

[PRACTICE NAME]

[Address] · [Phone] · [Privacy contact email]

Business Associate Agreement

This Agreement is made between **PRACTICE NAME** (the "Covered Entity") and **VENDOR NAME** (the "Business Associate"), effective **DATE**. It applies to protected health information ("PHI") that the Business Associate creates, receives, maintains or transmits for the Covered Entity under **NAME OF SERVICE AGREEMENT** (the "Services Agreement"). Terms used here have the meanings given in 45 CFR Parts 160 and 164.

1 Definitions and scope

45 CFR 164.504(e)(2)(i)

1. "Breach", "Security Incident", "Subcontractor", "Unsecured PHI" and other capitalized terms have the meanings in 45 CFR 160.103, 164.304, 164.402 and 164.501.
2. This Agreement covers all PHI the Business Associate creates, receives, maintains or transmits for the Covered Entity, in any form.

2 Permitted uses and disclosures

45 CFR 164.504(e)(2)(i), (e)(4)

1. The Business Associate may use and disclose PHI only to perform the services described in the Services Agreement: **DESCRIBE THE SERVICES**.
2. The Business Associate will use, disclose and request only the minimum PHI necessary for those services.
3. **Optional — delete if you do not grant this permission:** The Business Associate may use and disclose PHI for its proper management and administration or to carry out its legal responsibilities, provided that any disclosure for these purposes is required by law, or the Business Associate obtains reasonable assurances that the recipient will keep the PHI confidential, use or disclose it only as required by law or for the purpose for which it was disclosed, and notify the Business Associate of any breach of confidentiality.
4. The Business Associate may not use or disclose PHI in any way that would violate the Privacy Rule if done by the Covered Entity, **except as allowed in paragraph 3**, or to **provide data aggregation services relating to the Covered Entity's health care operations — delete if not needed**.

3 Obligations of the Business Associate

45 CFR 164.504(e)(2)(ii)(A)–(D); 164.314(a)(2)(i)

The Business Associate will:

1. Not use or further disclose PHI other than as this Agreement permits or requires or as required by law.
2. Use appropriate safeguards, and comply with 45 CFR Part 164, Subpart C (the Security Rule) for electronic PHI, to prevent use or disclosure other than as this Agreement provides.
3. Ensure that any Subcontractor that creates, receives, maintains or transmits PHI on its behalf agrees in writing to the same restrictions, conditions and requirements that apply to the Business Associate.

4 Reporting

45 CFR 164.504(e)(2)(ii)(C); 164.314(a)(2)(i)(C); 164.410

1. The Business Associate will report to the Covered Entity any use or disclosure of PHI not provided for by this Agreement, and any Security Incident, of which it becomes aware, including Breaches of Unsecured PHI as 45 CFR 164.410 requires.
2. The Business Associate will report a Breach of Unsecured PHI without unreasonable delay and no later than **10** business days after discovery, with the identity of each affected individual as far as it can be determined and the other information the Covered Entity needs to notify them.
3. **Optional — unsuccessful attempts:** the Parties agree that this paragraph is notice of routine unsuccessful Security Incidents, such as pings, port scans and blocked sign-in attempts that do not result in unauthorized access, use, disclosure, modification or destruction of PHI or interference with system operations, and that no further report of them is required. The Business Associate will still report unusual or significant patterns of such attempts, and any attempt that escalates, exploits a weakness or compromises a system.

5 Individuals' rights and HHS

45 CFR 164.504(e)(2)(ii)(E)–(I)

The Business Associate will, within **10** business days of a request:

1. Make PHI in a designated record set available to the Covered Entity so it can meet an individual's right of access under 45 CFR 164.524.
2. Make PHI available for amendment and incorporate amendments under 45 CFR 164.526.
3. Make available the information needed to provide an accounting of disclosures under 45 CFR 164.528.

And it will also:

4. Comply with the Privacy Rule requirements that apply to the Covered Entity when carrying out any of the Covered Entity's obligations under that Rule.
5. Make its internal practices, books and records relating to PHI available to the Secretary of HHS for determining compliance.

6 Term and termination

45 CFR 164.504(e)(2)(ii)(J), (e)(2)(iii)

1. This Agreement lasts as long as the Business Associate holds PHI for the Covered Entity.
2. The Covered Entity may terminate this Agreement and the Services Agreement if it determines that the Business Associate has violated a material term of this Agreement.
3. When this Agreement ends, the Business Associate will, if feasible, return or destroy all PHI it still holds in any form and keep no copies. If that is not feasible, it will extend the protections of this Agreement to that PHI and limit further uses and disclosures to the purposes that make return or destruction infeasible.

7 Signatures

COVERED ENTITY

Name of practice

PRACTICE NAME

Signed by (name and title)

Signature

Date

BUSINESS ASSOCIATE

Name of company

VENDOR NAME

Signed by (name and title)

Signature

Date