HIPAA BUSINESS ASSOCIATE AGREEMENT

1. 1. Parties, Purpose, and Definitions

This Business Associate Agreement (the "BAA") is made effective as of [EFFECTIVE DATE] between [COVERED ENTITY NAME], a [ENTITY TYPE] located at [COVERED ENTITY ADDRESS] (the "Covered Entity"), and [BUSINESS ASSOCIATE NAME], a [ENTITY TYPE] located at [BUSINESS ASSOCIATE ADDRESS] (the "Business Associate"). The Business Associate provides the following services under the [UNDERLYING SERVICES AGREEMENT TITLE] dated [UNDERLYING AGREEMENT DATE] (the "Services Agreement"): [DESCRIPTION OF SERVICES]. Terms used but not defined in this BAA have the meanings given in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, including "Protected Health Information" ("PHI"), "Electronic Protected Health Information" ("ePHI"), "Breach", "Security Incident", "Required by Law", "Designated Record Set", and "Subcontractor." This BAA is incorporated into the Services Agreement and controls over it on any matter concerning PHI.

2. 2. Permitted Uses and Disclosures of PHI

The Business Associate may use and disclose PHI only as necessary to perform the services described in Section 1, as permitted by this BAA, or as Required by Law. Specifically, the Business Associate may: (a) use PHI to perform the services; (b) disclose PHI to third parties as necessary to perform the services, subject to Section 6; (c) use PHI for the proper management and administration of the Business Associate and to carry out its legal responsibilities; and (d) disclose PHI for its proper management and administration only if the disclosure is Required by Law or if the Business Associate obtains reasonable written assurances from the recipient that the information will be held confidentially, used or further disclosed only as Required by Law or for the purpose it was provided, and that the recipient will notify the Business Associate of any breach of confidentiality. The Business Associate may de-identify PHI in accordance with 45 C.F.R. 164.514 and may provide Data Aggregation services relating to the health care operations of the Covered Entity only if expressly permitted here: [DATA AGGREGATION PERMITTED — YES OR NO].

3. 3. Prohibited Uses and Minimum Necessary

The Business Associate will not use or disclose PHI in any manner that would violate the Privacy Rule if done by the Covered Entity, except as permitted in Section 2(c) and 2(d). The Business Associate will not sell PHI, will not use or disclose PHI for marketing or fundraising, and will not use or disclose genetic information for underwriting purposes. The Business Associate will not use, disclose, transmit, store, or process PHI outside the United States without the prior written consent of the Covered Entity. In every use, disclosure, and request, the Business Associate will limit PHI to the minimum necessary to accomplish the intended purpose, consistent with 45 C.F.R. 164.502(b) and any guidance issued by the Secretary. The Business Associate will not re-identify de-identified information without written authorization.

4. 4. Safeguards

The Business Associate will use appropriate administrative, physical, and technical safeguards to prevent the use or disclosure of PHI other than as permitted by this BAA, and will comply with the Security Rule at 45 C.F.R. Part 164 Subpart C with respect to ePHI. Without limitation, the Business Associate will: conduct and document a security risk analysis at least [RISK ANALYSIS FREQUENCY, e.g., annually]; maintain written policies and procedures and a designated security official; encrypt ePHI at rest and in transit in accordance with guidance issued by the Secretary; enforce unique user identification, role-based access control, and multi-factor authentication for remote access; maintain audit logs of access to PHI for at least [LOG RETENTION PERIOD,

e.g., six years]; train workforce members on HIPAA obligations at hire and at least [TRAINING FREQUENCY, e.g., annually]; sanction workforce members who violate these obligations; and maintain a documented contingency, backup, and disaster recovery plan. The Business Associate will provide evidence of these safeguards on request.

5. 5. Reporting of Security Incidents and Breach Notification

The Business Associate will report to the Covered Entity any use or disclosure of PHI not permitted by this BAA, any Security Incident, and any Breach of Unsecured PHI of which it becomes aware. Notification will be made without unreasonable delay and in no case later than [NUMBER] days after Discovery of a Breach, and no later than [NUMBER] days after discovery of any other impermissible use or disclosure or of any Security Incident that resulted in unauthorized access to, or acquisition, use, disclosure, modification, or destruction of, PHI. Unsuccessful Security Incidents that do not result in unauthorized access to PHI — such as routine firewall pings, port scans, and blocked login attempts — will be reported in the aggregate [AGGREGATE REPORT FREQUENCY, e.g., quarterly]. The report will include, to the extent known: the identity of each individual whose PHI was involved; the date of the incident and the date of Discovery; a description of what occurred and the types of PHI involved; the steps taken to investigate, mitigate, and prevent recurrence; and any other information the Covered Entity needs to satisfy its own notification obligations under 45 C.F.R. Part 164 Subpart D. The Business Associate will supplement the report as additional information becomes available, will cooperate fully with the Covered Entity's risk assessment, and will not notify individuals, regulators, or the media without the Covered Entity's prior written approval unless Required by Law. Unless otherwise agreed in writing, the Business Associate is responsible for the reasonable costs of notification, credit monitoring, and mitigation arising from a Breach caused by the Business Associate or its Subcontractors.

6. 6. Subcontractors and Flow-Down

The Business Associate will ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to restrictions and conditions at least as protective as those that apply to the Business Associate under this BAA, in accordance with 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2). The Business Associate will maintain a current list of such Subcontractors and will provide it to the Covered Entity on request, together with a copy of the executed agreement. The Business Associate will [SELECT — obtain the Covered Entity's prior written consent before engaging any new Subcontractor / notify the Covered Entity at least [NOTICE PERIOD, e.g., 30 days] before engaging any new Subcontractor, with the right to object]. The Business Associate remains fully responsible to the Covered Entity for the acts and omissions of its Subcontractors relating to PHI as if they were its own.

7. 7. Individual Rights — Access, Amendment, and Accounting

Within [NUMBER] days of a written request from the Covered Entity, the Business Associate will make PHI it maintains in a Designated Record Set available to the Covered Entity, or as directed to the individual, so the Covered Entity can meet its obligations under 45 C.F.R. 164.524, including providing an electronic copy in the form and format requested where readily producible. Within [NUMBER] days of a written request, the Business Associate will incorporate any amendment to PHI in a Designated Record Set as directed by the Covered Entity under 45 C.F.R. 164.526. Within [NUMBER] days of a written request, the Business Associate will provide the information required for the Covered Entity to respond to a request for an accounting of disclosures under 45 C.F.R. 164.528, and will document disclosures and related information for at least six years. If an individual contacts the Business Associate directly with a request, the Business Associate will forward it to the Covered Entity within [FORWARDING PERIOD, e.g., five business days] and will not respond directly unless directed to do so in writing.

8. 8. Compliance with Restrictions and Covered Entity Obligations

The Business Associate will comply with any restriction on the use or disclosure of PHI that the Covered Entity has agreed to under 45 C.F.R. 164.522 and has communicated to the Business Associate, and with the Covered Entity's Notice of Privacy Practices and any limitation in an individual authorization or its revocation, to the extent those affect the Business Associate's permitted uses. The Covered Entity will notify the Business Associate of any such restriction, change to its Notice of Privacy Practices, or revocation of authorization that affects the Business Associate's use or disclosure of PHI. The Covered Entity will not request the Business Associate to use or disclose PHI in a manner that would violate HIPAA if done by the Covered Entity, except as permitted by Section 2(c) and 2(d).

9. 9. Availability of Books and Records to HHS

The Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received on behalf of, the Covered Entity available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with HIPAA. The Business Associate will notify the Covered Entity in writing within [AGENCY NOTICE PERIOD, e.g., five business days] of receiving any request, inquiry, subpoena, or notice of investigation from the Secretary or any other governmental authority concerning PHI received from the Covered Entity, unless prohibited by law, and will provide the Covered Entity with copies of any materials produced.

10. 10. Audit, Documentation, and Cooperation

On [AUDIT NOTICE PERIOD, e.g., 30 days] prior written notice and no more than [AUDIT FREQUENCY, e.g., once per year] except following a Breach, the Covered Entity or its designated representative may review the Business Associate's HIPAA policies, procedures, risk analyses, training records, and audit logs relating to PHI received from the Covered Entity. In place of an on-site audit, the Business Associate may provide a current [ALTERNATIVE EVIDENCE, e.g., SOC 2 Type II report, HITRUST certification, or independent security assessment] covering the systems used to process the Covered Entity's PHI. The Business Associate will retain all documentation required by this BAA and by HIPAA for at least six years from the date of creation or the date it was last in effect, whichever is later, and will cooperate with the Covered Entity in responding to individual complaints and regulatory inquiries.

11. 11. Term and Termination for Cause

This BAA takes effect on the Effective Date and continues until all PHI received from, or created or received on behalf of, the Covered Entity is returned or destroyed in accordance with Section 12, or until terminated as provided here. The Covered Entity may terminate this BAA and the Services Agreement immediately, without penalty, if it determines that the Business Associate has materially breached this BAA and the breach is not cured within [CURE PERIOD, e.g., 30 days] after written notice, or if cure is not possible. If neither termination nor cure is feasible, the Covered Entity will report the violation to the Secretary. Termination of the Services Agreement for any reason terminates this BAA, except that the obligations in Sections 5, 7, 9, 10, 12, and 13 survive.

12. 12. Return or Destruction of PHI on Termination

On termination or expiration of this BAA, the Business Associate will return to the Covered Entity or securely destroy all PHI received from, or created or received on behalf of, the Covered Entity that the Business Associate or its Subcontractors still maintain in any form, and will retain no copies. Return or destruction will be completed within [RETURN PERIOD, e.g., 30 days], in the format [RETURN FORMAT, e.g., a mutually agreed structured

electronic export], and destruction will follow a method consistent with guidance issued by the Secretary for rendering PHI unusable, unreadable, or indecipherable. The Business Associate will provide written certification of destruction within [CERTIFICATION PERIOD, e.g., 10 days] of completion. If return or destruction is infeasible — for example because PHI resides in immutable backups or must be retained by law — the Business Associate will notify the Covered Entity in writing, explain why, extend the protections of this BAA to that PHI for as long as it is retained, and limit further uses and disclosures to the purposes that make return or destruction infeasible.

13. 13. Indemnification, Insurance, and Liability

The Business Associate will indemnify, defend, and hold harmless the Covered Entity from claims, penalties, fines, regulatory assessments, notification costs, credit monitoring costs, and reasonable attorney fees arising out of the Business Associate's or its Subcontractors' breach of this BAA or violation of HIPAA. The Business Associate will maintain, throughout the term and for [TAIL COVERAGE PERIOD, e.g., two years] afterward, cyber liability and privacy insurance of at least [CYBER COVERAGE LIMIT, e.g., $2,000,000 per claim] covering breach response, notification, regulatory defense, and third-party claims, and will name the Covered Entity as an additional insured or provide evidence of coverage on request. Any limitation of liability in the Services Agreement does not apply to the obligations in this Section or to a Breach caused by the Business Associate.

14. 14. Interpretation, Amendment, and General Provisions

This BAA will be interpreted to permit compliance with HIPAA, and any ambiguity will be resolved in favor of a meaning that complies. The Parties will negotiate in good faith to amend this BAA as necessary to comply with any amendment to HIPAA or to guidance issued by the Secretary, and if agreement is not reached within [AMENDMENT NEGOTIATION PERIOD, e.g., 30 days], either Party may terminate on written notice. This BAA is governed by federal law and, to the extent not preempted, by the laws of the State of [GOVERNING STATE], and state health privacy laws that are more stringent than HIPAA continue to apply. There are no third-party beneficiaries. Neither Party may assign this BAA without written consent, and if any provision is unenforceable the remainder stays in effect.

15. 15. Signatures

By signing below, each Party confirms that it has read this BAA, understands the obligations it creates under HIPAA, and agrees to be bound as of the Effective Date. COVERED ENTITY: [COVERED ENTITY NAME]. Signature: _____. Printed Name: [SIGNER NAME]. Title: [TITLE]. Date: [DATE]. Privacy Officer contact: [PRIVACY OFFICER NAME AND EMAIL]. BUSINESS ASSOCIATE: [BUSINESS ASSOCIATE NAME]. Signature: _____. Printed Name: [SIGNER NAME]. Title: [TITLE]. Date: [DATE]. Security Officer contact: [SECURITY OFFICER NAME AND EMAIL]. This BAA may be signed in counterparts, and electronic signatures have the same effect as originals.

16. Disclaimer

This template is provided for general informational purposes only and is not legal advice, and it is not a substitute for a compliance program. HIPAA requirements are detailed and change over time, state health privacy laws may impose more stringent obligations that are not preempted, and additional rules apply to substance use disorder records under 42 C.F.R. Part 2, to genetic information, and to certain behavioral health data. A signed BAA does not by itself make either party compliant: risk analyses, policies, training, and technical safeguards do. Consult a licensed attorney with healthcare privacy experience and, where appropriate, a qualified security assessor before relying on this document. Use of this template does not create an attorney-client relationship with ScanContract.