Addus HomeCare
Privacy Policies

Addus HomeCare
PRIVACY POLICIES

TABLE OF CONTENTS

Addus HomeCare Privacy Policies		
Policy No: PP-01	Effective Date: 07/01/2017	
Pages: 3	Revision No. N/A	Date Reviewed: 08/23/2022

OVERVIEW AND DEFINITIONS

1. Uses and Disclosures of PHI. Under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy, security and standard transaction regulations (45 CFR Parts 160, 162 and 164) ("HIPAA Rules"), Addus HealthCare, Inc., and its subsidiaries and affiliated covered entities (collectively, "Addus") is a home care and home health company that is a Covered Entity because it is a health care provider that performs certain standardized transactions electronically. Addus will treat Protected Health Information as defined below in accordance with these policies and procedures ("Privacy Policies"). Addus may not use or disclose PHI except as specifically permitted or required by the HIPAA Rules.

2. Individual Rights. As a Covered Entity, Addus is also required to permit individuals to exercise certain rights with respect to their PHI (as detailed in PP-12-15). Addus will not require individuals to waive any of their rights under HIPAA, the Privacy Rules, or these Privacy Policies as a condition of treating the patient, payment for their care, eligibility for benefits or otherwise.

3. HIPAA State Law Preemption. Addus HomeCare will comply with applicable state laws where Addus operates as well as the federal HIPAA Rules, the HITECH Act and the HIPAA Omnibus Rules.

4. Definitions.

"Business Associate" means a person or entity who:

(1) on behalf of Addus, but other than in the capacity of a member of Addus' workforce, creates, receives, maintains, or transmits PHI for a function or activity regulated by the Privacy Rules, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed in 42 CFR § 3.20, billing, benefit management, practice management, and repricing; or

(2) provides, other than in the capacity of a member of Addus' workforce, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for Addus, where the provision of the service involves the disclosure of PHI from Addus, or from another Business Associate of Addus, to the person.

Subcontractors (as defined below) are also Business Associates.

"Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the privacy provisions of HIPAA and that compromises the security or privacy of the PHI, unless an exception applies as described in PP -17.

"Covered Entity" is a health plan, healthcare clearinghouse or healthcare provider who transmits any health information in electronic form in connection with a transaction covered under the Privacy Rules (including Addus).

"De-identified Information" means information that does not include any of the following identifiers of an individual or of the individual's employer, family members or household members: name; all geographic subdivisions smaller than a state (including street address, city, county, precinct and zip code); all elements of dates related to an individual (including birth date, admission date and discharge date) except for years (other than year of birth for those over 89); telephone numbers; fax numbers; electronic mail address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; serial number of a vehicle or other device identifier; internet URL; internet protocol (IP) address number; biometric identifiers, including finger and voice prints; full face photographic images and any other unique information that could reasonably be used alone or in combination with other information to identify an individual.

"Designated Record Set" means: a group of records maintained by or for Addus that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Addus to make decisions about individuals.

"Electronic PHI" or "EPHI" means PHI that is transmitted by electronic media or maintained in electronic media. The term "electronic media" means: (i) electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (ii) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

"Genetic Information" means information about (i) an individual's genetic tests, (ii) the genetic tests of family members of the individual, and (iii) the manifestation of a disease or disorder in family members of such individual. It includes any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. It does not include information about the sex or age of any individual.

"HHS" means the U.S. Department of Health and Human Services.

"Protected Health Information" or "PHI" means information whether oral, written or electronic that (a) is created or received by a health care provider, health plan, employer or health care clearinghouse; (b) relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (c) identifies the individual or provides a reasonable basis to believe the information at issue can be used to identify the individual. PHI pertains to both living and deceased individuals until the individual is deceased for 50 years.

Security Officer responsible for the implementation and support of information security initiatives throughout Addus HealthCare, Inc.

"Unsecured PHI" means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified on the HHS website (**www.hhs.gov/ocr/privacy**). For example, PHI that has not been encrypted in

accordance with HHS guidance or that has not been shredded or destroyed so that the information cannot be read or reconstructed is unsecured PHI.

"Workforce members" means employees and other persons whose conduct, in the performance of work for Addus, is under the direct control of Addus, whether or not they are paid by Addus, and who have access to PHI.

Other Terms. Terms contained herein and defined in the HIPAA Rules shall have the meaning given to such terms in the HIPAA Rules.

5. Privacy Officer

Addus HomeCare shall designate and maintain an active HIPAA Privacy Officer at all times. The Privacy Officer shall oversee the implementation and enforcement of these Privacy Policies. The obligations of the Privacy Officer described in these Privacy Policies shall be performed by the Privacy Officer or the Privacy Officer's designee. The Privacy Officer is responsible for all obligations specified in these Privacy Policies as being an action required to be performed by, or supervised by, the Privacy Officer and for taking acts necessary to carry out these Privacy Policies, including but not limited to the following:

5.1 ensuring Business Associate Agreements are in place with Addus' Business Associates and, in the event Addus acts as a Business Associate of a third party, ensuring that Subcontractor Business Associate Agreements are in place with Addus' vendors who handle PHI on its behalf;

5.2 reviewing, approving and negotiating Business Associate Agreements and Subcontractor Business Associate Agreements;

5.3 training Addus workforce members on these Privacy Policies;

5.4 responding to patterns of activity or practices that constitute violations of these Privacy Policies;

5.5 overseeing prompt and appropriate investigation and resolution of incidents or complaints;

5.6 implementing steps necessary to mitigate harm caused by violations of the HIPAA Rules or these Privacy Policies by Addus;

5.7 receiving, processing and implementing requests related to patient rights;

5.8 maintaining documentation required by these Privacy Policies;

5.9 making required HIPAA-related reports to individuals, the media and HHS and being the point person for interacting with individuals and third parties for issues related to compliance with the HIPAA Rules;

5.10 reviewing and revising these Privacy Policies as necessary to comply with the HIPAA Rules and changes to Addus' operations.

Addus HomeCare Privacy Policies		
Policy No: PP-02	Effective Date: 07/01/2017	
Pages: 3	Revision No. N/A	Date Reviewed: 08/23/2022

BUSINESS ASSOCIATE AGREEMENTS

1. In General. Addus is required to have in place Business Associate Agreements with all of its Business Associates who use or disclose PHI on behalf of Addus before allowing a Business Associate to receive PHI on its behalf. A Business Associate Agreement establishes the permitted and required uses and disclosures of PHI by the Business Associate and also authorizes termination by Addus of the Business Associate Agreement or other relationship if it is determined that the Business Associate has violated the terms of the agreement.

2. Agreements with Business Associates. Addus has developed a standard Business Associate Agreement template that meets the requirements set forth in the HIPAA Rules that is or will be attached to its template service agreements. At the beginning of a new relationship with a Business Associate and before allowing the Business Associate to receive PHI, Addus will confirm that a Business Associate Agreement is in place. When possible, Addus will use its Business Associate Agreement template. If a contractor requests Addus to sign its form, the agreement will be forwarded to the Privacy Officer for review and, if necessary, negotiation.

The Privacy Officer or his/her designee will sign all Business Associate Agreements with contractors (that are not incorporated into the relevant service agreement) and return an original to the contractor.

Copies of all signed Business Associate Agreements will be maintained in accordance with PP-19.

3. Required Components of Business Associate Agreement. The following items are required elements of a Business Associate Agreement (a "BAA"):

3.1 Requiring the Business Associate to only use or disclose PHI in accordance with the BAA or as required by law. The services and duties of the Business Associate must either be specified in an underlying service agreement or in the BAA.

3.2 Requiring the Business Associate to maintain appropriate administrative, technical and physical safeguards to protect the confidentiality of PHI and to comply with the applicable provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to Electronic PHI to prevent any use or disclosure of such information other than as provided by the BAA.

3.3 Requiring the Business Associate to report non-permitted uses and disclosures, security incidents and breaches to Addus (see PP-17).

3.4 Requiring the Business Associate to obligate Subcontractors to comply with the same requirements and conditions that apply to the Business Associate with respect to such information.

3.5 Requiring the Business Associate to make PHI available and to amend PHI to satisfy the individual rights provisions of the HIPAA Rules.

3.6 Requiring the Business Associate to document disclosures required to be reported under the accounting obligation and to provide such documentation to Addus.

3.7 Requiring the Business Associate to provide access to its internal practices, books and records to HHS for purposes of determining compliance with the HIPAA Rules.

3.8 Requiring the Business Associate to return or destroy all PHI upon termination of the BAA, if feasible, and to continue to abide by the BAA with respect to any PHI that is infeasible to return or destroy and only use and disclose retained PHI for purposes that make return or destruction infeasible.

3.9 Authorizing termination of the BAA if the Business Associate violates a material term of the BAA.

3.10 Requiring the Business Associate, to the extent that the Business Associate) is to carry out an obligation of a Covered Entity under the HIPAA Rules, to comply with the requirements of the HIPAA Rules that apply to the Covered Entity in the performance of such obligation.

3.11 Any other items required by the HIPAA Rules, as may be amended from time to time.

The BAA may also expressly address other items such as the minimum necessary standard, restrictions on the use or disclosure of PHI for marketing or fundraising, prohibitions on the sale of PHI and that the Business Associate may be subject to the penalty provisions of the HIPAA Rules.

If Addus is acting as a Business Associate of another party (for example, if Addus provides administrative services involving PHI to a hospice, home health agency or other provider), then Addus must sign a BAA with the other party. In this situation, Addus would be the Business Associate. The Privacy Officer must be consulted before signing any BAA that will obligate Addus as a Business Associate. Addus must comply with the terms of any BAA it signs, including any limitations on uses or disclosures that would otherwise be permitted by these Privacy Policies.

4. Oversight of Business Associates. Addus will perform reasonable and appropriate reviews of its Business Associates. The scope and frequency of such reviews will vary depending on the nature and extent of PHI being shared with the Business Associate and may involve surveys, obtaining signed certifications and on-site reviews as deemed appropriate by the Privacy Officer (in coordination with the Security Officer for Business Associates that access or receive electronic PHI).

An Addus workforce member who becomes aware of any pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the BAA with the Business Associate must promptly notify the Privacy Officer. Addus will take reasonable steps to

cure the breach or end the violation by the Business Associate. If such steps are unsuccessful, Addus shall terminate the agreement between the parties.

Addus HomeCare Privacy Policies		
Policy No: PP-03	Effective Date: 07/01/2017	
Pages: 7	Revision No. N/A	Date Reviewed: 08/23/2022

USES AND DISCLOSURES OF PHI- IN GENERAL

1. In General. Addus HealthCare, Inc. shall recognize all clients, regardless of referral source or source of payment, have rights concerning their Protected Health Information (PHI), including their individually identifiable health information. In compliance with the applicable provisions of this Policy, Addus may only use and disclose PHI as permitted or required under the HIPAA Rules. The HIPAA Rules continue to apply even after an individual is deceased until the individual is deceased for 50 years. Thus, Addus must continue to comply with these Privacy Policies with respect to the PHI of deceased individuals until it has evidence the individual has been deceased for at least 50 years. For more information on disclosures of PHI regarding deceased individuals, see PP-06.

To be permissible, a use or disclosure must comply with all applicable provisions of these Policies. Although a use or disclosure may be permissible, in many cases certain procedures or safeguards must be followed (see, for example, verification requirements set forth in PP-09). Any Addus workforce member who is not sure whether a contemplated use or disclosure is permissible must consult with the Privacy Officer before making the use or disclosure.

Before disclosing any PHI to a Business Associate of Addus, Addus must enter into a Business Associate Agreement as described in PP-02.

2. Minimum Necessary. Addus must make reasonable efforts to limit uses and disclosures of and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The minimum necessary requirement does not apply to: (a) disclosures to or requests by Addus for treatment; (b) uses or disclosures made to the individual who is the subject of the PHI; (c) uses or disclosures made pursuant to an authorization; (d) disclosures made to the HHS; or (e) uses or disclosures that are required for compliance with the HIPAA Rules.

2.1 Each Addus workforce member will only use and access the amount of PHI necessary to perform his or her assigned job duties.

2.2 For any routine disclosures or requests for PHI made by Addus, Addus will limit the amount of PHI disclosed or requested to the minimum amount of PHI necessary for the disclosure or request, based on such factors as (a) the type of PHI to be used, disclosed or requested; (b) the types of persons who will use the disclosure or who will receive the disclosure or the requests; (c) the conditions that will apply to the use, disclosure or request; and (d) the purpose for which the PHI will be used, disclosed or requested.

For non-routine disclosures and requests made by Addus, Addus will limit the PHI disclosed or requested to the information reasonably necessary to accomplish the purpose of the disclosure or request. Addus will comply with this standard by considering the following criteria for non-routine requests or disclosures: (1) what is the purpose of the request or disclosure? (2) what type of PHI is needed for this purpose? (3) how important is the need for the PHI (versus

De-Identified Information)? (4) are there reasonable alternatives to requesting PHI? (5) is the request or disclosure limited to the scope of PHI needed for the purpose of the disclosure or request? and (6) any other relevant factors specific to the request or disclosure.

2.3 Addus will not use, disclose or request an entire medical record except when the entire record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure or request. Addus may charge for the handling, duplication and postage related to the release of client Protected Health Information in accordance with its fee schedule to the extent permissible under the federal HIPAA Privacy Rule and applicable state-specific confidentiality laws.

3. Uses and Disclosures that Do Not Require an Authorization. Subject to the requirements outlined in Section 2 of this Policy, the requirements of more restrictive state law provisions and the terms of any restriction requests agreed to by Addus (see PP-14, Section 3), Addus may use and disclose PHI for treatment, payment and health care operations without obtaining an individual authorization.

3.1 Treatment. Addus may use an individual's PHI to provide the individual with medical treatment or services. Addus may disclose PHI to doctors, nurses, individuals, technicians, medical students and other trainees, or other personnel who are involved in taking care of the individual. Addus also may disclose PHI about individuals to other affiliated and non-affiliated health care providers involved in the individual's medical care.

3.2 Payment. Addus may use and disclose PHI about an individual so that the treatment and services the individual received may be billed to and payment may be collected from the individual, an insurance company, or a third party. Addus may also disclose to a health plan PHI about a treatment an individual is going to receive to obtain prior approval or to determine whether the individual's plan will cover the treatment. Addus has developed a consent form that is uses to document the individual's consent to the release of PHI for filing and collecting insurance claims.

3.3 Health Care Operations. Addus may use and disclose PHI about individuals for health care operations of Addus. These are uses and disclosures necessary to operate Addus and to make sure all individuals receive quality care. Such uses and disclosures include the following:

(a) conducting quality assessment and total quality improvement activities;

(b) population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and contacting of health care providers and individuals with information about treatment alternatives;

(c) reviewing the competence or qualifications of health care professionals, evaluating provider performance, health plan performance, conducting training programs, accreditation, certification, licensing or credentialing;

(d) conducting or arranging for medical review, legal services and auditing functions, including compliance programs;

(e) except as prohibited by Section 6 below, underwriting, enrollment, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care, provided certain requirements are met;

(f) business planning such as conducting cost-management and planning related analyses to manage and operate the Covered Entity, including formulary development and administration, and development of improvements in methods of payment;

(g) business management and general administrative activities; and

(h) creating De-identified Information or Limited Data Sets.

To the extent permitted by state law, Addus may disclose PHI to another Covered Entity to use for its health care operations if certain conditions are met. First, both Addus and the covered entity must have (or must have had) a relationship with the individual who is the subject of the PHI, and the disclosed PHI must pertain to that relationship. Second, the disclosure may be made only for the following purposes: (i) conducting quality assessment and improvement activities; (ii) population-based activities relating to improving health or reducing health care costs, case management and care coordination, and contacting of health care providers and individuals with information about treatment alternatives; (iii) reviewing the competence or qualifications of health care professionals, evaluating provider performance, conducting training programs, accreditation, certification, licensing or credentialing purposes; or (iv) fraud and abuse detection or compliance. Addus will only disclose PHI to another covered entity for its health care operations if the Privacy Officer has first determined that all applicable requirements have been met.

4. Certain Other Uses and Disclosures of PHI that Do Not Require Individual Authorization

4.1 Addus may use and disclose PHI under the following circumstances without obtaining an individual authorization. If Addus workforce members receive a request for a disclosure in one of the categories below that is not addressed by a separate Addus policy, such workforce member shall immediately contact the Privacy Officer for assistance in responding to the request and shall only use or disclose the PHI after receiving the Privacy Officer's approval. Many of the categories listed below contain detailed requirements and limitations not described below which must be complied with and may be further limited by state law. Except for disclosures pursuant to 4.1(k) and 4.1(l) below, the disclosures listed in this Section 4.1 must be recorded for purposes of providing the individual with an accounting (See PP-13):

(a) Uses and disclosures required by federal or state law, in compliance with and limited to the relevant requirements of such law;

(b) Disclosures for public health activities such as (i) reporting to a public health authority PHI to prevent disease and injury and to report vital statistics related to birth and death and other PHI to conduct public health surveillance, public health investigations and public health interventions; (ii) reporting to a public health authority or other appropriate government authority authorized to receive reports of child abuse or neglect; and (iii) disclosing to a person subject to the food and drug administration for FDA-regulated purposes;

(c) Disclosures to an authorized government agency to report victims of abuse, neglect or domestic violence (consistent with PP-07);

(d) Disclosures to health oversight agencies;

(e) Disclosures for judicial and administrative proceedings pursuant to a valid subpoena, court order or other lawful process of a court or administrative tribunal (consistent with PP-08);

(f) Disclosures to law enforcement for certain law enforcement purposes;

(g) Disclosures regarding death and decedents to coroners, medical examiners and funeral directors (consistent with PP-06);

(h) Uses and disclosures for cadaveric organ, tissue or eye donation (consistent with PP-06);

(i) Uses and disclosures for certain research activities;

(j) Uses and disclosures to prevent serious and imminent harm to health or safety of a person or the public;

(k) Uses and disclosures for specialized government functions, including: armed forces, national security and intelligence, protective services for the President and others, to the Department of the State to make medical suitability determinations;

(l) Disclosures to correctional institutions and law enforcement officials regarding an inmate;

(m) Disclosures regarding Worker's Compensation claims pursuant to appropriate compliance with state law requirements.

4.2 Limited Data Sets. Addus may use or disclose PHI that constitutes a Limited Data Set for purposes of research, public health or health care operations. A "Limited Data Set" is information that is De-identified (see PP-01), except that the individual's town, city, state and zip code, birth date and other dates may remain. Disclosures of a Limited Data Set for this purpose require a Data Use Agreement that meets requirements specified in the HIPAA Rules.

(a) If an Addus workforce member wishes to use or disclose PHI that constitutes a Limited Data Set, the workforce member should consult with the Privacy Officer first and ensure that a Data Use Agreement is in place. If a third party requests that an Addus workforce member sign a Data Use Agreement, the workforce member must send the Data Use Agreement to the Privacy Officer for review and approval.

(d) Copies of all Data Use Agreements must be retained in accordance with PP-19.

4.3 Incidental Uses and Disclosures. An incidental use or disclosure is a use or disclosure that cannot be reasonably prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure of PHI. Incidental uses and disclosures are permissible only to the extent that Addus has applied reasonable safeguards (see PP-11) and has implemented the minimum necessary standard (see Section 2 of this Policy) where applicable.

5. Disclosures Pursuant to an Authorization. Addus may use or disclose PHI as permitted by an authorization that complies with the requirements of this Section 5.

5.1 To be valid, an authorization must be written in plain language and contain the following information:

(a) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(b) Name or specific identification of the person or persons who can make the requested use or disclosure.

(c) Name or specific identification of the person or persons who may receive the requested use or disclosure.

(d) A description of each purpose of the requested use or disclosure (if the request was made by the individual and the individual does not wish to give the reason for the request, the authorization may include the words *"per individual request"* for the description).

(e) An expiration date or expiration event. (Expiration event must relate to the individual or the purpose of the use or disclosure. May use the statement *"end of research study"* if the authorization is for research.) If the authorization is for the creation or maintenance of a research database or research repository, no expiration date is needed and the statement *"none"* can be used.

(f) Statement of the individual's rights to revoke authorization in writing, exceptions to the right to revoke and description informing the individual how to revoke the authorization.

(g) Statement that Addus may not condition treatment, payment, enrollment or eligibility for benefits on the authorization (or, in the limited instances in which Addus may condition treatment or enrollment in a health plan on the signing of the authorization, the consequences of the individual's refusal to sign the authorization – see Section 5.5 below).

(h) Statement that information used or disclosed may be subject to re-disclosure by the recipient and no longer protected by the HIPAA Rules.

(i) **If the authorization is for <u>marketing</u>** as defined in PP-05, a statement regarding any remuneration that Addus will receive as a result of the use and/or disclosure of the PHI.

(j) **If the authorization is for the <u>sale of PHI</u>** as defined in PP-05, the authorization must state that the disclosure of PHI will result in payment to Addus.

(k) The individual's (or personal representative's (see PP-10) signature and date signed.

(l) If signed by a personal representative, a description of the representative's authority to act on behalf of the individual.

5.2 An individual may revoke an authorization at any time provided that the revocation is in writing, except to the extent that Addus already taken action in reliance on the authorization, or if the authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

5.3 Addus must obtain an authorization before using or disclosing PHI for a purpose not otherwise expressly permitted by these Privacy Policies. Further, an authorization is required to use or disclose psychotherapy notes, to use or disclose PHI for purposes of marketing or to sell PHI (see PP-05).

5.4 An authorization is invalid if and may not be relied upon if:

(a) The expiration date is past or the expiration event is known by Addus to have occurred;

(b) The authorization has not been filled out completely or the authorization does not contain all of the elements required by Section 5.1 to be included in a valid authorization;

(c) The authorization is a compound authorization, meaning it is combined with another permission form such as a consent to treatment (except in limited circumstances, and the Privacy Officer must verify whether such authorization is permitted if a workforce member has any questions regarding whether a compound authorization may be used);

(d) The authorization was provided to Addus improperly as a condition to the individual's being enrolled in a health plan or the individual's being eligible for benefits; or

(e) Addus knows the authorization contains material information that is false.

5.5 Addus will not condition the provision of treatment to an individual on the provision of an authorization, unless the authorization is sought for research purposes or if the authorization is for disclosure of PHI to a third party and the treatment of the individual is solely for the purpose of creating PHI for disclosure to a third party.

5.6 Copies of authorization forms and revocations will be retained by Addus in accordance with PP-19.

5.7 An authorization is not required for individuals requesting their own PHI. Addus will not require individuals to sign an authorization in order to exercise their access rights as described in PP-14.

6. Uses and Disclosures of Genetic Information

6.1 The Genetic Information Nondiscrimination Act of 2008 ("GINA") regulates health plans and employers, but does not currently regulate health providers performing health services. GINA generally prohibits health plans from: (a) requesting or requiring Genetic Information of an individual or an individual's family members; (b) adjusting premium or contribution amounts on the basis of Genetic Information; or (c) requesting or requiring Genetic Information for underwriting purposes. "Underwriting purposes" includes making decisions regarding eligibility for benefits, preexisting conditions and computing premiums or contribution amounts. GINA generally prohibits employers from using Genetic Information for hiring, firing, or promotion decisions, and for any decisions regarding terms of employment.

6.2 Many states have also enacted laws to protect the confidentiality of Genetic Information. The majority of these require individual patient consent in order to perform a genetic test or to obtain Genetic Information and require the individual's consent to disclose Genetic Information. Addus will comply with such laws as applicable.

Addus HomeCare Privacy Policies		
Policy No: PP-04	Effective Date: 07/01/2017	
Pages: 1	Revision No. N/A	Date Reviewed: 08/23/2022

USES AND DISCLOSURES TO FAMILY/THOSE INVOLVED IN CARE/DISASTER RELIEF

1. In General. Subject to the conditions set forth below, Addus may:

1.1 disclose to an individual's family member, other relative, or close personal friend, PHI directly relevant to such person's involvement with the individual's care or payment related to such care; or

1.2 use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, other relative, or other person responsible for the care of the individual or the individual's location or general condition.

2. When the Individual is Present or Capable of Making Decisions. If the individual is present or otherwise available and is capable of making health care decisions, Addus may disclose the PHI if: (a) the individual agrees to the disclosure; (b) Addus provides the individual with an opportunity to object to the disclosure and the individual does not object; or (c) Addus reasonably infers from the circumstances that the individual does not object to the disclosure.

3. If an Individual is not Present or Does not Have an Opportunity to Object. If the individual is not present or if Addus cannot provide the individual with the opportunity to object (such as in an emergency or if the individual is incapacitated), Addus may determine whether the disclosure is in the best interests of the individual. Addus may reasonably infer from the circumstances surrounding the request, or otherwise utilize the professional judgment of Addus' workforce members and its experience with common practice, to make reasonable inferences of the individual's best interest in disclosing PHI to a person on behalf of an individual. If so, Addus may only use or disclose PHI that is directly relevant to the person's involvement with the individual's health care.

4. For Disaster Relief Efforts. Addus may use or disclose PHI to a public or private entity authorized to assist in disaster relief efforts to coordinate the notification of a family member, personal representative or other person responsible for the individual's care regarding the individual's location, general condition, or death. The individual must be given notice of the proposed disclosure and an opportunity to agree or object unless Addus, in the exercise of professional judgment, determines that this requirement would interfere with its ability to respond to the emergency situation.

5. Form of Consent/Objection. Addus may orally inform an individual of, and obtain the individual's oral agreement or objection to, any of the uses or disclosures addressed in this Policy. To the extent Addus maintains written documentation of an individual's consent for or objection to a use or disclosure addressed in this Policy, Addus should retain such documentation in accordance with PP-19.

MARKETING AND SALE OF PHI

1. Marketing

1.1 In General. The HIPAA Rules prohibit the use or disclosure of PHI for marketing purposes without an authorization in accordance with PP-03, Section 5, unless an exception applies as discussed in this Policy. Workforce members who have questions about whether a proposed service or arrangement would involve the use or disclosure of PHI for marketing must contact the Privacy Officer before proceeding. The Privacy Officer must confirm that the proposed arrangement meets an exception or, if it does not, will assist with obtaining required authorizations.

"Marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. The HIPAA Rules expressly exclude certain communications from the definition of marketing, as discussed below.

1.2 Refill Reminders and Related Communications. Addus may provide refill reminders and related communications to individuals, which may involve the use or disclosure of PHI. The definition of "marketing" does **not** include communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication. The HIPAA Rules contain a number of requirements in order to meet this refill reminder exception. Since refill reminders are unlikely to apply to Addus, these are not discussed in this policy. If any Addus workforce member is considering an arrangement that would involve refill reminders, the workforce member must notify the Privacy Officer and these Privacy Policies will be revised.

1.3 Other Exceptions to the Definition of Marketing. The following types of communications are also carved out of the definition of marketing under the HIPAA Rules. Any workforce member who has a question regarding whether certain proposed communications or services are permitted without an authorization and pursuant to the Business Associate Agreement with the client must consult the Privacy Officer.

(a) Communications for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, provided that no financial remuneration is received in exchange for making the communication. "**Financial remuneration**" means direct or indirect payment from or on

behalf of the third party whose product or service is being described. Financial remuneration does **not** include non-financial or in-kind benefits (such as supplies or computers). It also does **not** include any payment for the treatment of an individual;

(b) Communications to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits, provided that no financial remuneration is received in exchange for making the communication; and

(c) Communications for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment, provided that no financial remuneration is received in exchange for making the communication.

1.4 Exceptions to the Rule Requiring an Authorization. For communications that meet the definition of marketing, an authorization is **not** required in (i) face-to-face marketing to an individual; or (ii) providing a promotional gift of nominal value to an individual.

2. Sale of PHI

2.1 In. General. The sale of PHI is defined as any disclosure of PHI by Addus where Addus directly or indirectly receives remuneration (i.e. anything of value) from or on behalf of the recipient of the PHI in exchange for the PHI, except for the following disclosures:

(a) for public health purposes under the HIPAA Rules public health exception or for public health purposes pursuant to the Limited Data Set rules as outlined in PP-03;

(b) for research purposes under the HIPAA Rules research exception or for research purposes pursuant to the Limited Data Set rules as outlined in PP-03 if the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

(c) for treatment and payment purposes in accordance with PP-03;

(d) for the sale, transfer, merger or consolidation of all or part of Addus and for related due diligence as permitted by the definition of healthcare operations in accordance with PP-03;

(e) to or by a Business Associate for activities that the Business Associate undertakes on behalf of Addus and the only remuneration provided is by Addus to the Business Associate for the performance of such activities (see PP-02);

(f) to an individual when requested under the access or accounting provisions of the HIPAA Regulations (see PP-13 and 14);

(g) required by law (see PP-03); and

(h) permitted by and in accordance with the applicable requirements of the HIPAA Rules where the only remuneration received by Addus is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

2.2 Authorization. Before engaging in the sale of PHI, Addus will first obtain written patient authorization in accordance with PP-03, Section 5. Workforce members who have questions about whether a proposed arrangement would involve the sale of PHI must contact the Privacy Officer before proceeding. The Privacy Officer must confirm that the proposed arrangement meets an exception or, if it does not, will assist with obtaining required authorizations.

3. Documentation. Any authorizations for the sale of PHI and/or a use or disclosure of PHI for marketing purposes must be retained by Addus in accordance with PP-19.

Addus HomeCare Privacy Policies		
Policy No: PP-06	Effective Date: 07/01/2017	
Pages: 1	Revision No.: N/A	Date Reviewed: 08/23/2022

USES AND DISCLOSURES CONCERNING DEATH

1. In General. The requirements of these Privacy Policies apply to the PHI of all living and deceased individuals for 50 years following death. After an individual has been deceased 50 years, his or her individually identifiable health information is no longer protected by HIPAA and is not subject to the Privacy Policies.

2. Family Member or Friend Involved in or Paid for the Care. A workforce member may disclose a deceased individual's PHI to a family member, or other person who was involved in or paid for the individual's care, in accordance with PP-04.

3. Uses and Disclosures about Decedents.

3.1 Addus may disclose PHI to a coroner or medical examiner for the purpose of (a) identifying a deceased individual, (b) determining a cause of death, (c) or other duties as authorized by law (consistent with PP-03, Section 4.1(f)).

3.2 Addus may disclose PHI to funeral directors as necessary to carry out their duties with respect to the deceased (which may include, if necessary, disclosing PHI prior to, and in reasonable anticipation of, an individual's death) (consistent with PP-03, Section 4.1(f)).

3.3 Addus may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation (consistent with PP-03, Section 4.1(g))

4. Disclosures to Personal Representatives. If under applicable law, an executor, administrator or other person has authority to act on behalf of a deceased individual or the individual's estate, Addus shall treat such person as a personal representative with respect to PHI relevant to such personal representation, in accordance with PP-10.

5. Verification. Workforce members should confirm the identity and authority of the person making the request for PHI (except pursuant to Section 2) in accordance with PP-09.

6. Documentation. For disclosures permitted under Section 3, Addus will document the disclosure in the log of disclosures in accordance with PP-13. Addus will retain copies of items required to be maintained pursuant to this Policy (such as documents used to verify identity and authority of requestors) as described in PP-19.

USES AND DISCLOSURES CONCERNING VICTIMS OF ABUSE, NEGLECT AND DOMESTIC VIOLENCE

1. In General. Addus may disclose PHI about a person that Addus reasonably believes to be a victim of abuse, neglect, or domestic violence if the following requirements are met.

1.1 Disclosures for this purpose may only be made to a government authority authorized by law to receive these types of reports.

1.2 Disclosures for this purpose may only be made if one of the following is true:

(a) The disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

(b) The disclosure is expressly authorized (but not necessarily required) by statute or regulation, and Addus workforce members believe, in the exercise of professional judgment, that the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(c) The disclosure is expressly authorized (but not necessarily required) by statute or regulation, and the individual is incapacitated, and the law enforcement or other public official who would receive the disclosure:

i. Is authorized to receive the report; and

ii. Represents that (i) the information is not intended to be used against the individual and that (ii) an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

2. Informing the Individual. If Addus makes a disclosure for this purpose, Addus must promptly tell the individual that the report has been or will be made, unless one of the following is true:

2.1 Addus workforce members believe, in the exercise of professional judgment, that informing the individual would place the individual at risk of serious harm; or

2.2 Addus would be informing the individual's personal representative and Addus workforce members reasonably believe, in the exercise of professional judgment that the personal representative is responsible for the abuse, neglect, or other injury, and that informing the personal representative would not be in the best interests of the individual.

3. Report of Child Abuse or Neglect. Disclosures to report child abuse to a public health authority are not subject to the conditions set forth in Sections 1 or 2 above. Addus may disclose PHI to a public health authority or other appropriate government agency authorized by law to receive reports of child abuse or neglect in accordance with PP-03, Section 4.1(b)).

4. Contacting Privacy Officer. Any workforce member that reasonably believes an individual may be a victim of abuse, neglect, or domestic violence shall consult with the Privacy Officer, who shall determine whether all the requirements for disclosure under this Policy are met prior to the disclosure.

5. Verification. To the extent applicable, Addus will verify the identity and authority of the recipient of the PHI in accordance with PP-09.

6. Documentation. For each disclosure as permitted by this Policy, Addus will document the disclosure in the log of disclosures in accordance with PP-13. Addus will also retain copies of all items required to be maintained pursuant to this Policy (such as documentation relied upon to verify a requestor's identity or authority) in accordance with PP-19.

DISCLOSURES OF PHI IN JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

1. In General. Before using or disclosing any PHI pursuant to this Policy, Addus must confirm all applicable provisions of this Policy and PP-03 have been met.

2. Authorization. Addus may disclose PHI in a lawsuit if the individual has authorized the release. The individual's authorization must be obtained in accordance with PP-03, Section 5.

3. Disclosures of PHI in Response to a Court Order. Addus may disclose PHI in response to an order of a court or administrative tribunal, provided that Addus discloses only the PHI expressly authorized by such order. If an Addus workforce member receives a court order requesting the disclosure of PHI, the workforce member must contact the Privacy Officer immediately. The Privacy Officer will review the order and consult with legal counsel as needed to confirm that the order is valid and to coordinate Addus' response.

4. Disclosures of PHI in Response to a Subpoena, Discovery Request or Other Lawful Process in the Absence of a Court Order. Addus may disclose PHI in response to a subpoena, discovery request or other lawful process in the absence of a court order, provided certain conditions are met.

4.1 In all cases when a workforce member receives a subpoena, discovery request or other lawful process, the workforce member must contact the Privacy Officer before responding in any way. PHI may not be disclosed unless Addus receives "satisfactory assurance" that the requesting party has made reasonable efforts either to (i) secure a qualified protective order or (ii) notify the individual(s) whose PHI is being sought as described below.

4.2 For disclosures when the requesting party has secured a qualified protective order (except when state law provides otherwise), Addus has received "satisfactory assurance" if Addus has received a written statement and accompanying documentation demonstrating that: (i) the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or (ii) the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal. For purposes of this condition, a "qualified protective order" means, with respect to PHI requested, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return to Addus or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

4.3 Alternatively, Addus may meet the satisfactory assurances requirement by making reasonable efforts to seek a qualified protective order as described above.

4.4 For disclosures when the requesting party has provided notice to the individuals, Addus receives "satisfactory assurance" if it has received a written statement and accompanying documentation demonstrating that: (i) the party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (ii) the notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and (iii) the time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objections were filed or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

4.5 Alternatively, Addus may meet the satisfactory assurances requirement by making reasonable efforts to notify the individual and allowing the individual to object as described above.

4.6 In response to a valid discovery request, subpoena or other lawful process, only the minimum amount of PHI necessary for the purpose may be disclosed in accordance with PP-03.

5. Party to Litigation. If Addus is a party to the litigation, Addus may not be required to comply with all provisions of this policy. For example, HIPAA permits the disclosure of PHI for health care operations (see PP-03) without an authorization, and certain provisions of state law may permit disclosure of PHI absent a subpoena when Addus is a party to the litigation. The Privacy Officer shall consult with legal counsel as appropriate and coordinate Addus' response.

6. Verification. Addus will verify the identity and authority of the recipient of the PHI in accordance with PP-09(2)(b).

7. Documentation. For disclosures permitted by Sections 3 or 4, Addus will document the disclosure in the log of disclosures in accordance with PP-13. Addus will also retain copies of all court orders, subpoenas and other documentation pursuant to which disclosures are made under this Policy as described in PP-19.

VERIFICATION

1. In General. Except for disclosures made pursuant to Policy # HIPAA-4 or as otherwise provided in this Policy, Addus will make reasonable efforts to verify the identity and authority of any person who requests PHI from Addus. Verification is the process of confirming the identity and authority of any person who requests PHI and of obtaining any required documentation regarding that request.

2. Verifying Identity

2.1 Before making a permitted disclosure of PHI, Addus must verify the identity of any person unknown to Addus who requests PHI and the authority of any person known or unknown to Addus to have access to PHI. Addus must also obtain any documentation required for release of PHI from the person requesting the PHI (such as a copy of a court order when a requestor claims disclosure is required pursuant to an order). Addus may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for disclosure, if Addus' reliance is reasonable under the circumstances and is in good faith.

2.2 The obligation to verify identity and authority does not apply if the person requesting the PHI and their authority to receive the PHI are known to Addus.

2.3 If Addus cannot verify a person's identity and authority to access PHI, Addus will not disclose the PHI.

2.4 If the person requesting PHI claims to be a public official or to be acting on behalf of a public official, Addus may rely on the following to verify the person's *identity*, if such reliance is reasonable:

(a) if the request is in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(b) if the request is in writing, the request is on appropriate government letterhead; or

(c) if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order that establishes that the person is acting on behalf of the public official.

3. Verifying Authority

3.1 Addus will also request evidence of *authority* of the public official to access PHI.

3.2 If it is reasonable to do so under the circumstances, Addus may rely on the following to verify the authority of a public official or a person acting on behalf of a public official: (a) a written statement of the legal authority under which the information is requested or, if a written statement of legal authority would be impracticable (such as an emergency), an oral statement of such legal authority; or (b) if the request is made pursuant to a legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

3.3 If the person requesting PHI is the individual, Addus will need to verify the individual's *identity* but not the individual's authority. An individual is always authorized to receive his or her own PHI.

3.4 If a disclosure is conditioned on particular documentation, statements or representations from the person requesting the PHI, Addus may reasonably rely on documentation, statements or representations that meet the applicable requirements. For example, for disclosures of PHI made pursuant to a subpoena (see PP-08), Addus may rely on the subpoena for verification of the authority of the person requesting the PHI under the subpoena.

4. Documentation. Any authorizations, documents, statements or representations received as required by this Policy should be retained in the individual's medical record. Addus should retain copies of documents relied upon in order to verify a requestor's identity or authority. This documentation should be maintained in accordance with PP-19.

Addus HomeCare Privacy Policies		
Policy No: PP-10	Effective Date: 07/01/2017	
Pages: 2	Revision No. N/A	Date Reviewed: 08/23/2022

PERSONAL REPRESENTATIVES

1. In General. In general, Addus shall treat a personal representative of an individual as the individual for purposes of these Privacy Policies.

2. Deceased Individuals. The requirements of this Policy and all Privacy Policies apply to the PHI of all living and deceased individuals until the individual has been deceased for 50 years. If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or the individual's estate, Addus shall treat such person as a personal representative with respect to PHI relevant to such personal representation.

3. Adults and Emancipated Minors. If under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, Addus shall treat such person as a personal representative with respect to PHI relevant to such personal representation. For example, a person may be authorized under a health care power of attorney to make health care decisions.

4. Unemancipated Minors. If under applicable law, a parent, guardian, or other person has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, Addus must treat such person as a personal representative with respect to PHI relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor if:

4.1 The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

4.2 The minor may lawfully obtain such health care service without the consent of the personal representative and consents to the health care service (e.g. minors can consent to HIV testing); or

4.3 The personal representative assents to an agreement of confidentiality between Addus and the minor.

5. Exceptions. Addus may elect not to treat a person as a personal representative if:

5.1 Addus has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or treating such person as the personal representative could endanger the individual; and

5.2 Addus, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

6. Verification. Before recognizing a person as a personal representative, Addus must verify the person's identity and authority to act as a personal representative in compliance

with PP-09. For example, Addus may request to see an individual's identity to verify identity and request a copy of a court order appointing such individuals as the individual's guardian.

7. Documentation. Addus will also retain copies of all items required to be documented pursuant to this Policy as described in PP-19.

SAFEGUARDS

1. In General. Addus will maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and accessibility of PHI consistent with the requirements of these HIPAA Policies and to safeguard PHI from intentional and unintentional non-permissible uses and disclosures. These safeguards will supplement and be consistent with security measures taken by Addus for EPHI (see PP-21 through #HIPAA-32).

2. General Safeguards. Addus' internal safeguards will include the following:

2.1 Addus will restrict access to files containing PHI to only workforce members of Addus.

2.2 Addus will store files containing PHI in a secure location when not in use (i.e, locked room or file cabinet).

2.3 Addus will use reasonable safeguards so that PHI on computer screens will not be visible to unauthorized persons, including locking down computer workstations when not in use or when leaving the workstation by activating a password protected screen saver and clearing PHI from the computer screen when the PHI is not actually being used.

2.4 Addus will keep firewalls in place to protect EPHI.

2.5 Addus will keep a Virtual Private Network (VPN) in place to protect EPHI.

2.6 Prior to discarding PHI, Addus will securely destroy PHI by, among other things, shredding documents or destroying hardware that contain PHI so that they cannot be read or reconstructed.

2.7 Addus will not hold phone conversations or other discussions in areas where unauthorized persons may overhear. Phone conversations involving PHI should not be held on speakerphone, unless everyone within listening distance is an authorized recipient of the PHI.

2.8 Addus will mark documents containing PHI that are delivered by mail or hand delivery as "confidential."

3. Facsimile Safeguards. Addus will take reasonable steps to send and receive facsimile transmissions securely, including the following safeguards:

3.1 Only sending PHI by fax when mail, encrypted e-mail or hand delivery are not feasible.

3.2 Notifying the recipient and double checking fax numbers before dialing.

3.3 Using Addus' standardized fax cover sheet that includes a confidentiality statement and a request that any erroneous recipient destroy or return the fax.

3.4 Picking up incoming faxes from the fax machine in a timely manner.

3.5 When sending a fax, remaining at the fax machine until the fax has been scanned completely and not using a fax machine that is accessible to the public.

3.6 Not leaving faxes to be sent or that have been sent at the fax machine unattended.

3.7 If aware of a misdirected fax, contacting the recipient and asking them to discard the misdirected fax (and reporting the incident immediately to the Privacy Officer).

3.8 Locating fax machines in secure areas not accessible to the general public or unauthorized staff.

4. E-mail Safeguards. Addus will only send PHI by e-mail securely by following these safeguards: (i) only send the minimum necessary PHI via e-mail; (ii) protect the email by encryption if emailed outside of Addus' network; and (iii) attach an email signature block stating the following:

> NOTICE: This email may contain PRIVILEGED and CONFIDENTIAL information and is intended only for the use of the specific individual(s) to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any unauthorized use, dissemination or copying of this email or the information contained in it or attached to it is strictly prohibited. You may be subject to penalties under law for any improper use or further disclosure of any Protected Health Information in this email. If you have received this email in error, please delete it and immediately notify the sender of this email by reply mail. Thank you.

Any Addus workforce member who becomes aware of a misdirected e-mail that contains PHI must notify the Privacy Officer immediately.

RESTRICTIONS ON DISCLOSURES AND CONFIDENTIAL COMMUNICATIONS

1. Right to Request Additional Privacy Restrictions and Confidential Communication. An individual has the right to request additional privacy restrictions with respect to the individual's PHI. An individual may request that Addus restrict uses or disclosures of the individual's PHI to carry out treatment, payment or healthcare operations and disclosures to family members of the individual and close personal friends of the individual as set forth in PP-04.

2. Exceptions. A restriction agreed to by Addus is not effective to prevent permitted or required uses or disclosures:

2.1 to the Secretary for purposes of investigating or determining Addus' compliance with the HIPAA Rules;

2.2 for facility directories; and

2.3 for which an authorization is not required pursuant to these HIPAA Policies.

3. Out of Pocket Requests. Addus is not required to agree to a restriction on disclosures, except for disclosures to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and which the individual, or a person other than the health plan, has paid in full out of pocket. Addus will not use or disclose PHI in violation of any agreed-to restrictions, except in the case of an emergency. If restricted PHI is necessary to provide emergency treatment, the restricted PHI may be disclosed only to a health care provider for purposes of providing such treatment and Addus must request that such health care provider not further use or disclose the information.

4. Termination. Addus may terminate a restriction on disclosures if:

4.1 The individual agrees to or requests the termination in writing;

4.2 The individual orally agrees to the termination and Addus documents the oral agreement; or

4.3 Addus informs the individual that it is terminating its agreement to a restriction, except that such termination is (a) not effective for PHI restricted under subsection 2 above, only effective with respect to PHI created or received after Addus has notified the individual of the termination.

5. Individual's Request for Confidential Communications.

5.1 Addus will accommodate an individual's reasonable request for "confidential communications" A "confidential communications"

request is a request by an individual that Addus communicate PHI to the individual by alternative means or at alternative locations.

5.2 Addus may condition its accommodation of the individual's request on the following: (i) whether the individual has made acceptable arrangements for billing, when appropriate; and (ii) whether the individual has provided an alternative address or other acceptable alternative means of communication.

5.3 Addus will not require the individual to provide an explanation as to the basis for the request as a condition of providing communications on a confidential basis.

5.4 An individual may make a request for additional privacy restrictions or confidential communications by submitting a written request to the Privacy Officer.

5.5 Any requests for restriction or confidential communications received by a workforce member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the request in compliance with the HIPAA Rules.

6. Documentation. Addus must document (i) requests for restrictions, (ii) acceptance or denial of a restriction, and (iii) any termination of a restriction, and retain such documentation in accordance with PP-19. Addus must document an accepted request for confidential communications in the individual's record so that workforce members will be made aware of the request, and must maintain any request for confidential communications, along with Addus' response, in accordance with PP-19.

RECORDING AND ACCOUNTING OF DISCLOSURES OF PHI

1. In General. Subject to certain exceptions, the HIPAA Rules give individuals the right to receive an accounting (a list) of disclosures of PHI that has been disclosed by Addus or its Business Associate(s) for certain purposes.

2. Exceptions. Addus is not required to provide an accounting for disclosures of PHI:

2.1 for treatment, payment or health care operations as defined in PP-03 (subject to a carve-out for disclosures made from an electronic health record as described in regulations to be issued at a later date by HHS);

2.2 to the individual or the individual's representative;

2.3 pursuant to an individual's or personal representative's authorization (See PP-03, Section 5);

2.4 incident to a use or disclosure that is otherwise permitted or required under the HIPAA Rules (See PP-03, Section 4.3);

2.5 for use in a Covered Entity's facility directory;

2.6 to a family member, other relative, or close personal friend who is involved with the individual's care in compliance with PP-04;

2.7 for national security or intelligence purposes (See PP-03, Section 4.1);

2.8 as part of a Limited Data Set as described in PP-03; or

2.9 made more than 6 years before the request.

3. Disclosures Required to be Recorded. The accounting of disclosures must include non-permissible disclosures of PHI by Addus that are known to Addus, as well as disclosures by Business Associates of Addus.

Note: The above list of recordable disclosures does not mean these disclosures *should* be made. Any disclosure of PHI must comply with these Privacy Policies.

In addition to the types of disclosures required to be included in an accounting, once HHS issues regulations, Addus will be potentially required to record uses and disclosures made by Addus from an electronic health record (and potentially other electronic PHI). These Privacy Policies will be modified to address this requirement when the final rules are published.

4. Information Required to be Recorded. For any disclosures that must be recorded pursuant to this Policy, Addus will record the following information (including the individual's name with unique identifier):

4.1 The date of the disclosure;

4.2 The name of the entity or person who received the PHI and, if known, the address of such entity or person;

4.3 A brief description of the PHI disclosed; and

4.4 A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or in lieu of such statement, a copy of a written request for a disclosure.

If Addus has made multiple disclosures of PHI to the same individual or entity during the period for which the accounting is requested, Addus may, with respect to such multiple disclosures, provide the information set forth above with respect to the first disclosure, describe the frequency or number of the disclosures made during the accounting period, and the date of the last disclosure. Special rules apply to disclosures for research purposes, which the Privacy Officer will follow if applicable.

5. Suspension of the Accounting Right. Addus must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by the agency or official, if the agency provides Addus with a written statement that indicates an accounting to the individual would be reasonably likely to impede the agency's activities and the written notice specifies the time for which a suspension is required. If the agency or official statement is made orally, Addus must: (i) document the statement, including the identity of the agency or official making the statement; (ii) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (iii) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement as describe above is submitted during that time.

6. Documentation. The Privacy Officer will maintain a log of any disclosures required to be recorded under this Policy as described in PP-19. Addus will maintain the written accounting provided to the individual in the medical record and the individual's written request for the accounting for 6 years from the date such records were created, consistent with PP-19 unless state specifies otherwise.

7. Provision of the Accounting. Addus will act on an individual's request for an accounting of disclosures within 60 days after receipt of the request or other period required by the HIPAA Rules if shorter. If Addus is unable to provide the accounting within 60 days of receiving the request, Addus may extend the time to provide the accounting by an additional 30 days (for a total response time of 90 days), provided Addus notifies the individual in writing of the reasons for the delay and the date by which Addus will provide the accounting.

Addus will provide the first accounting to an individual in any 12-month period without charge. Addus may impose a reasonable, cost-based fee for each subsequent request for an accounting made by the same individual within a single 12 month period; provided, however, Addus will notify the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request.

8. Other Documentation. Addus will document and retain the following for a period of at least 6 years, or from the date of its creation or the date when it last was in effect, whichever is later as described in PP-19:

8.1 Information required to be documented pursuant to this Policy;

8.2 Copies of any accounting information provided to the individual; and

8.3 The title of the persons or officer responsible for receiving and processing requests for an accounting (see below).

9. Privacy Officer. The Privacy Officer or his/her designee is responsible for responding to a request for an accounting of disclosures. Any Addus workforce member who receives a request for an accounting from an individual must forward the request immediately to the Privacy Officer to handle in compliance with this Policy.

Addus HomeCare Privacy Policies		
Policy No: PP-14	Effective Date: 07/01/2017	
Pages: 5	Revision No. N/A	Date Reviewed: 08/23/2022

ACCESS TO AND AMENDMENT OF PHI

Right to Access PHI

1. In General. Individuals have a right to inspect and copy their PHI that is a Designated Record Set, for as long as the PHI is maintained in the Designated Record Set by a Covered Entity. However, the right of access does not apply to psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a legal proceeding. Any requests for access received by a workforce member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the access request in compliance with the HIPAA Rules.

1.1 In order to request access to the individual's PHI, the individual must make a written request and indicate how the PHI should be delivered. Addus will provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format. If such form or format is not readily available, another readable, hard copy form will be provided to the individual. However, if the individual requests an electronic copy of PHI that is maintained in a Designated Record Set electronically, Addus will provide the individual with access to the PHI in the electronic form and format requested by the individual, or if the PHI is not readily producible in the requested form or format, in a readable electronic form and format agreed to by Addus and the individual.

1.2 Addus may provide a summary of the PHI in lieu of providing access, or may provide an explanation of the information to which access has been provided, if the individual agrees in advance to such a summary or explanation and the individual agrees in advance to the fees associated with providing such summary or explanation.

1.3 Addus may impose a reasonable, cost-based fee for copying PHI or preparing a summary or explanation of the information. The fee will include only the cost of copying (including the cost of supplies for, and labor of, copying), postage, when applicable, and the cost of preparing an explanation or summary of the PHI if a summary or explanation has been agreed to by the individual.

2. Denial of Access Requests.

2.1 Access requests will be granted unless a ground for denial permitted by the HIPAA Rules applies to the requested PHI. In the event Addus denies an individual access to the individual's PHI, Addus will provide a written denial to the individual within the time frame set forth below. The written denial will include a basis for the denial; a statement detailing the individual's review rights; a statement as to how the individual may exercise

such review rights; and a description of how the individual may file a complaint with Addus or with HHS.

2.2 The Privacy Officer will determine whether any exceptions listed above to the right to review apply (psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a legal proceeding). The individual does not have a right to have a denial of access based on these exceptions reviewed.

2.3 In addition, Addus may deny access in the following situations, provided that the individual is provided with an opportunity for a review of the denial:

(a) a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(b) the PHI makes reference to another person other than a healthcare provider, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(c) the request for access is made by an individual's personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

2.4 If the individual requests a review of a denial made based on one of the above reviewable reasons, the denial will be reviewed by a licensed healthcare professional who is designated by Addus and who did not participate in the original denial decision. Addus will abide by the determination of the reviewing licensed healthcare professional.

3. Timing. Addus will act on an individual's request for access no later than 30 days after receiving the request if the PHI requested is maintained by Addus on-site. Addus may be permitted to extend the time for acting on the request by 30 days, provided Addus provides the individual with a written statement detailing the reasons for the delay and the date by which Addus will complete its action on the request.

4. Transmission of PHI to Third Party. If the individual's request for access directs Addus to transmit the copy of PHI directly to another person,

4.1 Addus will provide the copy to the person designated by the individual, provided that the request is in writing, is signed by the individual and clearly identifies the recipient and where to send the PHI. PP-03 addresses requirements for a compliant authorization to use or disclose PHI. A request for access by an individual does not have to meet all of the requirements for a compliant authorization.

4.2 If an individual requests PHI to be sent to a third party (without including an authorization that includes the elements set forth at PP-03) the Privacy Officer will be consulted regarding whether additional documentation is required before responding to the request (i.e. does the request require an authorization? Should Addus confirm with the individual that he or she is exercising his or her access rights?).

4.3 Requests for PHI provided to Addus by third parties (anyone besides the individual or the individual's personal representative) must meet the requirements set forth in PP-03, unless Addus has confirmed that the individual is attempting to exercise his or her access rights. For example, Addus may confirm with the individual who is the subject of the PHI that he or she is exercising his or her access rights or it may be apparent from the wording of the request that the third party is delivering an access request on behalf of the individual who is the subject of the information (as opposed to the third party requesting a disclosure). When in doubt, the Privacy Officer will consult with legal counsel.

5. Documentation. Addus will document and retain for 6 years from the date of its creation the Designated Record Sets subject to access and title of Addus workforce members responsible for receiving and processing such requests (the Privacy Officer) as described in PP-19.

Right to Amend PHI.

1. In general. An individual may request Addus to amend PHI contained in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. An individual may request such an amendment by submitting a written request to the Privacy Officer.

1.1 Any requests for amendment received by workforce member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the amendment request in compliance with the HIPAA Rules. Addus will act on the individual's request for an amendment no later than 60 days after receiving such a request. If Addus is unable to act on the amendment within 60 days, Addus may extend the time for action by no more than 30 days, provided Addus provides the individual with a written statement of the reasons for the delay and the date by which Addus will complete its action on the request.

1.2 In the event Addus accepts the requested amendment, in whole or in part, Addus will:

(a) make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

(b) timely inform the individual that the amendment is accepted and obtain the individual's identification of an agreement to have Addus notify relevant parties of the amendment; and

(c) make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as having received PHI about the individual and needing the amendment, and/or persons, including Business Associates, that maintain PHI that is subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

2. Denial of Request for Amendment. Addus may deny an individual's request for amendment if it determines that:

2.1 the PHI record that is the subject of the request was not created by Addus, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

2.2 the information is not part of the Designated Record Set;

2.3 the information is not available for access under the HIPAA Rules; or

2.4 the information is accurate and complete.

3. Written Denial to Individual. In the event Addus denies the amendment request, in whole or in part, Addus will provide the individual with a written denial that sets forth the basis for the denial; the individual's right to submit a written statement disagreeing with the denial; a statement explaining how the individual may file such a statement; and a statement informing the individual that if the individual does not submit a statement of disagreement, the individual may request that Addus provide the individual's request for amendment and Addus' written denial with any future disclosures of the PHI that is the subject of the request. Addus' written denial will also include a description of how the individual may file a complaint with the Privacy Officer or HHS.

4. Written Rebuttals. If the individual submits a statement of disagreement, Addus may prepare a written rebuttal to a statement of disagreement filed by an individual. Whenever Addus prepares a rebuttal, Addus will provide a copy to the individual who submitted the statement of disagreement. If a statement of disagreement has been submitted by an individual, Addus will include the material appended or, at the election of Addus, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates. If the individual has not submitted a written statement of disagreement, Addus will include the individual's request for amendment and Addus' written denial, or an accurate summary of the information with any subsequent disclosure of the PHI, only if the individual has requested such action. If the individual has requested that the information be included with any subsequent disclosure, and it is not possible to include the additional material with the disclosure, Addus may separately transmit the material to the recipient of the PHI.

5. Amendments Granted by Another Covered Entity. If Addus is informed by another Covered Entity under the HIPAA Rules of an amendment to an individual's PHI, Addus will amend the PHI accordingly in Designated Record Sets maintained by Addus.

6. Documentation. Addus must document and retain the titles of those responsible for receiving and processing amendment requests (the Privacy Officer) and documentation created pursuant to this Section 2 (i.e. amendment requests and responses) as described in PP-19.

Addus HomeCare Privacy Policies		
Policy No: PP-15	Effective Date: 07/01/2017	
Pages: 1	Revision No. N/A	Date Reviewed: 08/23/2022

RIGHT TO RECEIVE A PRIVACY NOTICE

1. In General. An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the Covered Entity, and of the individual's rights and the Covered Entity's legal duties with respect to PHI ("Notice of Privacy Practices"). Addus will provide the Notice of Privacy Practices to any individual upon request (whether or not the individual is a patient). In addition, Addus will provide the Notice of Privacy Practices to individuals no later than the first date of service delivery or, in the case of emergency treatment, as soon as reasonably practicable after the individual has been treated.

2. Written Acknowledgement. Except in emergency situations, Addus will make a good faith effort to obtain a written acknowledgment from the individual or the individual's representative of receipt of the Notice of Privacy Practices, and if not obtained, document the attempts and the reason why acknowledgement was not obtained. Addus has developed an "acknowledgment of receipt of Notice of Privacy Practices" form as part of its consent form and, wherever possible, this form should be presented to individuals for obtaining and documenting their acknowledgment of receipt of the notice.

3. Availability of Notice of Privacy Practices. Addus will have the Notice of Privacy Practices available in its office(s) for individuals to take with them and will also post the Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect that individuals will be able to read the notice. Addus will prominently post its Notice of Privacy Practices on its website so that it is available electronically through its website.

4. Revisions of Notice of Privacy Practices. Addus must promptly revise and make available its Notice of Privacy Practices whenever there is a material change to the uses or disclosures, the individual's rights, Addus' legal duties or other privacy practices stated in the Notice of Privacy Practices. Except where required by law, a material change to the Notice of Privacy Practices will not be implemented before the effective date of the publication of the Notice of Privacy Practices.

5. Electronic Copy. Addus may provide an individual with an electronic copy of the Notice of Privacy Practices, provided the individual agrees to accept an electronic copy. If Addus becomes aware that the transmission of the electronic Notice of Privacy Practices has failed, Addus will mail a paper copy to the individual. An individual is entitled to receive a paper copy of the Notice of Privacy Practices upon request, even if the individual has previously agreed to accept an electronic copy.

6. Documentation. Addus must retain copies of all versions of the Notice of Privacy Practices issued by Addus, along with any written acknowledgements of individuals' receipt of the Notice of Privacy Practices, as described in PP-19.

Addus HomeCare Privacy Policies		
Policy No: PP-16	Effective Date: 07/01/2017	
Pages: 2	Revision No. N/A	Date Reviewed: 08/23/2022

PRIVACY INCIDENTS AND COMPLAINTS

1. In General. An individual may make a complaint regarding the privacy or security of PHI, and Addus will request that a complaint be made in writing. Any Addus workforce member who knows of, suspects, or has received a report from any individual, Business Associate or other Addus workforce member of, a violation of these Privacy Policies, including any non-permitted use or disclosure of PHI, must notify the Privacy Officer immediately. When in doubt on who must receive the report, the workforce member should report the potential violation to the Privacy Officer who will coordinate with the Security Officer. The Privacy Officer will oversee the review of and response to any potential violation of these Privacy Policies, including complaints from individuals.

2. No Waiver or Retaliation. As set forth in PP-01, Section 2, Addus will not require individuals to waive their rights under the HIPAA Rules or their rights to file complaints regarding compliance with the HIPAA Rules. Addus will not intimidate, threaten, coerce or engage in any other form of retaliation against a person who exercises any rights under the HIPAA Rules, reports an incident or complaint under this Policy, reports an incident to HHS or assists in any HHS proceeding or compliance review regarding the HIPAA Rules.

Any manager, supervisor or workforce member who engages in any form of retaliation is subject to discipline up to and including dismissal.

If any workforce member reports a concern regarding the workforce member's own inappropriate or inadequate actions, the report does not exempt the workforce member from the consequences of those actions. However, prompt and forthright disclosure of an error by a workforce member will be considered a positive constructive action.

3. Investigation and Mitigation. The Privacy Officer will oversee the prompt and appropriate investigation and resolution of any incidents or complaints reported under this Policy. The Privacy Officer will take reasonable and appropriate actions to mitigate any harm caused by any violations of the HIPAA Rules or these Privacy Policies by Addus, to the extent practicable. Appropriate mitigation steps will depend on the facts of the particular incident. Examples of mitigation steps include: (a) reporting a theft to the police; (b) requesting the recipient to return or destroy the PHI and certify in writing that the PHI and all copies of the PHI has been returned or destroyed; (c) deleting misdirected emails containing PHI; (d) changing passwords or other means of accessing systems or devices containing PHI; (e) adopting additional safeguards; (f) revising existing or adopting new policies and procedures; (g) providing additional training to affected workforce members; and (h) terminating a relationship with a Business Associate.

4. Other Policies or Required Actions. Addus will also take appropriate action under other applicable policies in response to any incident or complaint that is determined to constitute a violation of these Privacy Policies, including the following Policies, as applicable: Recording

and Accounting of Disclosures of PHI (PP-13), Breach Notification (PP-17) and Sanctions (PP-20).

5. Documentation. The Privacy Officer will document each reported incident and complaint and its resolution. This documentation will be maintained in compliance with PP-19.

BREACH NOTIFICATION

1. In General. All Addus workforce members must report any incidents believed or suspected to be breaches or non-permissible uses or disclosures of PHI to the Privacy Officer as soon as possible. The Privacy Officer will review any such incident to determine whether the incident constitutes a breach and/or whether the incident requires notification under these policies. The HIPAA breach notification requirements apply only to a breach of "unsecured" PHI, which is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. For example, if PHI is lost or stolen but is encrypted, the incident would not require notification under HIPAA.

2. Determining whether a breach has occurred. A breach is the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the PHI. Incidents that fall into one of the categories below are not required to be reported (unless state law requires a report). However, Addus' workforce members must always report to the Privacy Officer any incident believed to be a violation of the HIPAA Privacy and Security Manual so that the Privacy Officer can determine whether the incident is a breach and whether corrective actions or other measures should be taken in response to the incident.

2.1 Breach Exceptions. If any of the following exceptions apply, the incident is not a breach.

(a) Any unintentional acquisition, access, or use of PHI by Addus, workforce members or any individual acting under the authority of Addus or its Business Associate if:

i. the acquisition, access, or use was made in good faith and within the course and scope of authority; **and**

ii. the information is not further used or disclosed in a manner not permitted by HIPAA.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at Addus or its Business Associate to another person authorized to access PHI at Addus or the same Business Associate, if the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by HIPAA.

(c) A disclosure of PHI where Addus or its Business Associate has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is

incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office).

2.2 Unless an exception above applies, an acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA is *presumed* to be a breach unless Addus can demonstrate that there is a low probability that the PHI has been compromised. In order to make this determination, Addus will perform, and document the outcome of, a risk assessment taking into account at least the following factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

3. Timing of notification. If the Privacy Officer determines that a breach of unsecured PHI has occurred, the notification requirements below must be met. A breach of unsecured PHI shall be treated as "discovered" as of the first day on which such breach is known to Addus, or, by exercising reasonable diligence would have been known to Addus (includes breaches by Addus' Business Associates).

3.1 Each affected individual will be notified without unreasonable delay, but no longer than 60 days from the discovery of a breach. Addus will also comply with any applicable state law requirements that impose additional breach notification duties or more restrictive breach obligations (for example, state law may require a report to be made within a shorter period, that the notice letter contain specific wording not required by HIPAA, or that additional government agencies or other entities be notified).

3.2 If the breach involves more than 500 residents of a State or jurisdiction, Addus will notify prominent media outlets serving the State or jurisdiction without unreasonable delay, but no longer than 60 days from the discovery of a breach.

3.3 If the breach involves 500 or more individuals, Addus will notify the Department of Health and Human Services ("HHS") contemporaneously with the individual notice provided in Section 3(a), but no longer than 60 days from the discovery of a breach; or if the breach involves fewer than 500 individuals, Addus will maintain a log or other documentation of the breaches and, not later than 60 days after the end of each calendar year, notify HHS of the breaches.

3.4 Addus must delay notification to affected individuals of a breach if a law enforcement official states that notification would impede a criminal investigation or cause damage to national security as follows:

(a) if the law enforcement statement is in writing, Addus will delay the notification or posting for the time period specified in the statement; or

(b) if the law enforcement statement is made orally, Addus will delay the notification or posting for the time period requested or for 30 days, whichever time period is shorter. If the law enforcement official confirms an oral statement with a written request to delay notification or posting, Addus will delay the notification or posting for the time period specified in the written statement.

4. Content of notice.

4.1 Notification to affected individual(s) and the media (when required) will include:

(a) a brief description of what happened including the date of the breach and the date of the discovery of the breach;

(b) a description of the types of unsecured PHI that were involved in the breach;

(c) any steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) a brief description of what Addus is doing to investigate the breach and to mitigate harm to individuals; and

(e) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

4.2 Notification to individuals and the media must include any additional information required by state law if applicable.

4.3 Notification to HHS will include the items requested on HHS's website.

5. Method of notice.

5.1 Addus will notify affected individuals by first-class mail at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If Addus knows the individual is deceased and has the address of the next of kin or Personal Representative of the individual, Addus may provide such written notice to the next of kin or Personal Representative.

5.2 Substitute notice. If there is insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means. If there is insufficient or out-of-date contact information for 10 or more individuals, the substitute notice must (a) be in the form of either a

conspicuous posting for a period of 90 days on Addus' website or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside **and** (b) include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

6. Documentation of Breaches. Addus will maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. The following information will be collected/logged:

6.1 A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.

6.2 A description of the types of unsecured PHI that were involved in the breach (such as full name, social security numbers, date of birth, home address', account numbers, etc.)

6.3 A description of the action that will be taken in regards to notifying the individuals of the breach.

7. Incident reports, their resolution, assessments of harm and whether an incident was a breach, copies of notices provided to individuals, the media and HHS and all other information required to be kept by this policy will be documented and retained for a period of at least 6 years from the date of creation or the effective date of the document, whichever is later.

8. Other Policies. Consistent with the HIPAA Privacy Manual, Addus will: (a) train its workforce members on this policy; (b) accept complaints from individuals concerning its compliance with this policy; (c) implement sanctions for violations of this policy; (d) refrain from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for exercising his or her rights under this policy or any other aspect of the HIPAA Privacy Rules; and (e) not require individuals to waive their rights under this policy.

9. Addus as a Business Associate. When acting as a Business Associate, if Addus discovers an incident that is determined to be breach of unsecured PHI (consistent with the procedures outlined in this policy) held on behalf of a Covered Entity, Addus must notify the Covered Entity consistent with the terms of the applicable Business Associate Agreement, without unreasonable delay and not to exceed 60 days from discovery of the breach. The Privacy Officer will coordinate any communications with the Covered Entity. To the extent known, the notice will include the items set forth in Section 4(a) above.

Addus HomeCare Privacy Policies		
Policy No: PP-18	Effective Date: 07/01/2017	
Pages: 1	Revision No. N/A	Date Reviewed: 08/23/2022

WORKFORCE MEMBER TRAINING REGARDING HIPAA POLICIES

1. In General. All Addus workforce members will receive appropriate training regarding Privacy and Security Policies. Workforce members will be trained upon initial employment with Addus within a reasonable period of time after date of hire and on an as needed basis, including periodic updates (such as part of annual compliance training) and as necessary to address changes to Privacy and Security Policies and to improve compliance. Workforce members will receive additional training when Privacy or Security Policies are revised. The Privacy and Security Officer will oversee compliance with this Policy.

2. Documentation. Addus will maintain a record of all training materials and sessions regarding these Privacy Policies, in compliance with PP-19.

Addus HomeCare Privacy Policies		
Policy No: PP-19	Effective Date: 07/01/2017	
Pages: 1	Revision No. N/A	Date Reviewed: 08/23/2022

RECORD RETENTION

1. In General. Addus will maintain all documentation required to be made under these HIPAA Policies as listed in the company document retention policy.

2. Examples of Required Documentation. The following are examples of documentation that must be retained as specified in this Policy:

2.1 Business Associate Agreements;

2.2 Disclosures required to be recorded under PP-13;

2.3 Incidents or complaints and their resolution (PP-16);

2.4 Risk assessments and breach reports created under PP-17;

2.5 Training materials and documentation of the provision of training (PP- 18); and

2.6 These Privacy Policies.

3. Availability. Documentation created pursuant to these Privacy Policies will be available to appropriate Addus workforce members who need the documentation to perform their assigned duties. Copies of these Privacy Policies are available to all Addus workforce members. These Privacy Policies will be revised as necessary to comply with changes in the HIPAA Rules and applicable guidance.

4. Revisions/Updates. These Privacy Policies will be revised as necessary to comply with changes in the HIPAA Rules and applicable guidance. Addus may revise these Privacy Policies as necessary to improve compliance and as part of its mitigation efforts. Addus will provide training to affected workforce members in the event of material changes to these Privacy Policies consistent with PP-18.

Addus HomeCare Privacy Policies		
Policy No: PP-20	Effective Date: 07/01/2017	
Pages: 2	Revision No. N/A	Date Reviewed: 08/23/2022

SANCTIONS

1. In General. All Addus workforce members must comply with the policies and procedures of Addus. Addus will use appropriate sanctions against workforce members who fail to comply with these Privacy Policies.

2. Disciplinary Actions. The Privacy Officer and Human Resources, will review all reports of non-compliance and determine the severity of disciplinary actions necessary. Disciplinary actions may range from a verbal warning to termination and will be administered consistent with Addus' Human Resource policies. Factors that will impact the disciplinary action adopted include (a) whether the non-compliance was accidental, intentional, and/or malicious; (b) the scope of the violation, including the amount and types of PHI involved; (c) whether the individual has previous instances of non-compliance; and (d) whether the individual attempted to cover-up the violation, was forthcoming or tried to undermine the Privacy Officer's investigation. The unauthorized use or disclosure of PHI may also result in monetary penalties under HIPAA or other civil or criminal penalties.

3. Documentation. All sanctioning activities will be documented and retained by the Privacy Officer for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later, in compliance with PP-19.

4. Reports. Workforce members who become aware of a potential violation of these Privacy Policies must report the incident as set forth in PP-16. If the Privacy Officer is the subject of the incident report, the workforce member should report the incident to Human Resources or their supervisor simultaneously.

5. Exceptions. Addus will not apply disciplinary action to the extent the use or disclosure of PHI involves one of the following:

5.1 A whistleblower disclosure made in good faith to a health oversight agency or public health authority with respect to Addus' conduct or compliance with the law or to an attorney being retained to represent the person making the disclosure for purposes of determining the legal options of the whistleblower;

5.2 A limited disclosure by a victim of a crime to a law enforcement official, where the disclosure is about the suspected perpetrator of the criminal act and the information disclosed is limited to the information that may be disclosed to a law enforcement official under the HIPAA Rules;

5.3 Filing a complaint with Addus and/or HHS;

5.4 Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing concerning the HIPAA Rules;

5.5 Opposing any act or practice that is prohibited by the HIPAA Rules, provided that (i) the person has a good faith belief that Addus being opposed is unlawful; and (ii) the manner of opposition is reasonable and does not itself violate the HIPAA Rules.

6. Business Associates. If Addus becomes aware of any pattern of activity or practice of a Subcontractor that constitutes a material breach or violation of the BAA with the Business Associate (or the HIPAA Rules), Addus will take reasonable steps to cure the breach or end the violation by the Business Associate. If such steps are unsuccessful, Addus shall terminate the agreement between the parties. Any workforce member who becomes aware of a potential or actual breach of a BAA by a Business Associate or non-permitted use or disclosure of PHI by a Business Associate must immediately notify the Privacy Officer.

Addus HomeCare Privacy Policies		
Policy No: PP-21	Effective Date: 03/29/2017	
Pages: 2	Revision No. N/A	Date Reviewed: 08/23/2022

PHOTOGRAPHY AND VIDEO IMAGING

1. In General. To facilitate compliance with HIPAA and state privacy laws, Addus will take reasonable steps to protect clients from unauthorized photography, video surveillance, cell phone recordings, and other images.

2. Unauthorized Photography Prohibited. Workforce members will take reasonable steps to ensure clients are not photographed or recorded by Addus in an unauthorized manner. Workforce members are prohibited from photographing or recording clients or the client's family for personal use or for any purpose not permitted by this policy. This includes, but is not limited to, taking photographs or videos to share with friends and/or co-workers, to post on the internet using social media (*e.g.*, Facebook, Twitter), etc.

3. Circumstances when Photography/Video is Permissible. The following are specific instances when the use of video or photography is permissible:

3.1 Addus may use photography or video to record clients if specifically authorized by the client or client's legal representative (such as for marketing purposes) and if the workforce member receives written approval from the Privacy Officer prior to the recording. In addition to obtaining an authorization (see Policy No. PP-05), Addus will obtain an IP release prior to disclosing or further using any such recording of a client.

3.2 Addus may utilize photography or video to collect PHI for purposes of identification and client care and treatment. Informed consent (but not a HIPAA authorization) from the client or the client's legal representative is required before workforce members may photograph or video record a client for client care purposes. When photography or video is used for purposes of identification and/or to document client care and treatment, the resulting images are included in the client's record and appropriately labeled.

3.3 In cases of actual or suspected abuse and/or neglect, video surveillance or other photography by authorized Addus personnel may be used for medical documentation purposes. Addus will obtain consent for such use of photography or video, unless circumstances prevent obtaining such consent. (HIPAA authorization is not required.) Copies of images captured under these circumstances may be released to authorized representatives of an investigating agency and/or pursuant to a subpoena or court order. Addus shall comply with any state laws that are more restrictive than this policy with respect to the use of video or photography in such circumstances.

4. Photography by Patients, Family Members, and/or Patient's Visitors. Addus is not required to obtain consent from the client when the client is the subject of the photography or

video and such recording is performed by the client or the client's family members or visitors. Addus workforce members have the authority to instruct that the photography or video be discontinued if deemed necessary in the interest of patient care. Clients, family members, and/or visitors are not permitted to take photographs of or record *other* clients or workforce members without consent.

PRIVACY POLICIES AND PROCEDURES
EMPLOYEE ATTESTATION

By signing below, I certify that I have read and understand the Addus HomeCare Privacy Manual. I hereby acknowledge my obligation to abide by Addus HomeCare's Privacy Policies and Procedures.

I understand that violation and/or non-compliance with laws, regulations, standards, Addus HomeCare's policies and procedures, and Addus HomeCare's Privacy Policies and Procedures is grounds for immediate disciplinary action, up to and including termination of employment.

_____

Employee's Printed Name

_____

Employee's Signature

_____

Date