Customer Business Associate Agreement

H10 · Version 1.0 · Agreement reference: [Agreement reference]

1. Parties and effective date

This Business Associate Agreement (Agreement) is entered into by **[Customer legal entity]**, with its principal address at **[Customer address]** (Customer), and **[Sysevo contracting legal entity]**, with its principal address at **[Sysevo address]** (Business Associate). It supplements the services agreement identified in Schedule A (Services Agreement).

Customer acts as the covered entity or upstream business associate identified in Schedule A. Business Associate acts on Customer's behalf for the healthcare services described in that schedule. This Agreement becomes effective on the date of the last authorized signature below, unless Schedule A specifies a later effective date.

2. Definitions

HIPAA means the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations in 45 CFR Parts 160 and 164, including the Privacy Rule, Security Rule and Breach Notification Rule. Protected Health Information (PHI), Electronic PHI (ePHI), Breach, Unsecured PHI, Security Incident, Required by Law and other defined HIPAA terms have their regulatory meanings. PHI under this Agreement is limited to information Business Associate creates, receives, maintains or transmits on Customer's behalf for the services in Schedule A. Secretary means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

3. Permitted purposes and restrictions

Business Associate may use or disclose PHI only to perform the services and purposes specified in Schedule A, to meet this Agreement, or as Required by Law. It must not use or disclose PHI in a way that would violate the Privacy Rule if done by Customer, except to the extent an express permission in this Agreement and HIPAA permits otherwise.

Business Associate must apply the minimum-necessary standard where applicable. PHI must not be used for advertising, sale, unrelated product development or general-purpose model training. Permission to process PHI does not authorize a different service, integration, provider, model or purpose. Any additional permission for management, administration or data aggregation requires an express written amendment consistent with HIPAA.

4. Safeguards and Security Rule compliance

Business Associate must implement appropriate administrative, physical and technical safeguards against unauthorized use or disclosure. It must comply with applicable requirements of the Security Rule for ePHI, maintain authorized access, protect transmission and storage, and apply the service controls identified in Schedule A.

Where Business Associate performs a Privacy Rule obligation delegated by Customer, it must comply with the requirements that apply to Customer in performing that obligation. It must maintain policies, workforce controls, incident procedures and records appropriate to its obligations.

5. Reporting and cooperation

Business Associate must report uses or disclosures not permitted by this Agreement, Security Incidents of which it becomes aware, and Breaches of Unsecured PHI to the contacts and through the routes specified in Schedule B. Reporting must occur without unreasonable delay and within the shorter of the applicable legal deadline and the deadline in Schedule B. Initial reports may be supplemented as information becomes available; investigation must not delay a required report.

Breach reporting must include affected individuals' identities to the extent known and available information Customer reasonably needs for its notices, including relevant dates, data categories, circumstances, mitigation and contact details. The discovery standard and notification requirements in 45 CFR 164.410 apply. No contractual schedule extends the applicable statutory limit. The parties must cooperate on containment, investigation, mitigation, evidence preservation and required notifications.

6. Subcontractors

Before a subcontractor creates, receives, maintains or transmits PHI on Business Associate's behalf, Business Associate must obtain a written agreement imposing applicable equivalent restrictions, conditions and safeguards, including Security Rule requirements for ePHI. It must maintain the approved service and subprocessor schedule and address known material violations as required by HIPAA. If reasonable steps do not cure or end a material violation, it must terminate the relevant arrangement where feasible and take any further action required by law.

7. Access, amendment and disclosure accounting

Business Associate must make in-scope PHI available to Customer as necessary to support individual access under 45 CFR 164.524. It must assist with amendments under 45 CFR 164.526 and incorporate amendments or provide information needed for Customer to do so. It must document and supply information required for disclosure accountings under 45 CFR 164.528.

The record-set responsibilities, secure delivery routes and assistance deadlines in Schedule C apply. Business Associate must promptly forward individual requests to Customer unless Customer expressly authorizes direct handling. It must verify authority and recipient identity before disclosing information and must not independently refuse a request reserved to Customer. Assistance deadlines must support Customer's applicable legal deadlines.

8. Records and oversight

Business Associate must make its relevant internal practices, books and records concerning PHI under this Agreement available to the Secretary for determining compliance with HIPAA. It must provide Customer the service-specific evidence and cooperation specified in Schedule D, with safeguards for other customers'

information, privileged material and system security. Contractual review arrangements do not limit the Secretary's lawful access.

9. Customer responsibilities

Customer must provide lawful instructions and notify Business Associate of applicable restrictions, permission changes, notice-of-privacy-practices limitations and agreed amendments that affect the services. Customer is responsible for its permitted purpose, required individual notices or permissions, authorized users and obligations not expressly delegated. Neither party may require the other to perform an unlawful use or disclosure.

10. Term, termination and retained information

This Agreement continues while Business Associate handles PHI under the Services Agreement. Customer may terminate the affected services for a material breach of this Agreement. An agreed cure period must not prevent urgent protection or termination required by law.

On termination, Business Associate must return or destroy PHI, including relevant subcontractor-held copies, where feasible. If return or destruction is infeasible, it must document the basis, extend this Agreement's protections to retained PHI, and restrict further uses and disclosures to the purposes making return or destruction infeasible. Schedule E governs return formats, retention, backup expiry, legal holds and disposal evidence. These protections survive for as long as PHI remains retained.

11. Interpretation and changes

This Agreement controls conflicting provisions concerning PHI in the Services Agreement. Other commercial terms remain governed by the Services Agreement to the extent consistent with this Agreement and applicable law. The parties must cooperate on amendments required by changes in law. Amendments and changes to the approved service scope require authorized written agreement. No term limits a duty imposed directly by HIPAA.

12. Authorized signatures

For Customer	For Business Associate
Legal entity: [Customer legal entity]	Legal entity: [Sysevo contracting legal entity]
Name: [Customer signatory]	Name: [Sysevo signatory]
Title: [Customer signatory title]	Title: [Sysevo signatory title]
Signature: [Customer signature]	Signature: [Sysevo signature]
Date: [Customer signature date]	Date: [Sysevo signature date]

Schedule A — Service authorization

Item	Agreed information
Services Agreement	[Services agreement reference and date]
Effective date	[Effective date]
Customer HIPAA role	[Covered entity or upstream business associate]
Authorized healthcare service and purpose	[Workflows and permitted purposes]
Customer tenant or workspace	[Tenant or workspace reference]
PHI categories and individuals	[Data categories and population]
Enabled features and excluded features	[Enabled and excluded features]
Systems, providers, models and integrations	[Approved service and provider schedule reference]
Processing regions and subprocessors	[Approved locations and subprocessor schedule reference]
Customer configuration duties	[Required settings and customer responsibilities]
Additional applicable requirements	[Jurisdictions and any expressly agreed additional health-data terms]

Schedule B — Incident notification

Item	Agreed information
Customer primary and deputy contacts	[Names, monitored addresses and telephone numbers]
Business Associate primary and deputy contacts	[Names, monitored addresses and telephone numbers]
Secure notification route	[Approved communication route]
Initial incident and breach reporting deadline	[Deadline measured from applicable discovery or awareness trigger]
Update cadence	[Update interval and escalation route]
Routine unsuccessful security incidents	[Reporting method and interval; individual reporting where required by law]
Notice responsibilities	[Customer, Business Associate and regulator/individual notification responsibilities]

Schedule C — Individual rights assistance

Item	Agreed information
Designated record sets and custodian	[Record-set boundaries and responsible party]
Access, amendment and accounting request route	[Secure request channel]
Forwarding and assistance deadlines	[Contractual periods supporting applicable legal deadlines]
Verification and delivery	[Authority checks, approved recipient and delivery format]
Direct individual handling, if delegated	[Expressly delegated tasks or none]

Schedule D — Assurance and service changes

Item	Agreed information
Security evidence exchange	[Evidence scope, confidentiality and frequency]
Review and investigation cooperation	[Contacts and reasonable review process]
Service and subprocessor changes	[Notice, review, objection and approval process]
Insurance and commercial terms	[Relevant Services Agreement references]

Schedule E — Retention and termination

Item	Agreed information
Approved retention schedule	[Data classes, purposes, periods and triggers]
Return process	[Recipient verification, format, route and timescale]
Destruction process and evidence	[Method, responsible party and confirmation]
Backup expiry and restoration restrictions	[Backup lifecycle and safeguards]
Legal holds and infeasible disposal	[Approval, basis, continuing restrictions and review]