's BAA is not evidence of coverage for the route actually used.

Customer-selected integrations must be reviewed against their intended information flows and contractual responsibilities. Supplier, region and integration changes follow the agreed notice and review process. No universal US-only, UK-only or EU-only hosting commitment is made by this public statement.

11. Audit records, monitoring and operational logging

The agreed audit scope identifies the actions that require attributable records, including relevant access, changes, exports, support activity and sharing. Records should establish the actor or system, tenant context, action, time, outcome and useful correlation without unnecessarily duplicating PHI.

Operational logs, monitoring alerts, prompt traces, URLs, exception messages and support tickets require data-minimisation controls. Audio, transcripts, credentials, bearer tokens and unrestricted signed links must not become routine troubleshooting content.

Log access, integrity, retention and collection failures form part of the operational review. General security alerts and a successful request response do not, by themselves, demonstrate complete data-access accountability.

12. Retention, return, destruction and offboarding

The engagement schedule specifies retention by information class, including the purpose, triggering event, duration, responsible owner, return or disposal method, legal holds and verification. Audio, transcripts, AI-derived records, messages, attachments, indexes, temporary files, logs and supplier copies may require different schedules.

Contract termination includes verified return recipients, agreed formats and secure delivery, followed by destruction where feasible. Where return or destruction is infeasible, the basis and remaining copies must be documented, contractual protections continue, and further use or disclosure is limited to the purposes making disposal infeasible.

Backup expiry and restoration restrictions are addressed explicitly. A deletion from the live application is not assumed to remove historical backups or independently held supplier copies. Restoration procedures must account for applicable deletion instructions and legal holds.

HIPAA’s documentation-retention duties are distinct from the retention period for every patient record or recording. Applicable law, the customer’s instructions and the agreed service schedule determine the relevant data lifecycle.

13. Individual access, amendments and disclosure accountings

The BAA assigns assistance with access, amendment and accounting obligations and identifies the designated record sets or other relevant records held for the customer. The customer ordinarily coordinates the individual’s request unless direct handling has been expressly delegated.

The request process records receipt, verified authority, scope, responsible custodian, applicable deadline and secure delivery. Assistance periods must allow the customer to meet its own legal duties. Information must not be released to an unverified requester or the wrong tenant.

Requests may require examination of source and derived records, approved exports and relevant supplier-held information. Amendments and disclosure information are handled according to the agreement and applicable rules, with an attributable completion record and documented treatment of any lawful restriction.

14. Security incidents and breach response

The incident process distinguishes a suspected event, a security incident, an impermissible use or disclosure and a breach requiring notification. It assigns response ownership, containment, evidence preservation, investigation, mitigation, recovery and follow-up actions.

The privacy review considers applicable exceptions and, where relevant, whether a documented assessment supports a low probability that PHI was compromised. It examines the information involved, unauthorised recipients, evidence of acquisition or viewing, and mitigation. A technical fix alone does not settle the notification decision.

The BAA specifies monitored customer and supplier contacts, discovery or awareness triggers, initial reporting, updates and escalation. Business-associate breach notice must be provided without unreasonable delay and within the applicable legal limit; tighter contractual duties apply where agreed. Investigation must not postpone required reporting.

The parties identify who is responsible for individual, regulator and other required notices. Available affected-person information, relevant dates, data categories and mitigation details are communicated securely and supplemented as the investigation develops.

15. Availability, backup and recovery arrangements

The service review identifies critical dependencies, recovery priorities, acceptable data loss and restoration objectives for each approved workflow. Any committed recovery point or recovery time objective is recorded in the engagement schedule and supported by the relevant recovery evidence.

Recovery planning considers database records, authentication, recordings and other objects, configuration, keys, telephony, queues and supplier dependencies. A backup indicator does not establish that those components can be restored together with the correct access boundaries.

Exercises and operational procedures address integrity, tenant isolation, restoration order and reconciliation of pending work. Recovered automations must not create duplicate calls, messages or other customer actions. Clinical emergencies and continuity of patient care remain subject to the customer’s designated procedures.

16. Customer configuration and day-to-day responsibilities

The customer designates authorised administrators and maintains accurate users, roles, contact routes and permitted purposes. It communicates relevant restrictions, changes in permissions and agreed amendments, and ensures its staff understand the approved service boundaries.

The customer is responsible for lawful instructions and the notices, consents or other legal bases applicable to its use. HIPAA permission does not independently resolve call-recording, automated-calling, messaging, employment or other jurisdiction-specific requirements.

Customers must use the agreed channels for PHI, review recipient and integration settings, report suspected incidents promptly and involve Sysevo before extending the workflow. Public demonstrations, website enquiry forms and ordinary procurement emails are for business requirements rather than patient records.

17. Assurance, evidence review and material changes

Service-specific due diligence may include the BAA, completed schedules, supplier scope, relevant policies, access-control evidence, security-testing summaries, recovery results, retention arrangements and incident processes. Evidence is exchanged with proportionate confidentiality and protection for other customers and system security.

The review distinguishes documented requirements, configured controls, tested behaviour and operating evidence. The scope and date of an assessment matter; a document, vendor agreement or successful build alone is not a universal assurance conclusion.

Material feature, supplier, model, location, configuration or contractual changes require assessment against the approved service scope. The responsible owners record decisions, required testing, customer notices and any updated approval before changed PHI processing begins.

18. Documents, interpretation and enquiries

The public compliance library contains this statement, the customer BAA template, the security overview and general legal policies. The BAA template includes service authorisation, incident notification, individual-rights assistance, assurance/change and retention schedules for completion before signature.

The general Data Processing Agreement addresses its stated data-protection terms and does not replace a HIPAA BAA. HIPAA does not provide an official government software certification; SOC 2 reporting and ISO certification are separate assurance matters and must be assessed on their own evidence.

This statement is maintained as a versioned public document. The agreement and approved service schedules determine an engagement’s effective terms; downloading a new public version does not silently amend a signed contract. Additional laws or specialised data restrictions require their own applicability review.

Contact security@sysevo.io for healthcare scope, security-review coordination or incident routing. Include the organisation, relevant service and a safe reference to the request. Do not put patient details, recordings, credentials or other sensitive content into an initial website or ordinary email enquiry; request an approved secure exchange route.

Regulatory references

Official guidance supporting the framework; review applicable requirements for the engagement.

HHS: Business associate contracts

https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

HHS: Cloud computing and HIPAA

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

HHS: Breach Notification Rule

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HHS: Individual-rights responsibilities of business associates

https://www.hhs.gov/hipaa/for-professionals/faq/do-business-associates-have-obligations/index.html

HHS: Security Rule certification

https://www.hhs.gov/hipaa/for-professionals/faq/are-we-required-to-certify-our-organizations-compliance-with-the-standards/index.html

45 CFR 164.308: Administrative safeguards

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308

45 CFR 164.310: Physical safeguards

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.310

45 CFR 164.312: Technical safeguards

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

Public documents and customer BAA template: www.sysevo.io/compliance