

BUSINESS ASSOCIATE AGREEMENT

Agreement Pursuant to 45 CFR § 164.308(b), § 164.314(a), and § 164.504(e)

AVEECARE, LLC

Home Healthcare Management Platform

Document Type:	Business Associate Agreement (Standard Form)
Regulatory Reference:	45 CFR § 164.308(b), § 164.314(a), § 164.504(e); HITECH Act
Document Version:	1.0
Effective Date:	_____

Important Notice

This Business Associate Agreement ("BAA") is based on the model provisions published by the U.S. Department of Health and Human Services (HHS) and has been customized for AveeCare, LLC's cloud-based home healthcare management platform. This BAA is designed for use between AveeCare (as Business Associate) and home health agencies, hospice providers, and other Covered Entities (as Covered Entity clients) who use AveeCare's platform to manage patient care and store Protected Health Information (PHI).

PREAMBLE

This Business Associate Agreement ("Agreement" or "BAA") is entered into as of the Effective Date set forth below by and between:

COVERED ENTITY:	_____ ("Covered Entity" or "Client")
Address:	_____
City, State, ZIP:	_____
Contact Person:	_____
Email:	_____
Phone:	_____

AND

BUSINESS ASSOCIATE:	AveeCare, LLC ("Business Associate" or "AveeCare")
Address:	_____
City, State, ZIP:	_____

Contact Person:	_____
Email:	security@aveecare.com
Phone:	_____

Covered Entity and Business Associate are each referred to herein as a "Party" and collectively as the "Parties."

RECITALS

WHEREAS, Covered Entity is a home health agency, hospice, or other healthcare provider that qualifies as a "Covered Entity" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and their implementing regulations (collectively, the "HIPAA Rules");

WHEREAS, Business Associate provides a cloud-based home healthcare management platform known as "AveeCare" that enables Covered Entity to manage patient care, caregiver scheduling, visit documentation, messaging, and other healthcare operations;

WHEREAS, in connection with providing the Services, Business Associate will Create, Receive, Maintain, or Transmit Protected Health Information ("PHI") on behalf of Covered Entity;

WHEREAS, the HIPAA Rules require Covered Entity to obtain satisfactory assurances from Business Associate that Business Associate will appropriately safeguard PHI;

WHEREAS, under the HITECH Act, Business Associate is directly liable for compliance with certain provisions of the HIPAA Rules;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

ARTICLE I - DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules. The following definitions apply to this Agreement:

Section 1.1 - Regulatory Definitions

"Breach" shall have the meaning given to such term under 45 CFR § 164.402, as may be amended from time to time.

"Designated Record Set" shall have the meaning given to such term under 45 CFR § 164.501.

"Electronic Protected Health Information" or "ePHI" shall have the meaning given to such term under 45 CFR § 160.103, limited to information that Business Associate Creates, Receives, Maintains, or Transmits on behalf of Covered Entity.

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164, as amended by the HITECH Act and any subsequent amendments.

"Individual" shall have the meaning given to such term under 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"Protected Health Information" or "PHI" shall have the meaning given to such term under 45 CFR § 160.103, limited to information Created, Received, Maintained, or Transmitted by Business Associate on behalf of Covered Entity.

"Required By Law" shall have the meaning given to such term under 45 CFR § 164.103.

"Secretary" means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

"Security Incident" shall have the meaning given to such term under 45 CFR § 164.304.

"Subcontractor" shall have the meaning given to such term under 45 CFR § 160.103.

"Unsecured Protected Health Information" shall have the meaning given to such term under 45 CFR § 164.402.

Section 1.2 - Agreement-Specific Definitions

"**AveeCare Platform**" or "**Platform**" means the cloud-based home healthcare management software application provided by Business Associate, including all associated mobile applications, web interfaces, APIs, and related services.

"**Services**" means the home healthcare management services provided by Business Associate to Covered Entity through the AveeCare Platform, as further described in Exhibit A attached hereto.

"**Service Agreement**" means any master services agreement, subscription agreement, terms of service, or other agreement between the Parties governing Business Associate's provision of the Services to Covered Entity, as may be amended from time to time.

"**Workforce**" shall have the meaning given to such term under 45 CFR § 160.103.

ARTICLE II - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

Section 2.1 - Permitted Uses and Disclosures

Business Associate agrees to not Use or Disclose PHI other than as permitted or required by this Agreement or as Required By Law. Specifically, Business Associate may:

- (a) Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Service Agreement, provided that such Use or Disclosure would not violate the HIPAA Rules if done by Covered Entity;
- (b) Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate;
- (c) Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that:
 - (i) The Disclosure is Required By Law; or
 - (ii) Business Associate obtains reasonable assurances from the person to whom the PHI is Disclosed that it will be held confidentially and Used or further Disclosed only as Required By Law or for the purpose for which it was Disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
- (d) Use PHI to provide Data Aggregation services relating to the Health Care Operations of Covered Entity, if specifically authorized in the Service Agreement;
- (e) De-identify PHI in accordance with 45 CFR § 164.514(a)-(c), provided that Business Associate may Use or Disclose such de-identified information for any lawful purpose.

Section 2.2 - Minimum Necessary Standard

Business Associate agrees to make reasonable efforts to Use, Disclose, and Request only the minimum amount of PHI necessary to accomplish the intended purpose of the Use, Disclosure, or Request, except as otherwise permitted under 45 CFR § 164.502(b)(2).

Section 2.3 - Prohibited Uses and Disclosures

Business Associate shall NOT:

- (a) Use or Disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except as permitted under Section 2.1;
- (b) Use or Disclose PHI for fundraising or marketing purposes, unless expressly authorized in writing by Covered Entity and in compliance with 45 CFR § 164.514(f) or § 164.508;
- (c) Sell PHI, as defined under 45 CFR § 164.502(a)(5)(ii), without prior written authorization from the Individual and Covered Entity;
- (d) Use or Disclose PHI for underwriting purposes;
- (e) Use or Disclose genetic information for underwriting purposes in violation of the Genetic Information Nondiscrimination Act (GINA).

Section 2.4 - Safeguards

Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI that it Creates, Receives, Maintains, or Transmits on behalf of Covered Entity, including but not limited to:

(a) **Administrative Safeguards:**

- (i) Designating a security official responsible for the development and implementation of security policies and procedures;
- (ii) Implementing workforce security procedures, including access authorization, supervision, and termination;
- (iii) Conducting security awareness and training for all Workforce members;
- (iv) Maintaining security incident procedures for identifying, responding to, and mitigating Security Incidents;
- (v) Maintaining contingency plans including data backup, disaster recovery, and emergency mode operations;
- (vi) Conducting periodic technical and non-technical evaluations of security controls;

(b) **Physical Safeguards:**

- (i) Implementing facility access controls appropriate to the nature of Business Associate's operations;
- (ii) Implementing workstation use and security policies;
- (iii) Implementing device and media controls for hardware and electronic media containing ePHI;

(c) **Technical Safeguards:**

- (i) Implementing access controls including unique user identification, emergency access procedures, automatic logoff, and encryption;
- (ii) Implementing audit controls to record and examine activity in systems containing ePHI;
- (iii) Implementing integrity controls to protect ePHI from improper alteration or destruction;
- (iv) Implementing person or entity authentication mechanisms;
- (v) Implementing transmission security measures including encryption of ePHI transmitted over electronic networks;

AveeCare's Security Infrastructure

AveeCare's platform is hosted on Amazon Web Services (AWS), a HIPAA-eligible cloud infrastructure provider. Business Associate maintains a Business Associate Agreement with AWS. All ePHI is encrypted at rest using AES-256 encryption and in transit using TLS 1.2 or higher. Multi-factor authentication is required for all user accounts. Detailed security specifications are provided in Exhibit B.

Section 2.5 - Subcontractors

Business Associate agrees to:

- (a) In accordance with 45 CFR § 164.502(e)(1)(ii) and § 164.308(b)(2), ensure that any Subcontractor that Creates, Receives, Maintains, or Transmits PHI on behalf of Business Associate agrees in writing to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement with respect

(b) Maintain a list of Subcontractors that have access to PHI and provide such list to Covered Entity upon request;

(c) Remain responsible for the acts and omissions of its Subcontractors as if such acts or omissions were Business Associate's own.

Section 2.6 - Reporting Requirements

Business Associate agrees to report to Covered Entity:

(a) **Breach Notification:** Following the Discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity without unreasonable delay and in no case later than **thirty (30) calendar days** after Discovery. Such notification shall include, to the extent possible:

(i) A brief description of what happened, including the date of the Breach and the date of Discovery;

(ii) A description of the types of Unsecured PHI involved in the Breach (e.g., names, Social Security numbers, diagnoses);

(iii) Any steps Individuals should take to protect themselves from potential harm;

(iv) A brief description of what Business Associate is doing to investigate the Breach, mitigate harm, and protect against further Breaches;

(v) Contact information for Business Associate's representative;

(vi) The identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed;

(b) **Security Incidents:** Business Associate shall report to Covered Entity any Security Incident of which it becomes aware. For Security Incidents that do not involve a Breach, Business Associate may provide summary reports on a monthly basis or as otherwise agreed by the Parties;

(c) **Unsuccessful Security Incidents:** The Parties acknowledge that unsuccessful Security Incidents (such as pings, port scans, unsuccessful log-in attempts, and denial of service attacks that do not result in unauthorized access) occur with regularity. Business Associate is not required to report such unsuccessful Security Incidents but will maintain logs and make them available to Covered Entity upon reasonable request.

Section 2.7 - Access to PHI

Business Associate agrees to:

- (a) Provide access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under 45 CFR § 164.524;
- (b) Provide such access in the time and manner reasonably designated by Covered Entity, and in no event more than **fifteen (15) business days** following a request;
- (c) If PHI is maintained electronically, provide access in the electronic form and format requested by the Individual, if readily producible, or in a readable electronic form and format agreed to by Covered Entity and the Individual;
- (d) If Business Associate receives a request for access directly from an Individual, Business Associate shall forward such request to Covered Entity within **five (5) business days**.

Section 2.8 - Amendment of PHI

Business Associate agrees to:

- (a) Make PHI in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 CFR § 164.526;
- (b) Complete such amendments within **fifteen (15) business days** of receiving instructions from Covered Entity;
- (c) If Business Associate receives a request for amendment directly from an Individual, Business Associate shall forward such request to Covered Entity within **five (5) business days**.

Section 2.9 - Accounting of Disclosures

Business Associate agrees to:

- (a) Document Disclosures of PHI and information related to such Disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528;
- (b) Provide to Covered Entity, within **fifteen (15) business days** of a request, information collected in accordance with this Section to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures;
- (c) Make accounting information available for at least **six (6) years** prior to the date on which the accounting is requested;
- (d) If Business Associate receives a request for an accounting directly from an Individual, Business Associate shall forward such request to Covered Entity within **five (5) business days**.

Section 2.10 - Availability of Books and Records

Business Associate agrees to make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or Created or Received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of determining compliance with the HIPAA Rules. Business Associate shall provide Covered Entity with **ten (10) business days** prior written notice of any such request by the Secretary, to the extent permitted by law.

Section 2.11 - Documentation and Retention

Business Associate agrees to:

- (a) Maintain documentation of its security policies, procedures, and practices as required by the Security Rule;
- (b) Retain such documentation for **six (6) years** from the date of creation or the date when it was last in effect, whichever is later;
- (c) Make such documentation available to Covered Entity upon reasonable request.

ARTICLE III - OBLIGATIONS OF COVERED ENTITY

Section 3.1 - Provision of Notice of Privacy Practices

Covered Entity shall provide Business Associate with a copy of its Notice of Privacy Practices produced in accordance with 45 CFR § 164.520, as well as any changes to such Notice, to the extent that such changes may affect Business Associate's obligations under this Agreement.

Section 3.2 - Changes in Authorization or Restriction

Covered Entity shall provide Business Associate with any changes in, or revocation of, the permission by an Individual to Use or Disclose PHI, to the extent that such changes may affect Business Associate's permitted Uses or Disclosures.

Section 3.3 - Notification of Restrictions

Covered Entity shall notify Business Associate of any restriction on the Use or Disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's permitted Uses or Disclosures.

Section 3.4 - Permissible Requests

Covered Entity shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity, except as specifically permitted under Section 2.1 of this Agreement.

Section 3.5 - Accurate Information

Covered Entity represents and warrants that it has obtained all necessary consents, authorizations, and permissions required under applicable law for the Disclosure of PHI to Business Associate and for Business Associate's Use and Disclosure of PHI as contemplated by this Agreement and the Service Agreement.

ARTICLE IV - TERM AND TERMINATION

Section 4.1 - Term

This Agreement shall become effective on the Effective Date and shall remain in effect until the earlier of:

- (a) Termination of the Service Agreement between the Parties;
- (b) Termination of this Agreement in accordance with Section 4.2 or 4.3; or
- (c) The date on which Business Associate no longer maintains any PHI received from, or Created or Received on behalf of, Covered Entity.

Section 4.2 - Termination for Cause

Either Party may terminate this Agreement if the other Party materially breaches this Agreement and:

- (a) The breaching Party fails to cure the breach within **thirty (30) calendar days** after receiving written notice specifying the nature of the breach; or
- (b) The breach is of a nature that cannot reasonably be cured.

In the event of a material breach that cannot be cured, the non-breaching Party may immediately terminate this Agreement upon written notice to the breaching Party.

Section 4.3 - Termination for Convenience

Either Party may terminate this Agreement for convenience upon **ninety (90) calendar days** prior written notice to the other Party, subject to Business Associate's obligations under Section 4.4.

Section 4.4 - Effect of Termination

Upon termination of this Agreement for any reason:

- (a) **Return or Destruction:** Business Associate shall, at Covered Entity's election:
 - (i) Return to Covered Entity all PHI received from, or Created or Received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form; or
 - (ii) Destroy all such PHI and retain no copies in any form;
- (b) **Infeasibility:** If Business Associate determines that returning or destroying PHI is infeasible, Business Associate shall:
 - (i) Provide written notice to Covered Entity explaining the conditions that make return or destruction infeasible;
 - (ii) Extend the protections of this Agreement to such PHI;
 - (iii) Limit further Uses and Disclosures of such PHI to those purposes that make return or destruction infeasible; and
 - (iv) Return or destroy such PHI when and if return or destruction becomes feasible;
- (c) **Data Export:** Upon Covered Entity's request made within **thirty (30) calendar days** of termination, Business Associate shall provide Covered Entity with an export of Covered Entity's data in a commonly used electronic format;
- (d) **Survival:** The obligations of Business Associate under this Section 4.4 shall survive the termination of this Agreement.

Data Retention After Termination

Business Associate will retain Covered Entity's data for a period of **ninety (90) calendar days** following termination to allow for data export. After this period, data will be securely destroyed unless return or destruction is infeasible, in which case the provisions of Section 4.4(b) shall apply. Covered Entity acknowledges that certain data may be retained in backup systems for a limited period as part of Business Associate's standard backup and disaster recovery procedures.

ARTICLE V - LIABILITY AND INDEMNIFICATION

Section 5.1 - HITECH Direct Liability

The Parties acknowledge and agree that, pursuant to the HITECH Act, Business Associate is directly liable for violations of the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule as if Business Associate were a Covered Entity. Nothing in this Agreement shall be construed to limit Business Associate's direct liability under applicable law.

Section 5.2 - Indemnification by Business Associate

Business Associate shall indemnify, defend, and hold harmless Covered Entity and its directors, officers, employees, and agents from and against any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to:

- (a) Any Breach of Unsecured PHI caused by Business Associate or its Subcontractors;

- (b) Any violation of this Agreement by Business Associate or its Subcontractors;

(c) Any violation of the HIPAA Rules by Business Associate or its Subcontractors;

(d) Any negligent or wrongful act or omission of Business Associate or its Subcontractors in connection with this Agreement.

Section 5.3 - Indemnification by Covered Entity

Covered Entity shall indemnify, defend, and hold harmless Business Associate and its directors, officers, employees, and agents from and against any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to:

- (a) Any violation of this Agreement by Covered Entity;
- (b) Any violation of the HIPAA Rules by Covered Entity;
- (c) Covered Entity's failure to obtain required Individual authorizations or consents;
- (d) Any instructions provided by Covered Entity that are not in compliance with the HIPAA Rules.

Section 5.4 - Limitation of Liability

EXCEPT FOR LIABILITY ARISING FROM (I) INDEMNIFICATION OBLIGATIONS UNDER THIS ARTICLE V, (II) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (III) A BREACH OF CONFIDENTIALITY OR SECURITY OBLIGATIONS, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Section 5.5 - Insurance

Business Associate shall maintain, at its own expense, the following insurance coverage:

- (a) Commercial General Liability insurance with limits of not less than \$1,000,000 per occurrence;
- (b) Professional Liability (Errors and Omissions) insurance with limits of not less than \$1,000,000 per claim;
- (c) Cyber Liability insurance with limits of not less than \$1,000,000 per claim, covering data breach response costs, notification costs, regulatory fines and penalties (where insurable), and third-party claims arising from data breaches.

Business Associate shall provide Covered Entity with certificates of insurance evidencing such coverage upon request.

ARTICLE VI - GENERAL PROVISIONS

Section 6.1 - Regulatory References

A reference in this Agreement to a section of the HIPAA Rules means the section as in effect or as amended from time to time. This Agreement shall be interpreted in accordance with the HIPAA Rules and any applicable guidance issued by HHS.

Section 6.2 - Amendment

The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. No amendment to this Agreement shall be effective unless in writing and signed by both Parties.

Section 6.3 - Interpretation

Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules. In the event of any conflict between this Agreement and the Service Agreement with respect to obligations relating to PHI, this Agreement shall control.

Section 6.4 - No Third-Party Beneficiaries

Nothing in this Agreement shall confer upon any person or entity other than the Parties and their respective successors and permitted assigns any rights, remedies, obligations, or liabilities whatsoever. Individuals whose PHI is subject to this Agreement are not third-party beneficiaries of this Agreement.

Section 6.5 - Assignment

Neither Party may assign this Agreement or any rights or obligations hereunder without the prior written consent of the other Party, except that Business Associate may assign this Agreement to an affiliate or in connection with a merger, acquisition, or sale of all or substantially all of its assets, provided that the assignee agrees in writing to be bound by the terms of this Agreement.

Section 6.6 - Notices

All notices, requests, demands, and other communications under this Agreement shall be in writing and shall be deemed given when:

- (a) Delivered personally;
- (b) Sent by certified or registered mail, return receipt requested, postage prepaid;
- (c) Sent by a nationally recognized overnight courier service; or
- (d) Sent by email with confirmed receipt;

to the addresses set forth in the Preamble or to such other address as either Party may designate in writing from time to time.

Section 6.7 - Waiver

The failure of either Party to enforce any provision of this Agreement shall not be deemed a waiver of such provision or of the right to enforce such provision at a later time.

Section 6.8 - Severability

If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect. The Parties shall negotiate in good faith to replace any invalid or unenforceable provision with a valid and enforceable provision that achieves, to the extent possible, the original intent of the Parties.

Section 6.9 - Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of _____, without regard to its conflicts of law principles, except to the extent preempted by federal law. Any dispute arising out of or relating to this Agreement shall be resolved in the state or federal courts located in _____.

Section 6.10 - Entire Agreement

This Agreement, together with the Service Agreement and any exhibits attached hereto, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous agreements, understandings, and communications, whether written or oral, relating to such subject matter.

Section 6.11 - Counterparts

This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Signatures transmitted by facsimile or electronic means (including PDF) shall be deemed original signatures for all purposes.

EXECUTION

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

Effective Date
This Agreement is effective as of: _____

COVERED ENTITY

By signing below, the undersigned represents that they are authorized to bind Covered Entity to the terms of this Agreement.

Legal Entity Name:	_____
---------------------------	-------

Authorized Signature

Title

Printed Name

Date

BUSINESS ASSOCIATE

AveeCare, LLC, by its authorized representatives:

Authorized Representative #1

Authorized Signature

Title

Printed Name

Date

Authorized Representative #2

Authorized Signature

Title

Printed Name

Date

EXHIBIT A - DESCRIPTION OF SERVICES

This Exhibit A describes the Services provided by Business Associate to Covered Entity under this Agreement.

A.1 - Platform Overview

AveeCare provides a cloud-based home healthcare management platform ("Platform") that enables home health agencies, hospice providers, and other healthcare organizations to:

1. Manage patient records, including demographics, medical history, medications, allergies, and care plans;
2. Schedule and track caregiver visits, including visit documentation and task completion;
3. Facilitate secure messaging between caregivers, administrators, patients, and family members;
4. Generate reports and analytics on patient care and agency operations;
5. Manage caregiver information, credentials, and schedules;
6. Document incidents and maintain compliance records;
7. Support billing and invoicing processes;
8. Provide mobile applications for caregivers and patients.

A.2 - Categories of PHI

In providing the Services, Business Associate may Create, Receive, Maintain, or Transmit the following categories of PHI on behalf of Covered Entity:

Category	Examples
Patient Demographics	Name, address, date of birth, gender, contact information
Patient Identifiers	Medicaid ID, Medicare ID, insurance ID numbers
Medical Information	Diagnoses, comorbidities, medications, allergies, care plans
Clinical Documentation	Visit notes, assessments, care observations, incident reports
Treatment Information	Services provided, ADLs completed, tasks performed
Communications	Messages between care team members regarding patient care
Signatures	Patient signatures acknowledging visits, consent forms
Documents	Uploaded patient documents, medical records, forms

A.3 - Permitted Purposes

Business Associate is permitted to Use and Disclose PHI for the following purposes:

1. Providing the Platform and Services to Covered Entity;
2. Technical support and customer service;
3. Platform maintenance, updates, and improvements;
4. Quality assurance and performance monitoring;
5. Compliance with legal and regulatory requirements;

6. As otherwise permitted or required under this Agreement.

A.4 - AI-Powered Features

The Platform includes optional artificial intelligence (AI) features that may process PHI to provide functionality such as report generation, form auto-fill, and care insights. Covered Entity may disable AI features through the Platform settings. When AI features are enabled:

- (a) PHI may be processed by AI models hosted on AWS infrastructure;
- (b) Business Associate implements data minimization practices to limit PHI exposure;
- (c) AI processing is covered under Business Associate's BAA with AWS;
- (d) No PHI is used for AI model training purposes.

EXHIBIT B - SECURITY SPECIFICATIONS

This Exhibit B describes the technical and administrative security measures implemented by Business Associate to protect ePHI.

B.1 - Infrastructure Security

Security Control	Implementation
Cloud Provider	Amazon Web Services (AWS) - HIPAA-eligible services only
Data Center Security	AWS data centers with SOC 2, ISO 27001, and other certifications
Network Security	Virtual Private Cloud (VPC), security groups, network ACLs
DDoS Protection	AWS Shield for distributed denial-of-service protection

B.2 - Encryption

Data State	Encryption Standard
Data at Rest (Database)	AES-256 encryption via AWS DynamoDB
Data at Rest (File Storage)	AES-256 encryption via AWS S3
Data in Transit	TLS 1.2 or higher for all communications
Key Management	AWS Key Management Service (KMS)

B.3 - Access Controls

Control	Implementation
User Authentication	AWS Cognito with mandatory multi-factor authentication (TOTP)
Role-Based Access	Granular permissions based on user roles (Admin, Caregiver, Patient)
Multi-Tenancy	Company-based data isolation; users can only access their organization's data
Session Management	Automatic session timeout and secure token handling
Password Policy	Minimum 12 characters with complexity requirements

B.4 - Audit Controls

Audit Capability	Implementation
Application Audit Logs	All Create, Update, Delete operations logged with user, timestamp, and details
Infrastructure Logs	AWS CloudTrail for API activity logging
Log Retention	Minimum 6 years per HIPAA requirements

Log Integrity	Logs stored in append-only, immutable storage
---------------	---

B.5 - Business Continuity

Capability	Implementation
Data Backup	Automated daily backups with point-in-time recovery
Geographic Redundancy	Data replicated across multiple AWS Availability Zones
Disaster Recovery	Documented recovery procedures with regular testing
Uptime Target	99.9% availability (excluding scheduled maintenance)

B.6 - Subcontractor BAAs

Business Associate maintains Business Associate Agreements with the following key Subcontractors:

Subcontractor	Service	BAA Status
Amazon Web Services (AWS)	Cloud infrastructure, database, storage, authentication	Active

EXHIBIT C - BREACH NOTIFICATION PROCEDURES

This Exhibit C describes the procedures for reporting and responding to Breaches of Unsecured PHI.

C.1 - Breach Discovery and Internal Response

Upon Discovery of a potential Breach, Business Associate shall:

1. Immediately activate its incident response procedures;
2. Preserve evidence and document the incident;
3. Conduct a preliminary assessment to determine if a Breach has occurred;
4. If a Breach is confirmed, identify the scope and affected Individuals;
5. Implement measures to mitigate harm and prevent recurrence.

C.2 - Notification to Covered Entity

Business Associate shall notify Covered Entity of a confirmed Breach within **thirty (30) calendar days** of Discovery. Notification shall include:

- (a) **Description of the Breach:** What happened, when it happened, when it was discovered;
- (b) **Types of PHI Involved:** Categories of information compromised (names, SSNs, diagnoses, etc.);
- (c) **Affected Individuals:** List of Individuals whose PHI was affected, to the extent known;
- (d) **Investigation Status:** Summary of investigation findings and ongoing activities;
- (e) **Mitigation Measures:** Steps taken to mitigate harm and prevent future incidents;
- (f) **Recommended Actions:** Suggestions for Individual notification content and protective steps;
- (g) **Contact Information:** Point of contact for questions and coordination.

C.3 - Covered Entity Notification Responsibilities

Covered Entity retains responsibility for:

1. Determining whether notification to affected Individuals is required under 45 CFR § 164.404;
2. Preparing and sending notification letters to affected Individuals;
3. Reporting to the Secretary as required under 45 CFR § 164.408;
4. Providing media notification if required under 45 CFR § 164.406;
5. Maintaining required documentation of Breach notifications.

C.4 - Cooperation

Business Associate shall cooperate fully with Covered Entity in:

1. Investigating the Breach;
2. Preparing notification materials;
3. Responding to inquiries from affected Individuals, regulators, and media;
4. Implementing corrective actions;
5. Providing information necessary for regulatory reporting.

C.5 - Contact Information for Breach Reporting

Business Associate Breach Notification Contact	
Name:	Security Officer, AveeCare, LLC
Email:	security@aveecare.com
Phone:	_____

Covered Entity shall provide its designated contact for Breach notifications:

Covered Entity Breach Notification Contact	
Name:	_____
Title:	_____
Email:	_____
Phone:	_____

Document Control

Version	Date	Author	Description of Changes
1.0	January 31, 2026	AveeCare Compliance	Initial document creation based on HHS model BAA provisions

Next Scheduled Review: _____ (Recommend annual review or upon regulatory changes)

Legal Disclaimer

This Business Associate Agreement is prepared based on the model provisions published by the U.S. Department of Health and Human Services (HHS) and applicable HIPAA regulations. While prepared with reference to current law and HHS guidance, this document does not constitute legal advice. Both Parties should consult with qualified legal counsel to ensure this Agreement meets their specific legal requirements and circumstances.

Regulatory Sources

- 45 CFR § 164.308(b) - Business Associate Contracts and Other Arrangements
- 45 CFR § 164.314(a) - Business Associate Contracts or Other Arrangements
- 45 CFR § 164.504(e) - Business Associate Contracts
- HITECH Act, Public Law 111-5, Subtitle D
- HHS Sample Business Associate Agreement Provisions (<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>)

— End of Document —