Business Associate Agreement

HIPAA Business Associate Agreement for HCBS MedPass customers

Reedstem, LLC · Aurora, Colorado, United States · hcbsmed.com
Last updated October 25, 2026 · Version 1.0

Contents

1. Purpose
2. Definitions
3. Obligations of Business Associate
4. Permitted Uses and Disclosures by Business Associate
5. Obligations of Covered Entity
6. Term and Termination
7. Miscellaneous
8. Contact for Privacy and Security Matters

This Business Associate Agreement (the "BAA") is entered into between the organization that subscribes to HCBS MedPass ("Covered Entity," which, if the organization is itself a business associate of a covered entity, means that organization in its capacity as a business associate) and **Reedstem, LLC**, Aurora, Colorado ("Business Associate"). It forms part of the HCBS MedPass Terms of Service (the "Terms") and takes effect when the Covered Entity accepts the Terms.

1. Purpose

Business Associate provides the HCBS MedPass service (the "Services") to Covered Entity, which involves creating, receiving, maintaining, or transmitting Protected Health Information on Covered Entity's behalf.

The parties enter into this BAA to comply with the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations at 45 C.F.R. Parts 160 and 164, as amended from time to time (together, "HIPAA"), including the Privacy Rule, the Security Rule, and the Breach Notification Rule.

2. Definitions

Capitalized terms used but not defined in this BAA have the meanings given in HIPAA. These include Breach, Data Aggregation, Designated Record Set, Disclose, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Protected Health Information" or "PHI" means protected health information, as defined at 45 C.F.R. § 160.103, that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

3. Obligations of Business Associate

3.1 Use and disclosure

Business Associate will not Use or Disclose PHI other than as permitted or required by this BAA or as Required by Law.

3.2 Safeguards

Business Associate will use appropriate administrative, physical, and technical safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent Use or Disclosure of PHI other than as this BAA provides.

3.3 Reporting

Business Associate will report to Covered Entity any Use or Disclosure of PHI not provided for by this BAA of which it becomes aware. This includes Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410 and Security Incidents of which it becomes aware.

Business Associate will report a Breach of Unsecured PHI without unreasonable delay and in no case later than **ten (10) business days** after discovery. The report will include, to the extent known:

- the identification of each Individual affected;
- a description of what happened, including the dates of the Breach and its discovery;
- the types of PHI involved;
- steps Individuals should take to protect themselves;
- what Business Associate is doing to investigate, mitigate, and prevent recurrence;
- any other information Covered Entity reasonably needs to meet its notification obligations.

Business Associate will supplement the report as more information becomes available.

3.4 Unsuccessful Security Incidents

The parties agree that this Section is notice by Business Associate of the ongoing existence and occurrence of unsuccessful Security Incidents, for which no further notice is required. Unsuccessful Security Incidents are attempts that do not result in unauthorized access, Use, Disclosure, modification, or destruction of PHI, or interference with system operations. Examples include pings, port scans, blocked sign-in attempts, and denial-of-service attempts that do not succeed.

3.5 Mitigation

Business Associate will mitigate, to the extent practicable, any harmful effect known to it of a Use or Disclosure of PHI in violation of this BAA.

3.6 Subcontractors

In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate will 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 Business Associate, including implementing reasonable and appropriate safeguards. Business Associate's Subcontractors include its cloud hosting and database providers.

3.7 Access

To the extent Business Associate maintains PHI in a Designated Record Set, it will make the PHI available to Covered Entity, or as Covered Entity directs to an Individual, within ten (10) business days after Covered Entity's request, as necessary for Covered Entity to meet 45 C.F.R. § 164.524. This includes access in electronic form. The Services' export and reporting features may be used for this purpose.

3.8 Amendment

Business Associate will make amendments to PHI in a Designated Record Set as Covered Entity directs or agrees to under 45 C.F.R. § 164.526, or will provide Covered Entity the means to do so in the Services, within ten (10) business days after the request.

3.9 Accounting of disclosures

Business Associate will maintain and, within ten (10) business days after request, provide to Covered Entity the information required for Covered Entity to respond to a request for an accounting of disclosures under 45 C.F.R. § 164.528.

3.10 Individuals' requests

If an Individual contacts Business Associate directly with a request regarding PHI, Business Associate will forward the request to Covered Entity within five (5) business days and will not respond except as Covered Entity directs or as Required by Law.

3.11 Covered Entity's obligations

To the extent Business Associate carries out an obligation of Covered Entity under Subpart E of 45 C.F.R. Part 164, it will comply with the requirements of Subpart E that apply to Covered Entity in performing that obligation.

3.12 Books and records

Business Associate will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining compliance with HIPAA.

3.13 Minimum necessary

Business Associate will request, Use, and Disclose only the Minimum Necessary PHI to accomplish the intended purpose.

3.14 No sale or marketing

Business Associate will not sell PHI or Use or Disclose PHI for marketing, except as HIPAA permits with any required authorization.

3.15 Location

Business Associate will store and process PHI only in the United States.

4. Permitted Uses and Disclosures by Business Associate

4.1 Services

Business Associate may Use or Disclose PHI as necessary to provide the Services under the Terms, including hosting, backup, support, security, maintenance, and the features Covered Entity enables, such as reports, exports, and pharmacy connections.

4.2 De-identification

Business Associate may de-identify PHI in accordance with 45 C.F.R. § 164.514(a) through (c) and may use de-identified information for any lawful purpose. It will not attempt to re-identify it.

4.3 Management and administration

Business Associate may Use PHI for its proper management and administration or to carry out its legal responsibilities. It may Disclose PHI for those purposes if the Disclosure is Required by Law. It may also Disclose PHI for those purposes if it obtains reasonable written assurances from the recipient that:

- the PHI will be held confidentially;
- the PHI will be Used or further Disclosed only as Required by Law or for the purpose for which it was disclosed;
- the recipient will notify Business Associate of any instance of which it is aware in which the confidentiality of the PHI has been breached.

4.4 Data Aggregation

Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations, only if Covered Entity requests them.

4.5 Reporting violations

Business Associate may Use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

4.6 Limits

Business Associate will not Use or Disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the purposes in Sections 4.3 and 4.4.

5. Obligations of Covered Entity

Covered Entity will:

- notify Business Associate of any limitation in its Notice of Privacy Practices, to the extent it may affect Business Associate's Use or Disclosure of PHI;
- notify Business Associate of any change in, or revocation of, an Individual's permission to Use or Disclose PHI, to the extent it may affect Business Associate;
- notify Business Associate of any restriction on the Use or Disclosure of PHI that Covered Entity has agreed to under 45 C.F.R. § 164.522, to the extent it may affect Business Associate;
- not request that Business Associate Use or Disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity;
- configure User access in the Services consistent with the Minimum Necessary standard, and promptly remove access for Users who no longer need it;
- obtain any consents or authorizations required by HIPAA or more stringent state law before entering PHI into the Services;
- notify Business Associate in writing before entering records subject to 42 C.F.R. Part 2 (substance use disorder treatment records). The parties will then agree any terms Part 2 requires, such as qualified service organization terms, and Business Associate agrees to be bound by Part 2 for such records to the extent it applies.

6. Term and Termination

6.1 Term

This BAA remains in effect for as long as the Terms are in effect and thereafter until all PHI is returned or destroyed under Section 6.3.

6.2 Termination for cause

If either party determines that the other has violated a material term of this BAA, it may give written notice and an opportunity to cure within thirty (30) days. If the violation is not cured, the non-breaching party may terminate this BAA and the affected Services. If cure is not possible, the non-breaching party may terminate immediately.

6.3 Return or destruction

On termination, Business Associate will return to Covered Entity, or at Covered Entity's direction destroy, all PHI that it or its Subcontractors maintain in any form, and will retain no copies. Covered Entity may obtain a return in the form of an export during the sixty (60) day period after the subscription ends. After that period, or sooner on Covered Entity's written request, Business Associate will destroy the PHI.

PHI in encrypted backups will be destroyed as those backups are overwritten in the ordinary course, generally within approximately thirty (30) days. Until then, it remains protected by this BAA.

If return or destruction is infeasible, Business Associate will notify Covered Entity of the conditions that make it infeasible. It will extend the protections of this BAA to that PHI and limit further Uses and Disclosures to the purposes that make return or destruction infeasible, for as long as it maintains the PHI.

6.4 Survival

Business Associate's obligations under Section 6.3 survive termination.

7. Miscellaneous

- **Regulatory references.** A reference to a section of HIPAA means that section as in effect or as amended.
- **Amendment.** The parties will take action to amend this BAA as necessary for compliance with changes to HIPAA or other Applicable Law, including any revisions to the Security Rule. Business Associate may update this BAA to reflect such changes on notice to Covered Entity.
- **More stringent state law.** Where state law relating to the privacy or security of health information is more stringent than HIPAA and applies to a party, that party will comply with it.
- **Interpretation.** Any ambiguity will be resolved to permit compliance with HIPAA. This BAA controls over any conflicting term of the Terms with respect to PHI.
- **Liability.** Liability under this BAA is subject to the limitations of liability in the Terms, including the increased limit stated there for Breaches of Unsecured PHI, except where Applicable Law does not permit limitation.
- **No third-party beneficiaries.** Nothing in this BAA confers rights on any person other than the parties and their respective successors and permitted assigns.
- **Independent contractor.** Business Associate is an independent contractor and not an agent of Covered Entity.
- **Governing law.** This BAA is governed by federal law and, to the extent not preempted, the laws of the State of Colorado.

8. Contact for Privacy and Security Matters

Reedstem, LLC · HCBS MedPass · Aurora, Colorado, United States (mailing address at hcbsmed.com) · support@hcbsmed.com (subject: "HIPAA Notice")

This BAA is provided as a professionally drafted template based on the HHS sample business associate agreement provisions. It should be reviewed by counsel before use.