

FAMILY ELDERCARE

[Draft] Business Associate Agreement

Per RFP Section 4, proposals should affirm willingness to execute a HIPAA Business Associate Agreement as a condition of award. Thus, Family Eldercare distributes this draft for review to all registered respondents; respondents should identify any proposed exceptions to this draft in their proposals (see [Consolidated Vendor Q&A](#) item 10.2). Bracketed text will be completed at execution. Respondents should not sign or return this form with their proposals.

This draft is subject to mutually agreeable revision between Family Eldercare and the selected respondent during contract negotiation.

This Business Associate Agreement (“Agreement”) is entered into as of [Effective Date] (the “Effective Date”) by and between Family Eldercare, Inc., 1700 Rutherford Lane, Austin, Texas 78754 (the “Organization”), and [Business Associate legal name], [entity type and state of organization], [address] (“Business Associate”). The Organization and Business Associate are each a “Party” and together the “Parties.”

Recitals

- A. The Organization provides services to older adults and adults with disabilities (the “Clients”) and applies the standards of the HIPAA Rules organization-wide to protected health information and other sensitive information it holds.
- B. The Parties are entering into an agreement for co-managed information technology services (the “Services Agreement”), under which Business Associate will perform services that involve receiving, maintaining, or transmitting Sensitive Information (as defined in Section 1.3) on the Organization’s behalf.
- C. The Parties intend this Agreement to satisfy the business associate contract requirements of 45 CFR [164.502\(e\)](#), [164.504\(e\)](#), [164.308\(b\)](#), and [164.314\(a\)](#). To the extent the Organization is not itself a covered entity with respect to any protected health information, Business Associate agrees to comply with this Agreement as though the Organization were a covered entity. To the extent the Organization acts as a business associate of another covered entity, the Business Associate is the Organization’s subcontractor within the meaning of 45 CFR [160.103](#).

1. Definitions

1.1 HIPAA Rules

The following terms used in this Agreement have the same meaning as those terms and standards in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Minimum Necessary and Notice of Privacy Practices are used with the same meaning as the respective standard and requirement in the HIPAA Rules.

1.2 Specific Definitions

- (a) “Organization” generally has the same meaning as the term “covered entity” at 45 CFR [160.103](#) and, in reference to the Party to this Agreement, means Family Eldercare, Inc.
- (b) “Business Associate” generally has the same meaning as the term “business associate” at 45 CFR [160.103](#) and, in reference to the Party to this Agreement, means [Business Associate legal name].
- (c) “HIPAA Rules” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR [Part 160](#) and [Part 164](#), as amended.
- (d) “Discovery,” “Incident Notification,” and “Incident Notification List” have the meanings given in the Services Agreement (see RFP Section 3.3).
- (e) “Unsuccessful Security Incident” means an attempted Security Incident that does not result in unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations, such as pings, port scans, blocked log-on attempts, and denial-of-service attempts that do not affect availability.

1.3 Sensitive Information

“PHI” means Protected Health Information. “Sensitive Information” means PHI, all other individually identifiable information about Clients, and personally identifiable information about the Organization’s employees, volunteers, board members, and donors, in each case that Business Associate creates, receives, maintains, or transmits on the Organization’s behalf, in any form, including copies in backups, exports, logs, tickets, screenshots, and documentation. Sensitive Information that is not PHI is protected under this Agreement as a matter of contract, whether or not the HIPAA Rules apply to it. As applied to Sensitive Information that is not PHI, “Breach” means any acquisition, access, use, or disclosure not permitted by this Agreement that compromises its security, confidentiality, or integrity.

2. Obligations and Activities of Business Associate

2.1 Limits on Use and Disclosure

Business Associate agrees to not use or disclose Sensitive Information other than as permitted or required by this Agreement or as Required By Law.

2.2 Safeguards

Business Associate agrees to use appropriate administrative, physical, and technical safeguards, and comply with 45 CFR [Part 164, Subpart C](#) with respect to Electronic Protected Health Information, to prevent use or disclosure of Sensitive Information other than as provided for by this Agreement. These safeguards include, at a minimum, multi-factor authentication for all administrative access to Organization systems and encryption of Sensitive Information in electronic form in transit and at rest within systems and storage under Business Associate's control.

2.3 Reporting

- (a) **Incident Notification.** Business Associate agrees to report to the Organization any Security Incident (other than an Unsuccessful Security Incident), any Breach of Unsecured PHI or of other Sensitive Information, and any use or disclosure of Sensitive Information not provided for by this Agreement, by Incident Notification to every recipient on the Incident Notification List within four (4) hours of Discovery, at any hour, by the method stated in the Services Agreement. Business Associate shall not delay Incident Notification pending confirmation of scope, cause, or attribution.
- (b) **Written report.** Business Associate agrees to, within five (5) business days of Discovery, provide a written report that includes to the extent known the information required by 45 CFR [164.410\(c\)](#), including the identification of each person whose Unsecured PHI or other Sensitive Information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed, and any other information the Organization needs to meet its own notification obligations under the HIPAA Rules and applicable state law, including [Texas Business and Commerce Code Chapter 521](#). Business Associate shall supplement the report promptly as further information becomes available, preserve relevant logs and forensic evidence, and cooperate with the Organization's investigation, including with any forensic firm, insurer, or law enforcement agency involved.
- (c) **Relationship to legal deadlines.** The timeframes in this Section 2.3 are stricter than—and applied in addition to—those in 45 CFR [164.410](#). Nothing in this Agreement extends any deadline under the HIPAA Rules or other applicable law.

- (d) **Unsuccessful Security Incidents.** Business Associate agrees to summarize in its regular service reporting all Unsuccessful Security Incidents, for which no further individual report is required.
- (e) **Notifications to third parties.** The Organization determines whether a Breach has occurred and controls all notifications to Individuals and other affected persons, the Secretary, the Texas Attorney General and other regulators, the media, funders, and any upstream covered entity, unless it delegates a notification to Business Associate in writing. Business Associate shall not make any such notification regarding the Organization's Sensitive Information without the Organization's prior written consent, except as Required By Law.
- (f) **Mitigation and costs.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect known to Business Associate of a use or disclosure of Sensitive Information in violation of this Agreement. Where a Breach results from the failure of Business Associate or its Subcontractor to comply with this Agreement or the HIPAA Rules, Business Associate shall reimburse the Organization's reasonable, documented costs of investigation, notification, call-center support, and credit monitoring or identity protection services offered to affected persons. Business Associate's obligations under this Section 2.3(f) are not subject to any limitation or exclusion of liability in the Services Agreement, but shall not exceed the cyber liability insurance limits required by the Services Agreement.

2.4 Data Location and Personnel

Business Associate agrees to store Sensitive Information, including backup copies, only in data centers and cloud regions located in the United States, and comply with the personnel location and remote administrative access requirements of the Services Agreement (see RFP Addendum No. 1, Section 3). Business Associate shall disclose to the Organization in advance, and limit to the minimum necessary, any access to Sensitive Information by personnel located outside the United States.

2.5 Subcontractors

In accordance with 45 CFR [164.502\(e\)\(1\)\(ii\)](#) and [164.308\(b\)\(2\)](#), Business Associate agrees to ensure that any Subcontractor or other third party (including providers of Business Associate's remote monitoring and management, remote access, ticketing, documentation, and backup tools) that creates, receives, maintains, or transmits Sensitive Information on behalf of Business Associate agrees in writing to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement, including Sections 2.3 and 2.4. Subcontractors must be disclosed and approved as provided in the Services Agreement (see RFP Addendum No. 1, Section

1.2). Business Associate shall furnish a copy of each subcontractor business associate agreement to the Organization on request and remains responsible to the Organization for its Subcontractors' compliance. In this Agreement, references to Business Associate's Subcontractors include each such third party.

2.6 Minimum Necessary

Business Associate agrees to limit its uses, disclosures, and requests of Sensitive Information to the minimum necessary, consistent with 45 CFR [164.502\(b\)](#) and the Organization's minimum necessary policies and procedures as provided to Business Associate.

2.7 Workforce

Business Associate agrees to ensure that each member of its workforce and each Subcontractor individual with access to Sensitive Information has completed the background screening required by the Services Agreement and has received training on the HIPAA Rules, applicable Texas privacy law (including [Texas Health and Safety Code Chapter 181](#)), and this Agreement appropriate to that individual's role.

2.8 Access

To the extent Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make it available to the Organization within ten (10) business days of the Organization's request, as necessary to satisfy the Organization's obligations under 45 CFR [164.524](#). Business Associate shall forward to the Organization within five (5) business days any such request it receives directly from an Individual.

2.9 Amendment

To the extent Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make any amendment directed or agreed to by the Organization under 45 CFR [164.526](#) within ten (10) business days of the Organization's request, and forward to the Organization within five (5) business days any request for amendment it receives directly from an Individual.

2.10 Accounting of Disclosures

Business Associate agrees to maintain and, within ten (10) business days of the Organization's request, make available the information required for the Organization to provide an accounting of disclosures under 45 CFR [164.528](#).

2.11 Privacy Rule Obligations

To the extent Business Associate carries out one or more of the Organization's obligations under 45 CFR [Part 164, Subpart E](#), Business Associate agrees to comply

with the requirements of Subpart E that apply to the Organization in the performance of those obligations.

2.12 Books and Records

Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules, and, unless prohibited by law, promptly notify the Organization of any such request.

2.13 Security Assurance

On the Organization's request, Business Associate agrees to provide, not more than once annually and following any Breach, its most recent independent third-party attestation of its own controls (for example, a SOC 2 report or ISO/IEC 27001 certification) or, if none exists, a written description of its safeguards for Sensitive Information, subject to the audit and monitoring support terms of the Services Agreement.

3. Permitted Uses and Disclosures by Business Associate

3.1 Permitted Uses and Disclosures

- (a) **Services and Legal Requirements.** Business Associate may use or disclose Sensitive Information as necessary to perform the services set forth in the Services Agreement or as Required By Law.
- (b) **Management and Administration.** Business Associate may use Sensitive Information for its proper management and administration or to carry out its legal responsibilities, and may disclose it for those purposes only if the disclosure is Required By Law or Business Associate obtains reasonable assurances from the recipient that it will keep the information confidential, use or further disclose it only as Required By Law or for the purpose for which it was disclosed, and notify Business Associate of any breach of confidentiality of which it becomes aware.

3.2 Restrictions

- (a) **Privacy Rule Limits.** Business Associate may not use or disclose PHI in a manner that would violate 45 CFR [Part 164, Subpart E](#) if done by the Organization, except for the specific uses and disclosures set forth in Section 3.1(b).

- (b) **Prohibited Uses.** Business Associate shall not (i) de-identify Sensitive Information, except as necessary to perform the services or with the Organization's prior written approval; (ii) provide Data Aggregation services; (iii) sell Sensitive Information or use or disclose it for marketing or fundraising; or (iv) use Sensitive Information, or data derived from it, to train, fine-tune, or improve any machine learning or artificial intelligence model, or for analytics or product development for Business Associate's own purposes.

4. Obligations of the Organization

4.1 Limitations

The Organization shall notify Business Associate of any limitation in its Notice of Privacy Practices under 45 CFR [164.520](#), any change in or revocation of an Individual's permission to use or disclose PHI, and any restriction on the use or disclosure of PHI the Organization has agreed to under 45 CFR [164.522](#), in each case to the extent it may affect Business Associate's use or disclosure of PHI.

4.2 Incident Notification List

The Organization shall maintain and provide to Business Associate its current Incident Notification List, as provided in the Services Agreement.

4.3 Impermissible Requests

The Organization shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under 45 CFR [Part 164, Subpart E](#) if done by the Organization, except as permitted in Section 3.1(b).

5. Term and Termination

5.1 Term

This Agreement is effective as of the Effective Date and terminates on the later of the termination or expiration of the Services Agreement or the date on which all Sensitive Information has been returned or destroyed under Section 5.3.

5.2 Termination For Cause

The Organization may terminate this Agreement and the Services Agreement if Business Associate violates a material term of this Agreement and fails to cure the violation within thirty (30) days of written notice, or immediately on written notice if cure is not possible.

5.3 Obligations On Termination

Upon termination or expiration of this Agreement for any reason, Business Associate shall, and shall cause its Subcontractors to:

- (a) return to the Organization, or to a successor provider at the Organization's written direction, all Sensitive Information that Business Associate or its Subcontractors maintain in any form, including backup data and retention history, in a commonly readable or usable format consistent with the transition obligations of the Services Agreement (see RFP Section 3.1 and Q&A items 10.3 and 10.4);
- (b) continue to retain and protect backup data without gap until the Organization confirms in writing that the successor provider's backups have been verified;
- (c) within thirty (30) days after that confirmation, destroy all remaining Sensitive Information other than Sensitive Information retained under Section 5.3(d), using methods consistent with [NIST Special Publication 800-88](#) Rev. 2, and certify the destruction to the Organization in writing;
- (d) retain only Sensitive Information that is necessary for Business Associate to continue its proper management and administration or carry out its legal responsibilities, or that is contained in records Business Associate must retain under 2 CFR [200.334](#) as provided in the Services Agreement (see Q&A item 4.4), and notify the Organization in writing of the Sensitive Information retained and the reason; and
- (e) for as long as any Sensitive Information is retained, continue to apply the protections of this Agreement and 45 CFR [Part 164, Subpart C](#) to it, not use or disclose it other than for the purposes for which it was retained, and return or destroy it when it is no longer needed for those purposes.

5.4 Survival

The obligations of Business Associate under Sections 2.3, 5.3, and 6.3 survive the termination of this Agreement.

6. Miscellaneous

6.1 Regulatory References

A reference in this Agreement to a section of the HIPAA Rules, 2 CFR Part 200, or a Texas statute means the section as in effect or as amended.

6.2 Amendment

This Agreement may be amended only by a written instrument signed by both Parties. The Parties shall negotiate in good faith to amend this Agreement as necessary to comply with any change in the HIPAA Rules or other applicable law,

including any final rule modifying the HIPAA Security Rule. If the Parties have not agreed on a necessary amendment within sixty (60) days after either Party requests it, the Organization may terminate this Agreement and the Services Agreement on written notice.

6.3 Interpretation and Order of Precedence

Any ambiguity in this Agreement shall be resolved to permit compliance with the HIPAA Rules and other applicable law. With respect to Sensitive Information, this Agreement controls over any conflicting term of the Services Agreement; where both impose an obligation regarding Sensitive Information, the obligation more protective of Sensitive Information applies.

6.4 Independent Contractor

Business Associate is an independent contractor and not an agent of the Organization.

6.5 No Third-Party Beneficiaries

Nothing in this Agreement confers any rights or remedies on any person other than the Parties and their respective successors and permitted assigns.

6.6 Governing Law

This Agreement is governed by the laws of the State of Texas, except to the extent preempted by federal law.

6.7 Notices

Notices under this Agreement shall be in writing and delivered by hand, courier, or email to the addresses below. Incident Notifications and reports under Section 2.3 are delivered as provided in that Section, not under this Section 6.7.

6.8 Counterparts; Electronic Signatures

This Agreement may be executed in counterparts and by electronic signature, each of which is deemed an original.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

FAMILY ELDERCARE, INC.	[BUSINESS ASSOCIATE]
By: _____	By: _____
Name: Dr. Aaron Alarcon	Name: [Name]
Title: Chief Executive Officer	Title: [Title]
Date: _____	Date: _____
<i>Address for notices:</i>	<i>Address for notices:</i>
Attn: Chief Executive Officer	Attn: [Name and title]
with a copy to: IT & Data Manager	[Street address]
1700 Rutherford Lane	[City, State ZIP]
Austin, Texas 78754	[Email]
[Email]	