

BUSINESS ASSOCIATE AGREEMENT

HIPAA Privacy, Security, and Breach Notification Addendum

PRODUCTION VERSION 2026-08-12.2 - ELECTRONIC ACCEPTANCE

Effective Date: The date and time recorded in the electronic acceptance record

Customer: The legal organization identified in the electronic acceptance record

Business Associate: OT Bestie LLC

Related Agreement: The School OT Terms of Use version identified in the electronic acceptance record

This Business Associate Agreement ("Agreement") is entered into as of the Effective Date by and between Customer and OT Bestie LLC ("OT Bestie"). OT Bestie is a Business Associate or subcontractor Business Associate to the extent it creates, receives, maintains, or transmits Protected Health Information on Customer's behalf.

This Agreement supplements the Related Agreement. If the documents conflict regarding Protected Health Information, this Agreement controls. The parties intend this Agreement to satisfy the applicable business-associate contract requirements of the HIPAA Rules.

1. Purpose, Scope, and Relationship

1.1 Purpose. This Agreement states the safeguards, permitted uses and disclosures, reporting duties, individual-rights assistance, subcontractor requirements, and termination obligations that apply when OT Bestie handles Protected Health Information for Customer.

1.2 Scope. This Agreement applies only to Protected Health Information that OT Bestie creates, receives, maintains, or transmits on Customer's behalf in performing the services in the Related Agreement and Exhibit A.

1.3 Customer Status. Customer may be a Covered Entity or a Business Associate acting for an upstream Covered Entity. Customer is responsible for determining that status and for identifying any upstream restrictions that apply to OT Bestie's work.

1.4 FERPA Records. Education records excluded from the HIPAA definition of Protected Health Information because they are protected by FERPA are outside this Agreement and remain governed by the education-record terms in the Related Agreement, unless the parties expressly agree otherwise in writing.

2. Definitions

2.1 Defined HIPAA Terms. Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use have the meanings assigned in the HIPAA Rules.

2.2 Business Associate. Business Associate has the meaning in 45 C.F.R. section 160.103 and, when referring to a party to this Agreement, means OT Bestie LLC.

2.3 Customer. Customer means the organization identified in the electronic acceptance record. When Customer is a Business Associate, references to a Covered Entity include Customer's upstream Covered Entity to the extent needed to satisfy Customer's lawful obligations.

2.4 HIPAA Rules. HIPAA Rules means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended.

3. Permitted and Required Uses and Disclosures

3.1 Service Delivery. OT Bestie may Use or Disclose Protected Health Information only as necessary to perform the services in the Related Agreement and Exhibit A, to follow Customer's documented lawful instructions, or as Required by Law.

3.2 Minimum Necessary. OT Bestie will limit its Uses, Disclosures, and requests for Protected Health Information to the Minimum Necessary to accomplish the intended purpose and will follow Customer's communicated minimum-necessary policies to the extent applicable to the services. This provision does not apply where the HIPAA Rules exclude a Use, Disclosure, or request from the Minimum Necessary standard.

3.3 Management and Administration. OT Bestie may Use Protected Health Information for its proper management and administration or to carry out its legal responsibilities. OT Bestie may Disclose Protected Health Information for those purposes only when the Disclosure is Required by Law or OT Bestie obtains reasonable written assurances that the recipient will keep the

information confidential, use or further disclose it only for the stated purpose or as Required by Law, and notify OT Bestie of any known confidentiality breach.

3.4 Required by Law. When a law, court order, subpoena, or other legal process requires a Disclosure, OT Bestie will limit the Disclosure to what is legally required and, when legally permitted, notify Customer sufficiently in advance to allow Customer to seek protection.

3.5 Prohibited Uses. OT Bestie will not Use or Disclose Protected Health Information in a manner that would violate the HIPAA Rules if done by Customer, except for the limited management and administration activities expressly permitted above. OT Bestie will not sell Protected Health Information or use it for marketing, targeted advertising, or development, training, or evaluation of products unrelated to Customer's contracted services.

4. Safeguards and Compliance

4.1 Safeguards. OT Bestie will use appropriate administrative, physical, and technical safeguards to prevent any Use or Disclosure of Protected Health Information other than as permitted by this Agreement and to protect the confidentiality, integrity, and availability of Electronic Protected Health Information.

4.2 Security Rule. OT Bestie will comply with the applicable requirements of 45 C.F.R. Part 164, Subpart C, with respect to Electronic Protected Health Information, including security management, assigned responsibility, workforce access, information-system activity review, incident procedures, contingency planning, business-associate arrangements, access control, integrity, authentication, transmission security, and periodic evaluation.

4.3 Workforce. OT Bestie will authorize workforce access only as needed for assigned duties, require confidentiality, provide applicable privacy and security training, and apply appropriate sanctions for material violations.

4.4 Mitigation. OT Bestie will mitigate, to the extent practicable, harmful effects known to OT Bestie resulting from a Use or Disclosure of Protected Health Information in violation of this Agreement.

4.5 Customer Functions. To the extent OT Bestie performs an obligation of Customer under 45 C.F.R. Part 164, Subpart E, OT Bestie will comply with the requirements that apply to Customer in performing that obligation.

5. Security Incidents and Breach Notification

5.1 Reportable Events. OT Bestie will report to Customer any Use or Disclosure of Protected Health Information not permitted by this Agreement, any Breach of Unsecured Protected Health Information, and any Security Incident of which OT Bestie becomes aware, subject to the standing notice for routine unsuccessful events in Section 5.6.

5.2 Timing. OT Bestie will provide initial notice without unreasonable delay and no later than ten (10) business days after discovery. OT Bestie will provide supplemental information promptly as it becomes available. Nothing in this section extends the maximum period permitted by 45 C.F.R. section 164.410.

5.3 Notice Content. To the extent known, the notice will identify the nature and date of the event; the date of discovery; the affected individuals; the types of Protected Health Information involved; corrective and mitigating actions taken or planned; and a contact for follow-up. OT Bestie will provide other available information Customer reasonably needs to meet applicable notification duties.

5.4 Investigation and Cooperation. OT Bestie will take reasonable steps to contain and investigate the event, preserve relevant evidence, mitigate harmful effects, correct identified control failures, and cooperate with Customer's legally required risk assessment and response.

5.5 External Notification. Unless Required by Law or separately agreed in writing, Customer controls determinations and notifications to Individuals, the Secretary, regulators, or the media. OT Bestie will not notify an Individual on Customer's behalf without Customer's instruction unless law independently requires OT Bestie to do so.

5.6 Routine Unsuccessful Events. The parties acknowledge that unsuccessful login attempts, network probes, pings, port scans, denial-of-service attempts, and similar events occur routinely. This Agreement constitutes standing notice of those events only when they do not result in unauthorized access to, acquisition, use, disclosure, modification, or destruction of Protected Health Information or material interference with system operations.

6. Subcontractors

6.1 Required Agreements. Before allowing a Subcontractor to create, receive, maintain, or transmit Protected Health Information on OT Bestie's behalf, OT Bestie will enter a written agreement requiring the Subcontractor to comply with the same applicable restrictions, conditions, and safeguards imposed on OT Bestie by this Agreement and the HIPAA Rules.

6.2 Responsibility. OT Bestie remains responsible for its Subcontractors to the extent provided by the HIPAA Rules and the Related Agreement. OT Bestie will limit Subcontractor access to the function performed and will maintain an appropriate current record of Subcontractors that handle Protected Health Information.

6.3 Material Violations. If OT Bestie knows of a pattern of activity or practice by a Subcontractor that constitutes a material breach, OT Bestie will take reasonable steps to cure the breach or end the violation and, if those steps are unsuccessful, terminate the arrangement if feasible.

7. Individual Rights and Regulatory Cooperation

7.1 Access. Within ten (10) business days after Customer's request, OT Bestie will make Protected Health Information in a Designated Record Set available to Customer in the form and format reasonably requested, to the extent needed for Customer to satisfy 45 C.F.R. section 164.524. OT Bestie will forward a request received directly from an Individual to Customer and will not respond directly unless Customer instructs it to do so or law requires otherwise.

7.2 Amendment. Within ten (10) business days after Customer's request, OT Bestie will make Protected Health Information available for amendment and incorporate amendments as directed or agreed by Customer, to the extent needed for compliance with 45 C.F.R. section 164.526.

7.3 Accounting. OT Bestie will document and make available information concerning Disclosures of Protected Health Information as needed for Customer to provide an accounting under 45 C.F.R. section 164.528. OT Bestie will provide available requested information within ten (10) business days.

7.4 Secretary Access. OT Bestie will make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information available to the Secretary for purposes of determining compliance with the HIPAA Rules.

8. Customer Obligations

8.1 Lawful Instructions. Customer will not request or direct OT Bestie to Use or Disclose Protected Health Information in a manner that would violate the HIPAA Rules if done by Customer, except where the HIPAA Rules permit a Business Associate to do so.

8.2 Privacy Practices and Restrictions. Customer will notify OT Bestie of any limitation in Customer's Notice of Privacy Practices, change or revocation of an Individual's permission, or restriction under 45 C.F.R. section 164.522 that affects OT Bestie's permitted Uses or Disclosures.

8.3 Authorization and Minimum Data. Customer is responsible for the legal basis for each disclosure to OT Bestie, for providing only the Protected Health Information reasonably necessary for the services, and for notifying OT Bestie when that authority changes.

8.4 Users and Systems. Customer is responsible for authorizing its users, assigning appropriate roles, safeguarding credentials and devices, promptly removing access, reviewing exports and downstream disclosures, and protecting Protected Health Information after it leaves OT Bestie's controlled Service at Customer's direction.

8.5 Incident Cooperation. Customer will promptly notify OT Bestie of suspected unauthorized account or record access, provide information reasonably needed for containment, and avoid instructions that would compromise evidence or violate law.

9. Term, Noncompliance, and Termination

9.1 Term. This Agreement begins on the Effective Date and continues while OT Bestie creates, receives, maintains, or transmits Protected Health Information on Customer's behalf, unless terminated earlier under this Agreement.

9.2 Termination for Cause. Customer may terminate this Agreement and the affected services if Customer determines that OT Bestie violated a material term and OT Bestie does not cure the violation within ten (10) business days after written notice. Customer may terminate immediately when cure is not possible or delay would create a material risk to Protected Health Information.

9.3 Customer Noncompliance. If OT Bestie knows of a material Customer pattern or practice that would cause OT Bestie to violate this Agreement or the HIPAA Rules, OT Bestie may suspend affected processing while the parties seek a lawful resolution. OT Bestie will take reasonable steps to cure the breach or end the violation and, if unsuccessful, terminate the affected arrangement if feasible. If termination is not feasible and the HIPAA Rules require it, OT Bestie will report the problem to the Secretary.

10. Return or Destruction

10.1 Customer Election. Upon termination, OT Bestie will, at Customer's written election and if feasible, return Protected Health Information to Customer or securely destroy it, including Protected Health Information held by Subcontractors. OT Bestie will retain no copies after an agreed export and the applicable destruction process are complete.

10.2 Infeasibility or Required Retention. If return or destruction is infeasible or retention is Required by Law, OT Bestie will notify Customer, retain only the Protected Health Information that cannot lawfully or feasibly be returned or destroyed, continue this Agreement's protections, and limit further Uses and Disclosures to the purpose that makes return or destruction infeasible.

10.3 Backups. Protected Health Information remaining in secured backup media will not be restored except for legitimate recovery, legal preservation, or security validation and will be destroyed through the normal protected backup lifecycle. Any restored information remains subject to this Agreement.

10.4 Survival. OT Bestie's obligations under this section survive termination for as long as OT Bestie retains Protected Health Information.

11. Documentation, Audit Evidence, and Records

11.1 Documentation. Each party will maintain the documentation the HIPAA Rules require for the period required by those Rules. OT Bestie will preserve this Agreement, applicable policies, required assessments, training or workforce evidence, incident records, and agreement evidence for at least six years from creation or the date last in effect, whichever is later, unless a longer period applies.

11.2 Acceptance Evidence. The authenticated acceptance record, including Customer identity, signer identity and title, account, acceptance time, document version, exact SHA-256 hash, and evidence digest, is incorporated into this Agreement and may be retained and reproduced to establish execution and scope.

11.3 Security Information. Customer may request reasonable information needed for its vendor-risk review. OT Bestie may protect confidential security architecture, credentials, vulnerability details, other customers' information, and information that disclosure would make less secure, and may provide summaries or independent evidence instead of unrestricted system access.

12. General Terms

12.1 Regulatory References. A reference to the HIPAA Rules means the cited provision as in effect or as amended. The parties will take reasonably necessary action to amend this Agreement for changes in applicable law.

12.2 Interpretation. Any ambiguity will be interpreted to permit compliance with the HIPAA Rules. Nothing authorizes a Use or Disclosure prohibited by applicable law.

12.3 Order of Control. This Agreement controls over the Related Agreement regarding Protected Health Information. The Claims Processing Addendum controls the claim-service details and amends Exhibit A only as it expressly states. The Related Agreement's limitation of liability, indemnity, dispute, notice, assignment, and other general terms apply unless they conflict with the HIPAA Rules or an express provision of this Agreement.

12.4 No Third-Party Beneficiaries. This Agreement benefits only the parties and their permitted successors and assigns and creates no third-party beneficiary rights.

12.5 Entire BAA; Counterparts. This Agreement is the complete agreement between the parties concerning OT Bestie's handling of Protected Health Information and supersedes prior discussions on that subject. It may be executed in counterparts and by electronic signature, each deemed an original.

12.6 Notices. Notices under this Agreement must be sent to the contacts below and are effective when received. Security and Breach notices must also be sent by email to the designated privacy or security contact.

13. Electronic Signatures and Notice Contacts

OT Bestie executes this Agreement by publishing this production version for authenticated electronic acceptance. Customer executes it when its authorized representative accepts it in The School OT. The electronic acceptance evidence described in Section 11.2 is the parties' signature record.

CUSTOMER	BUSINESS ASSOCIATE
Organization: See electronic acceptance record	Organization: OT Bestie LLC
Authorized signer: See electronic acceptance record	Electronic signature: Publication of Version 2026-08-12.2
Title and date: See electronic acceptance record	Date: August 12, 2026
Notice: Workspace-owner email in the acceptance record	Privacy and security: contact@theschoolot.com

Exhibit A - Services and PHI Scope

A.1 Services. OT Bestie provides the caseload, service-plan, due-date, scheduling, service-documentation, progress-reporting, clinical-supervision, report, export, account-security, and support functions Customer selects under the Related Agreement. Claim services are included only when Customer separately accepts the current Claims Processing Addendum and the feature is enabled.

A.2 Permitted Purpose. OT Bestie may process Protected Health Information only to provide, secure, support, maintain, recover, and document the contracted services; respond to Customer-authorized requests; comply with law; and perform this Agreement.

A.3 Anticipated Data Categories. Depending on Customer's use, Protected Health Information may include identifiers and limited demographics; contact and coverage information; service plans, goals, frequencies, deadlines, accommodations, and clinical requirements; schedules, attendance, therapy documentation, observations, consultations, and credited minutes; progress measurements, reports, review decisions, corrections, and audit history; clinician assignments, supervision, authorized-user and access information; and, only under the Claims Processing Addendum, billing, provider, payer, diagnosis, authorization, claim, status, and remittance information.

A.4 Subcontractor Functions. Approved Subcontractors may provide contracted hosting, database, network, backup, security, and recovery functions. A clearinghouse and payer network may process claim information only when the Claims Processing Addendum applies. Account email and consumer payment channels are outside the Protected Health Information flow unless separately approved in writing.

A.5 Excluded Uses. OT Bestie is not authorized to use Customer's Protected Health Information for advertising, marketing, sale, targeted advertising, unrelated analytics, or development, training, or evaluation of products unrelated to Customer's contracted services.

A.6 Customer-Specific Limits. None unless the parties identify additional limits in a separately executed writing. Customer must communicate any applicable Notice of Privacy Practices limitation, authorization change, or agreed restriction before it expects OT Bestie to apply that limit.