



BUSINESS ASSOCIATE AGREEMENT

Last updated: March 2026

You and VALD have entered into a Subscription Agreement. This Business Associate Agreement is incorporated into and forms part of the Subscription Agreement.

The Client wishes to disclose certain information to VALD. VALD is deemed a business associate of the Client pursuant to the terms of this agreement and the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') ('**Business Associate**') because some of the information provided by the Client to the Business Associate consists of Protected Health Information ('PHI'), which definition includes Electronic Protected Health Information ('ePHI'), as those terms are defined under HIPAA.

The Client and the Business Associate intend to protect the privacy of and provide for the security of PHI disclosed by the Client to the Business Associate pursuant to this agreement and in compliance with all applicable health data privacy and security laws, as may be amended from time to time.

The parties agree that the obligations under this agreement only apply to the extent that:

- (a) the Client is a "covered entity" and VALD is a "business associate", as those terms are defined under 45 CFR §160.103 of HIPAA; and
- (b) the information disclosed by the Client to the Business Associate is PHI.

All capitalised terms not defined in this agreement or by reference to HIPAA have the meaning given to them in the Subscription Agreement.

1. THE BUSINESS ASSOCIATE'S OBLIGATIONS

1.1 General Obligations

- (a) The Business Associate must take commercially reasonable steps to:
 - (i) maintain the confidentiality, integrity, and availability of all Client PHI it creates, receives, maintains, or transmits;
 - (ii) protect Client PHI against any reasonably anticipated threats or hazards to the security or integrity of such information;
 - (iii) maintain Client PHI, to the maximum extent possible, and in accordance with the latest technical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, in an encrypted manner so as to prevent the unauthorised access to the PHI by an unauthorised individual;
 - (iv) protect against any reasonably anticipated Uses or Disclosures of such information that are not permitted or required under HIPAA and this agreement;
 - (v) ensure that its Workforce complies with HIPAA and this agreement; and
 - (vi) ensure that any agent, including subcontractors or consultants, to whom it provides PHI, agree in writing to no less stringent restrictions and conditions that apply to the Business Associate with respect to PHI.
- (b) In this agreement:
 - (i) '**Use**' means the sharing, employment, application, utilisation, examination, or analysis of PHI within an entity that maintains such PHI;
 - (ii) '**Disclose**' or '**Disclosure**' means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information; and

- (iii) **'Workforce'** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Client or the Business Associate, is under the direct control of the Client or the Business Associate, whether or not they are paid by the Client or the Business Associate.

1.2 Permitted Uses and Disclosures of Protected Health Information

- (a) The Business Associate must only Use or Disclose PHI:
 - (i) for the proper management and administration of the Business Associate's commercial business activities;
 - (ii) to carry out the legal responsibilities of the Business Associate, including performance of the obligations of the Business Associate under the Subscription Agreement;
 - (iii) to provide data processing and other data aggregation services relating to the health care or business operations of the Client;
 - (iv) to complete any data processing as permitted or required under the Subscription Agreement, this agreement or by law; and
 - (v) as permitted or required by this agreement or as required by law.

1.3 Safeguards

- (a) Unless otherwise agreed, the Business Associate will use reasonable and appropriate safeguards designed to prevent inappropriate Use and Disclosure of PHI and comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule and Annexure 1 of this agreement.
- (b) The Business Associate must ensure that any Workforce who receives Client PHI agrees to similar restrictions and conditions that apply to the Business Associate with respect to the relevant PHI under this agreement.

1.4 Reporting of Disclosures

- (a) The Business Associate must, within 21 days of its receipt of any subpoena, discovery request or judicial, governmental or administrative order (**'Required Disclosure Document'**), notify the Client in writing pursuant to clause 6 below and provide the Client with a copy of the Required Disclosure Document requesting or requiring the Business Associate to Disclose PHI.
- (b) The Business Associate must, within 21 days of the Business Associate learning of any Use or Disclosure of PHI not permitted by this agreement or law, document and notify the Client in writing pursuant to clause 6 below of such Use or Disclosure.

1.5 Availability of Information to Client

- (a) The Business Associate agrees to provide, at the Client's request, access to PHI in order to meet the requirements under 45 CFR § 164.524. The Business Associate agrees to provide such access within 30 days of the Client's request.
- (b) The Business Associate must document Disclosures of PHI so that the Client may respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.
- (c) The Business Associate must make its internal practices, books, and records (including policies and procedures) relating to the Use and Disclosure of PHI available to the Secretary for the purpose of determining the Client's compliance with HIPAA in accordance with 45 CFR § 160.310.
- (d) In this Agreement:
 - (i) **'Disclosure'** means the release, transfer, provision of access to, or divulging in any manner of PHI outside the entity holding the information;
 - (ii) **'Individual'** means the person who is the subject of PHI and must include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g); and
 - (iii) **'Secretary'** means Secretary of the U.S. Department of Health and Human Services or their designee.

1.6 Amendments to PHI

- (a) If the Client is required to amend inaccurate or incomplete PHI pursuant to its obligations under HIPAA, the Business Associate must:
 - (i) make copies of PHI available to the Client; and
 - (ii) either:
 - (A) incorporate (as reasonably directed by the Client) any amendments to PHI into any copies of such PHI maintained by the Business Associate; or
 - (B) provide to the Client, in writing, the reasons why the amendment to the PHI requested by the Client (or to the Client by the Individual) is not feasible at the time.
- (b) If the amendment to the PHI is not feasible at the time, then the Business Associate will use reasonable endeavours to delete the applicable PHI. If deletion is not feasible (for example if the PHI is stored in a historical backup for the purposes of disaster recovery, business continuity, system integrity and security) VALD will comply with this agreement until such point that the data is deleted.

1.7 Breach Notification and the Business Associate's Obligations

- (a) During the term of this agreement, the Business Associate must notify the Client in writing without unreasonable delay, but in no event more than 72 hours after any confirmed actual Breach of security, intrusion, or unauthorised Use or Disclosure of Unsecured PHI and/or any confirmed actual Use or Disclosure of PHI in violation of any applicable federal and state laws or regulations.
- (b) A notice under clause 1.7(a) will (to the extent permitted by law) include:
 - (i) the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or Disclosed during such Breach;
 - (ii) a brief description of what happened, including the date of the Breach and the date of the Business Associate's discovery of the Breach;
 - (iii) a description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - (iv) any steps Individuals should take to protect themselves from potential harm resulting from the Breach; and
 - (v) a brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches.
- (c) In the event of a Breach, the Business Associate must take commercially reasonable steps to cure any such deficiencies and any action pertaining to such unauthorised Disclosure required by applicable federal and state laws or regulations.
- (d) A Breach must be treated as discovered by the Business Associate as of the first day on which such Breach is known to the Business Associate.
- (e) In this agreement:
 - (i) **'Breach'** means the confirmed acquisition, access, Use, or Disclosure of PHI in a manner not permitted under this agreement or the applicable HIPAA provisions which compromise either the security or privacy provisions of the PHI. 'Breach' excludes:
 - (A) any unintentional acquisition, access, or Use of PHI by a Workforce member or person acting under the authority of the Client or the Business Associate, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under HIPAA or this agreement;
 - (B) any inadvertent Disclosure by a person who is authorised by a Client or Business Associate to access PHI to:
 - (I) another person authorised to access PHI by a Client or Business Associate; or
 - (II) an organised health care arrangement in which the Client participates; and

- (III) the information received as a result of such disclosure is not further Used or Disclosed in a manner not permitted under HIPAA or this agreement; and
- (C) a Disclosure of PHI where the Client or the Business Associate has a good faith belief that an unauthorised person to whom the Disclosure was made would not reasonably have been able to retain such information.
- (ii) **'Unsecured PHI'** means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorised persons through the use of one or more of the following technologies or methodologies:
 - (A) the encryption of ePHI by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached; or
 - (B) the destruction of the media on which the PHI is stored or recorded.

2. CLIENT OBLIGATIONS

2.1 Safeguards During Transmission

Client must use appropriate safeguards in accordance with the standards and requirements of HIPAA to maintain and ensure the confidentiality, privacy, and security of PHI transmitted to the Business Associate pursuant to the terms of this agreement until such time the PHI is safely received by the Business Associate.

2.2 Notifications

The Client must promptly notify the Business Associate in writing of:

- (a) any limitation(s) in the Client's notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation(s) may affect the Business Associate's Use or Disclosure of PHI;
- (b) any changes made by the Client to, or any revocation of, an Individual's permission to Use or Disclose PHI to the extent that such changes may affect the Business Associate's Use or Disclosure of PHI; and
- (c) any restriction to the Use or Disclosure of PHI that Client has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect the Business Associate's Use or Disclosure of PHI.

3. TERM, TERMINATION AND SURVIVAL

3.1 Term

This agreement shall continue in effect until the expiration or termination of the Client's Subscription Agreement.

3.2 Grounds for Termination

- (a) A finding or stipulation in any administrative or civil proceeding in which the other party has been joined, that such party has violated any standard or requirement of HIPAA or other privacy or security laws, is a **'HIPAA Finding'**.
- (b) The parties agree that any HIPAA Finding will be deemed an Event of Default under the Subscription Agreement, and any other breach of this agreement will be subject to of the provisions of the Subscription Agreement relating to termination for breach of the Subscription Agreement.

3.3 Effect of Termination or Expiration

On termination or expiration of this agreement, VALD will anonymise, delete or return all PHI provided by the Client that VALD holds, if it is feasible to do so. This clause will apply except where VALD is required to retain the PHI in accordance with any applicable law, or where the PHI is archived on a back-up system, in which case that data will be securely stored for no longer than what is reasonably necessary, and ultimately deleted in accordance with VALD's policies. VALD will continue to comply with this agreement until your PHI is anonymised, deleted or returned.

3.4 Survival

The respective obligations and rights of the Client and the Business Associate relating to protecting the confidentiality of PHI must survive for a period of 2 years after the termination or expiration of the Subscription Agreement, or such longer period that the Business Associate retains any PHI or if otherwise required by law.

4. AMENDMENTS

- (a) The parties acknowledge that state and federal laws relating to health information privacy and security may rapidly evolve and that amendments to this agreement may be required from time to time.
- (b) The parties specifically agree to take such action as may be necessary to implement any new or revised legally mandated health information privacy or security requirements, including without limitation, HIPAA standards. Upon the Client's request, the Business Associate must promptly enter into negotiations with the Client concerning the terms of an amendment to this agreement consistent with the standards and requirements of HIPAA or other applicable health information privacy and security laws.

5. INTERPRETATION

This agreement must be interpreted as broadly as necessary to implement and comply with HIPAA and all applicable state laws. The parties agree that any ambiguity in this agreement must be resolved in favour of a meaning that complies and is consistent with HIPAA.

6. MANNER OF NOTIFICATION

Any notice given under this agreement must be in accordance with the applicable notice provisions under the applicable Subscription Agreement.

ANNEXURE 1 – SECURITY REQUIREMENTS

The Business Associate has adopted, implemented, and maintains (and will ensure that its employees, contractors and agents adopt, implement and maintain) the security controls as described below.

- (a) **Maintain a formal information security program, with a named individual responsible for its overall execution.** The Business Associate's information security program must have executive support and be defined based on the characteristics of its business. It must include documented security plans, policies, and procedures designed to protect the confidentiality, integrity, and availability of its information assets. The Business Associate maintains staffing and technical resources at an appropriate level to support the information security program's plans, policies, procedures, ongoing operations, monitoring, and continuous improvement.
- (b) **Periodically conduct an Information Technology ('IT') security risk assessment.** As part of the information security program, the Business Associate periodically conducts an IT security risk assessment to identify threats and vulnerabilities that may affect the systems that are used to deliver services to the Client. The Business Associate prioritises identified risks based on potential business impact and likelihood of occurrence. The Business Associate develops remediation plans for identified vulnerabilities, and prioritises resources to implement remediation plans based on the prioritisation of the associated risks. Risk assessment findings, remediation plans, and exceptions are reviewed and approved by the Business Associate's senior management. Risk assessment is updated periodically or after significant changes to the Business Associate's IT environment.
- (c) **Maintain formal documented instructions for reporting security breaches.** The Business Associate maintains documentation for reporting security breaches, and the Business Associate's users are trained on the process. In the event of a security breach involving the Client's PHI, the Business Associate will notify the Client in accordance with clause 1.7 of this agreement.
- (d) **Assess and manage security risks associated with the Business Associate and subcontractors.** The Business Associate maintains a program for assessing and managing information security risks associated with its Business Associate and subcontractors that have physical or logical access to the Business Associate's IT systems and networks. Where appropriate, required security requirements should be incorporated into contracts between the Business Associate and its subcontractors. Contracts between the Business Associate and its subcontractors will flow down requirements for maintaining any applicable regulatory requirements, such as those for HIPAA, the Federal Information Security Management Act, or the Payment Card Industry Data Security Standard.
- (e) **Maintain employee on-boarding and off-boarding policies and procedures.** Ensure that new employees receive a level of screening appropriate for their roles, including, but not necessarily limited to, professional reference checks and criminal background checks. Require that new employees complete security awareness training, which should include relevant information on HIPAA and the handling of PHI, within 30 days of the later of their hire date or their official start date with the Business Associate. Upon employee termination, ensure that access to the Business Associate's systems and networks (including remote access via VPN) is discontinued in a timely fashion, and any Business Associate-issued IT assets (e.g., laptops, mobile phones, or portable storage media) are collected prior to the employee's separation from the company. The Business Associate must ensure that terminated employees are not able to access systems or information related to the delivery of services to the Client.
- (f) **Ensure continuing employee awareness of and education on security policies, standards, and procedures.** The Business Associate will provide formal security training to all employees and contract staff. Formal procedures and scope of administrator's roles and security procedures are specified. All of the Business Associate's users will undergo annual security training. The Business Associate maintains security policies, rules, procedures and instructions for continued security awareness and education.
- (g) **Maintain policies and procedures that establish the rules for granting and modifying access, documentation of changes to access rights, and account termination procedures.** All the Business Associate's user accounts are set up based on their roles and are restricted to privileges based on job duties, project responsibilities, and other relevant business activities. The Business Associate user accounts are removed from all critical systems immediately upon termination of employment or contractual relationship with the Business Associate.
- (h) **Prevent access to information and resources unless authorised.** The Business Associate has policies, procedures, and technical controls in place to ensure that access to the Business Associate's systems and applications will be denied unless the user has entered a valid user ID and password. The Business

Associate's user accounts will be configured to lock after a minimum of 3 unsuccessful login attempts. Only authorised networks and users are allowed access to the Business Associate's servers and applications.

- (i) Maintain policies and procedures for the supervision and accountability of people who have physical access to servers and other essential components, or sensitive information. The Business Associate ensures that policies and procedures are in place and monitored to secure servers, and other essential components of the system, via for example, physical security practices achieved under the Cloud Shared Responsibility Model. 'Cloud Shared Responsibility Model' means a cloud-security framework that defines, based on the type of cloud service used, which security responsibilities rest with the cloud service provider and which remain with the client or customer. These responsibilities change depending on whether the service is IaaS (Infrastructure as a Service), PaaS (Platform as a Service), or SaaS (Software as a Service).
- (j) **Limit the time that an unattended, logged-in system is vulnerable to unauthorised use.** Workstations, laptops, and mobile devices used or managed by the Business Associate's Personnel will be configured to implement screen-lock and require re-authentication after a maximum of 15 minutes of inactivity.
- (k) Maintain password management policies and procedures, including personal accountability for user accounts and limited exposure from password disclosures. The Business Associate's policies, procedures and security features require a unique user ID and password for each user. Any party, including the Business Associate's Personnel or system administrators, cannot discover passwords. At minimum, the Business Associate's users must change their individual passwords on suspicion or confirmation of account compromise and ensure that the Business Associate's password management is aligned with NIST 800-63 standards. Where possible, multi-factor (also called two-factor or two-step) authentication should be used to supplement password security for access into critical systems.
- (l) **Protect systems and networks with firewalls and intrusion detection/prevention systems ('IDS/IPS').** The Business Associate uses firewalls and IDS/IPS to protect its servers, workstations, laptops mobile devices, and other network devices. A combination of network- and host-based firewalls and IDS/IPS may be used to address different risk profiles as determined by the Business Associate's risk assessment. The Business Associate regularly reviews firewall and IDS/IPS rules to ensure that they are still applicable. Firewalls and IDS/IPS are configured to generate automated alerts based on matching signatures of malicious network activity, and management consoles are routinely monitored by the Business Associate's Personnel.
- (m) **Evaluate and install security patches in a timely fashion.** The Business Associate will maintain formally documented security patch management procedures. The Business Associate will evaluate, test, and install security patches based on a risk-based schedule prioritised by the Common Vulnerability Scoring System ('CVSS') score, or a functionally equivalent approach. Security patches identified as a high priority, generally those that address vulnerabilities with a CVSS base score of 7.0 to 10.0, should be installed within 30 calendar days of release, including any system reboots that may be necessary to fully install the patch. The Business Associate will maintain a formal exception management process to review and address risks associated with high priority patches that cannot be installed during this window.
- (n) **Encrypt sensitive information.** The Business Associate will encrypt all sensitive information in transit (e.g., through SSL, SSH, or site-to-site VPNs). A minimum level of 256-bit AES encryption will be employed. Administrative access to the production network is performed over an encrypted channel. Passwords are encrypted during transit and at rest. Full-disk encryption software (e.g., PGP, BitLocker, FileVault, or equivalent) is used to protect any of the Business Associate's workstations and laptops that may be used for either temporary or long-term storage of the Client's PHI.
- (o) **Protect systems against self-propagating malware.** Endpoint security software is installed and maintained on all of the Business Associate's workstations and servers. The software will be properly configured and maintained with an up-to-date scan engine and anti-virus definition files. Endpoint security software will be configured to periodically perform an automated full scan of the system, as well as to actively scan incoming and outgoing network traffic (e.g., through email or web browsing) for viruses. Endpoint security software may be omitted from systems that are not commonly affected by malware (e.g., mainframes) based on the Business Associate's formal, documented risk assessment of those systems.
- (p) **Routinely review and archive operating system and application server logs.** Operating system and application server (e.g., web server, database server, middleware server) logs are regularly automatically

reviewed for account creation or modification, unusual account login activity, system restarts, unusual network events, and other hardware or software alarms that may indicate a system fault or malicious activity. All operating system and application logs are archived in accordance with a documented log retention policy.

- (q) **Use standardised secure build processes to harden servers, workstations, laptops, and other network devices against attack.** The Business Associate has policies and/or procedures in place for building all systems, including servers, workstations, laptops, mobile devices, and network devices, in a manner that hardens them against attacks. Secure build procedures should disable or remove unnecessary network services, applications, and data from systems before placing them into production use.
- (r) **Perform periodic testing for the presence of security measures.** External and internal penetration testing is periodically performed to identify potential security risks that may be exploited by an attacker to gain unauthorised access to the Business Associate's systems and networks. A qualified third-party assessor is used to perform an external penetration test on at least an annual basis. The Business Associate may use its own staff to perform penetration testing if those staff members have adequate training, experience, and certification to conduct such assessments.
- (s) **Maintain a change management program.** The change management program should be formally documented and include processes for requesting, classifying, reviewing, approving, testing, and communicating change requests. The Business Associate agrees to notify the Client of any changes that significantly impact or modify the security of the facilities, processes, and systems used to deliver services to the Client.
- (t) Maintain data backup plans to ensure that the data necessary for service delivery can be recovered in the event of a hardware, software, or facilities failure. The Business Associate maintains policies, procedures, and systems for data backup and restoration, including routine testing of recovery processes to ensure that systems and data can be properly restored.
- (u) Document the chain of custody for backup media and final disposition of electronic data, and/or the hardware on which electronic data is stored. To the extent applicable for services provided to the Client, the Business Associate will maintain documented chain of custody policies and procedures for data backup media that is removed from the Business Associate's data centre and placed in secure storage location (e.g., an off-site vault). The Business Associate will ensure that only authorised Personnel can retrieve the data media from storage locations. In addition, all Client data will be removed from all media before the hardware is disposed of. The Client data on operational storage is securely wiped prior to disposal. Defective storage is physically destroyed prior to disposal.
- (v) Maintain disaster recovery plan, emergency mode operation plan (down-time operation plan) and testing of disaster recovery plan requirements. To the extent applicable for supporting the services provided to the Client, the Business Associate will maintain a documented business continuity and disaster recovery plan and will ensure that testing of the plan has been implemented. Testing of disaster recovery plans is performed periodically to ensure their effectiveness, with the interval of testing occurring, at minimum, once per year.
- (w) Upon the Client's request, provide the Client with documentation describing how the Client data is stored, processed, and transmitted within the Business Associate's IT environment. Documentation requests may include physical and/or logical network maps (including network port numbers and protocols), data flow diagrams, hardware configurations, and software inventories. Storage durations (i.e., delineations between short- and long-term storage) and third-party facilities should be included when applicable. Documentation should be specific to the Client's services with the Business Associate and should not reveal confidential, sensitive or proprietary information related to services that the Business Associate provides to other clients.
- (x) **At the end of the agreement or upon the Client's request, securely destroy the Client's PHI.** The Business Associate will use industry best practices, such as those outlined in NIST Special Publication 800-88, to remove the Client's PHI from all media types, including hard drives, portable storage devices, mobile devices, backup tapes, and paper files upon the Client's request. Attestation and confirmation of destruction must be provided to the Client. Any such Client request is subject to applicable requirements under HIPAA and other applicable laws or regulations.
- (y) **Access the Client's network using the Client approved secure remote access.** The Business Associate agrees to access the Client's network only through Client-provided solutions. Access should occur on an as-needed basis. Remote and onsite access by the Business Associate must be limited to the minimum

necessary information. All of the Business Associate's activities while accessing the Client's systems may be monitored by the Client.