

HIPAA Business Associate Agreement

An agreement for a business associate that handles protected health information for a covered entity. Template v1.0.

Effective date: _____

Covered entity: _____

Business associate: _____

The covered entity named above (the Covered Entity) uses the business associate named above (the Business Associate) for services that involve protected health information. This agreement sets out how that information is protected.

1. Definitions

HIPAA Rules means the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164. Terms such as Breach, Designated Record Set, Protected Health Information (PHI), Security Incident, Subcontractor and Unsecured PHI have the meanings the HIPAA Rules give them. In this agreement PHI means PHI that the Business Associate creates, receives, keeps or sends for the Covered Entity.

2. Services

Services that involve PHI:

3. Permitted uses and disclosures

The Business Associate uses and discloses PHI only to perform the services above, as this agreement allows or as the law requires. It does not use or disclose PHI in a way that would break the HIPAA Rules if the Covered Entity did it. It may also use PHI for its own proper management and administration and to meet its legal duties. It may disclose PHI for those purposes only if the law requires it or the recipient gives written assurance that it will keep the PHI confidential and report any breach of that duty.

The Business Associate uses, discloses and asks for only the minimum PHI necessary for each purpose, as the HIPAA Rules require. It does not sell PHI or use it for marketing unless the HIPAA Rules allow it.

4. Safeguards

The Business Associate uses appropriate safeguards to prevent any use or disclosure of PHI that this agreement does not allow. For electronic PHI it complies with the Security Rule, including its administrative, physical and technical safeguards and its policy and documentation requirements.

5. Reporting

The Business Associate reports to the Covered Entity any use or disclosure of PHI that this agreement does not allow, and any Security Incident, promptly after it becomes aware of it. Unsuccessful attempts, such as pings and port scans that do not lead to access, need no separate report, and this sentence is notice of them.

Breach report deadline after discovery: _____

The Business Associate reports any Breach of Unsecured PHI to the Covered Entity without unreasonable delay and within the time above after discovering it, and never later than the HIPAA Rules allow. The report names each affected individual where known and gives the other information the Covered Entity needs to give notice. The Business Associate takes reasonable steps to limit any harmful effect it knows of.

6. Subcontractors

The Business Associate makes sure that any Subcontractor that creates, receives, keeps or sends PHI for it agrees in writing to the same restrictions, conditions and requirements that apply to the Business Associate under this agreement.

7. Rights of individuals

In time for the Covered Entity to meet its duties under the HIPAA Rules, the Business Associate:

- (a) makes PHI in a Designated Record Set available so individuals can access it
- (b) makes any amendment to PHI in a Designated Record Set that the Covered Entity directs or agrees to
- (c) keeps and provides the information needed for an accounting of disclosures

If an individual makes such a request to the Business Associate directly, it passes the request to the Covered Entity promptly.

8. Carrying out the Covered Entity's obligations

If the Business Associate carries out an obligation of the Covered Entity under the Privacy Rule, it complies with the requirements of the Privacy Rule that apply to the Covered Entity for that obligation.

9. Duties of the Covered Entity

The Covered Entity tells the Business Associate about any limit in its notice of privacy practices, any change in or withdrawal of an individual's permission and any restriction it agrees to, where these affect the Business Associate's use or disclosure of PHI. It does not ask the Business Associate to use or disclose PHI in a way the HIPAA Rules would not allow the Covered Entity to.

10. Books and records

The Business Associate makes its internal practices, books and records about PHI available to the Secretary of the US Department of Health and Human Services for the purpose of finding out whether the parties comply with the HIPAA Rules.

11. Term and termination

This agreement starts on the effective date and lasts until all PHI has been returned or destroyed under section 12. If either party learns that the other has materially breached this agreement, it gives written notice. If the breach is not cured within 30 days of the notice, the party that gave notice may end this agreement and the services that involve PHI. If a cure is not possible, it may end them at once.

12. Return or destruction of PHI

When the services end, the Business Associate returns to the Covered Entity or destroys all PHI, including PHI held by its Subcontractors, and keeps no copies. If return or destruction is not feasible,

the Business Associate tells the Covered Entity why, extends the protections of this agreement to that PHI and limits further use and disclosure to the purposes that make return or destruction not feasible, for as long as it keeps the PHI.

13. Interpretation and general

Any unclear term is read in the way that best allows the parties to comply with the HIPAA Rules. A reference to the HIPAA Rules means them as amended and in force. If they change, the parties will amend this agreement as needed. If this agreement conflicts with another agreement between the parties about PHI, this agreement controls. There are no third party beneficiaries. A change is valid only in writing signed by both parties.

Apart from the HIPAA Rules, this agreement is governed by the laws of:

The Business Associate names its privacy contact for notices under this agreement.

Privacy contact name and email: _____

Business associate

Covered entity

Signature

Signature

Name

Name

Date

Date

Title

Title