

BUSINESS ASSOCIATE AGREEMENT

HIPAA Privacy, Security, and Breach Notification Addendum

PRODUCTION VERSION 2026-08-11 - 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 the Customer identified above ("Customer") and OT Bestie LLC ("OT Bestie"). Customer may be a Covered Entity or a Business Associate acting for a Covered Entity. 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 parties' Related Agreement. If the documents conflict regarding Protected Health Information, this Agreement controls. FERPA education records that are excluded from the HIPAA definition of Protected Health Information are outside this Agreement unless the parties agree otherwise in writing.

1. Purpose and Scope

1.1 Purpose. This Agreement documents the safeguards, permitted uses and disclosures, reporting duties, individual-rights assistance, and termination obligations required 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 described in the Related Agreement and Exhibit A.

2. Definitions

2.1 HIPAA Terms. Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, 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 party identified above. If Customer is itself a Business Associate, references in this Agreement to a Covered Entity include Customer's upstream Covered Entity to the extent necessary to satisfy Customer's 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 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, as Customer directs in writing, 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.

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 if 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 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, advertising, or unrelated product purposes.

4. OT Bestie's Safeguard and Compliance Obligations

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.

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 risk analysis, risk management, access controls, information-system activity review, incident response, contingency planning, and periodic evaluation.

4.3 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.

4.4 Compliance with Customer Functions. To the extent OT Bestie performs any 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 Reporting. OT Bestie will notify Customer of any Use or Disclosure of Protected Health Information not permitted by this Agreement, any Breach of Unsecured Protected Health Information, and any Security Incident that results in unauthorized access to, acquisition, use, disclosure, modification, or destruction of Electronic Protected Health Information or material interference with system operations.

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 notification 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 individuals and 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 Notification Responsibility. Unless Required by Law or separately agreed in writing, Customer is responsible for determining and making notifications to Individuals, the Secretary, regulators, or the media. OT Bestie will reasonably cooperate with Customer's investigation, risk assessment, mitigation, and notification process.

5.5 Routine Unsuccessful Events. The parties acknowledge that unsuccessful login attempts, network probes, pings, port scans, denial-of-service attempts, and similar events may occur routinely. This Agreement constitutes notice of those unsuccessful events only when they do not result in unauthorized access, 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 into 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 Material Violations. If OT Bestie knows of a pattern of activity or practice by a Subcontractor that constitutes a material breach of the Subcontractor's obligations, 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 necessary for Customer to meet its obligations under 45 C.F.R. section 164.524. OT Bestie will forward any 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 necessary 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 necessary for Customer to provide an accounting under 45 C.F.R. section 164.528. OT Bestie will provide the requested information within ten (10) business days after Customer's request.

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 Authorized Access. Customer is responsible for authorizing its users, assigning appropriate roles, safeguarding user credentials, promptly removing access that is no longer appropriate, and providing OT Bestie only the Protected Health Information reasonably necessary for the services.

9. Term 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 applicable services if Customer determines that OT Bestie has 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 a delay would create a material risk to Protected Health Information.

9.3 OT Bestie Response to Customer Violation. If OT Bestie knows of a Customer practice that would cause OT Bestie to violate this Agreement or the HIPAA Rules, OT Bestie may suspend the affected processing while the parties seek a lawful resolution and may terminate the affected services if the violation cannot be cured.

10. Return or Destruction of Protected Health Information

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. OT Bestie will retain no copies after completing any agreed export and the applicable destruction process.

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 the protections of this Agreement, and limit further Uses and Disclosures to the purpose that makes return or destruction infeasible. Protected Health Information remaining in protected backup media will not be restored except for legitimate recovery purposes and will be destroyed through the normal secured backup lifecycle.

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

11. General Terms

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

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

11.3 Relationship to Related Agreement. Except as modified by this Agreement, the Related Agreement remains in effect. Its governing-law, limitation-of-liability, dispute-resolution, notice, assignment, and other general provisions apply to this Agreement unless they conflict with the HIPAA Rules or this Agreement's express terms concerning Protected Health Information.

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

11.5 Entire BAA; Counterparts. This Agreement is the complete agreement between the parties regarding 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 of which is deemed an original.

11.6 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.

12. Signatures

OT Bestie LLC executes this Agreement by publishing this production version for electronic acceptance. Customer executes it when its authenticated, authorized representative accepts it in The School OT. The resulting electronic acceptance record, including the Customer identity, signer identity and title, exact document hash, and Effective Date, is incorporated into and forms part of this Agreement.

CUSTOMER Organization: See electronic acceptance record Electronic signature: See electronic acceptance record Authorized representative: See electronic acceptance record Title: See electronic acceptance record Date: See electronic acceptance record	BUSINESS ASSOCIATE OT Bestie LLC Electronic signature: Publication of Version 2026-08-11 Name: OT Bestie LLC Title: Business Associate Date: August 11, 2026
---	--

Notice Contacts

Customer Notice contact: Workspace-owner email identified in the electronic acceptance record	OT Bestie LLC Privacy and security email: contact@theschoolot.com
---	--

Exhibit A - Services and PHI Scope

A.1 Services. OT Bestie provides the caseload, service-plan, due-date, scheduling, session-documentation, progress-reporting, and clinical-supervision functions selected by Customer under the Related Agreement.

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

A.3 Anticipated Data Categories. Depending on Customer's use, Protected Health Information may include:

- individual names, school or local identifiers, contact details, and limited demographic information;
- service plans, goals, service frequencies, deadlines, accommodations, and related clinical requirements;
- schedules, attendance, therapy-session documentation, observations, consultation records, and credited service minutes;
- progress measurements, progress reports, review decisions, corrections, and audit history; and
- clinician assignments, supervision relationships, authorized-user information, and access records linked to an Individual.

A.4 Excluded Uses. OT Bestie is not authorized to use Customer's Protected Health Information for advertising, marketing, sale, unrelated analytics, or development of products unrelated to Customer's contracted services.

A.5 Customer-Specific Limits. None, unless the parties state additional customer-specific terms in a separately executed writing.