A.C.T. HOME CARE, INC.

BUSINESS ASSOCIATES POLICY

I. APPLICABILITY

All Departments/Units Involved with doing business (negotiating and entering into contracts) with Business Associates ("BAs") of Organization Name and BA Subcontractors.

II. PURPOSE

To establish guidelines for A.C.T. HOME CARE, INC. to identify those vendor/business relationships, which meet the HIPAA definition of a "business associate" and provide direction in establishing formalized business associate agreements. A.C.T. HOME CARE, INC. shall implement the required procedures and ensure documentation to establish satisfactory assurance of compliance.

III. DEFINITIONS

Business Associate (BA): A person who:

1. A person/entity that: On behalf of such covered entity or of an organized health care arrangement creates, receives, maintains or transmits protected health information for a function or activity regulated by this subchapter, including:

a. claims processing or administration

b. data analysis, processing or administration

c. utilization review

d. quality assurance

e. patient safety activities listed at 42 CFR 3.20

f. billing

g. benefit management

h. practice management

i. repricing

2. Provides services to or for such covered entity other than in the capacity of a member of the workforce of such covered entity

a. legal,

b. actuarial,

c. accounting,

d. consulting,

e. shredding

f. data aggregation,

g. management,

h. administrative,

1. accreditation, or

j. financial services

3. A covered entity may be a business associate of another covered entity.

4. Business associate now also includes:

• A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access· on a routine basis to such protected health information;

• A person that offers a personal health record to one or more individuals on behalf of a covered entity; and

• A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

Business Associate Agreement (BAA): Under the HIP AA Privacy and Security Rules, a required and legally binding agreement entered into by a covered entity and business associate that establishes permitted and required uses and disclosures ofprotected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. Attached as Exhibit A to this policy is a list of all of the regulatory mandates that must be included in a BA agreement.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI). Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

• Past, present or future physical or mental health or condition of an individual.

• The provision of health care to an individual.

• The past, present, or future payment for the provision of health care to an individual.

IV. POLICY

It is the policy of this organization to comply with the regulatory requirements governing Business Associates and their subcontractors. This organization shall be responsible for ensuring that appropriate Business Associate arrangements are identified, business associate contracts are entered into and maintained in a systematic way.

V. PROCEDURE

1. The organization shall determine who will be responsible for overseeing the management and compliance with business associates and their subcontractors. Responsibility may be delegated to: (a) Privacy Officer; (b) Security Officer and/or (c) HIPAA Privacy & Security Team. For purposes of this policy, the term "Privacy Officer" shall be used throughout to refer to such individual/(s) responsible.

2. The Privacy Officer shall work with the organization's departments/business units to identify and assess current and future business associate relationships. The organization may determine the need for BAA's through:

a) Mapping the flow of PHI and identifying where PHI is used or disclosed or created by external entities.

b) Reviewing contract management documents/software and identifying where PHI is disclosed to external entities.

c) Reviewing 1099 tax forms to identify vendors and then identify vendors with business arrangements where PHI is disclosed to external entities or used internally by vendor.

d) Assessing new vendor/business arrangements to determine if PHI will be used and/or disclosed.

The following criteria may assist in defining a business associate under HIPAA:

e) The vendor/business' staff members are not members of the organization's workforce.

f) The vendor/business' is doing something on behalf of the organization;

g) That "something" involves the use and/or disclosure of PHI.

h) Note that there are certain disclosures to vendors/businesses that do not require establishment of a BAA (see 45 CFR § 164.502(e) (I). These disclosures include:

i) Disclosures to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

ii) Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

iii) Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

3. Once the business associates have been identified, the Privacy Officer shall work with the organization's compliance officer to ensure that the Business Associate has not been excluded from Federal or State Health care Programs.

4. Once it has been identified that a BA arrangement exists, the Privacy Officer shall work with appropriate the department/business unit leader to formalize a Business Associate Agreement that shall be an addendum to the BA's service contract. Attached as Exhibit B is a the organization's BA Addendum that must be used for all service contracts however, the Privacy Officer shall work with the department/business unit leaders to customize the BA Agreement if needed.

5. The department/business unit leader shall provide the following information to "customize" the BAA:

a) The name and contact information of the BA.

b) A general description of the type of service being provided by the BA.

c) Permitted uses and disclosures as applicable to the arrangement.

d) The name of the organization's department/business unit and leader who established the BAA.

e) Date of establishment of the business associate relationship and BAA.

f) Name/signature line for the department/business unit leader or Privacy Officer.

g) Name/signature line for the business associate contact.

6. The privacy officer shall establish procedures to monitor the organization's business associates and ensure that BAs and their subcontractors are appropriately notifying the organization of any potential or actual breaches of pm as well as that the BA has appropriate policies and procedures and safeguards to protect PHI and ePHI.

7. VI. APPLICABLE FEDERAL REGULATIONS

• 45 CFR § 164.308(b) (1) -HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements

• 45 CFR §164.314 -HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements

• 45 CFR § 164.502(e)(I) -HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules -Disclosures to Business Associates

• 45 CFR §164.504 -HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

EXIHIBIT A: HIPAA Requirements for Business Associates

Privacy Rule Provisions 45 CFR § 164.504(e)(2):

a) Stated Purposes for Which Business Associate May Use or Disclose Protected Health Information: Business Associate is permitted to use and disclose Protected Health Information it creates or receives for or from the organization for the purposes as

described in the addendum. Business Associate may also use Protected Health Information it creates or receives for or from the organization as minimally necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities.

b) Limitations on Use and Disclosure of Protected Health Information: Business Associate agrees it shall not use or disclose, and shall ensure that its directors, officers, employees, contractors and agents do not use or disclose Protected Health Information for any purpose other than as expressly permitted by the BA Agreement, or required by law, or in any manner that would constitute a violation of the Privacy Standards if used by the organization.

i) The BAA may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate; and

ii) The BAA may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

c) Disclosure by Others: To the extent Business Associate is authorized by this Agreement to disclose Protected Health Information to a third party, Business Associate must obtain, prior to making any such disclosure, reasonable assurances from the third party that the Protected Health Information will be held confidential as provided pursuant to the Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Health Information, to the extent it has obtained knowledge of such breach.

d) Minimum Necessary: Business Associate shall disclose to its subcontractors, agents or other third parties, and request from the organization, only the minimum Protected Health Information necessary to performing or fulfilling a specific required or permitted function.

e) Safeguards Against Misuse of Information: Business Associate will establish and maintain all appropriate safeguards to prevent any use or disclosure of Protected Health

Information other than pursuant to the terms and conditions of the Agreement.

f) Reporting of Disclosures of Protected Health Information: Business Associate shall, within [0] days of discovery of any use or disclosure of Protected Health Information in violation of the Agreement, report any such use or disclosure to the organization.

g) Agreements by Third Parties: Business Associate shall enter into an agreement with any agent or subcontractor that will have access to Protected Health Information that is received from, or created or received by Business Associate on behalf of, the organization pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to Business Associate pursuant to the Agreement with respect to Protected Health Information.

h) Access to Information: Within [0] days of a request by the organization for access to Protected Health Information about an individual contained in a Designated Record Set, Business Associate shall make available to the organization the Protected Health Information it requests for so long as that information is maintained in the Designated Record Set. If any individual requests access to Protected Health Information about the individual directly from Business Associate, Business Associate shall make available and provide a right of access to the Protected Health Information to the individual, at the times and in the manner required by the Privacy Standards (see 45 C.P.R. § 164.524, or its successor as it may be amended from time to time). After receiving the request, Business Associate shall notify the organization within "0" days of such request.

i) Availability of Protected Health Information for Amendment: Business Associate agrees to make Protected Health Information available for amendment and to incorporate any such amendments in the Protected Health Information, at the times and in the manner required by the Privacy Standards (see 45 C.P.R. § 164.526, or its successor as it may be amended from time to time).

j) Accounting of Disclosures: Within [0] days of notice by the organization to Business Associate that it has received a request for an accounting of disclosures of Protected

Health Information regarding an individual during the six years prior to the date on which the accounting was requested, Business Associate shall make available to the organization such information as is in Business Associate's possession and is required for the organization to make the accounting required by the Privacy Standards (see 45 C.P.R. § 164.528, or its successor as it may be amended from time to time). At a minimum, Business Associate shall provide the organization with the following information: the date of the disclosure; the name of the entity or person who received the Protected Health Information, and, if known, the address of such entity or person; a brief description of the Protected Health Information disclosed; and a brief statement of the purpose of the disclosure which includes an explanation of the basis for the disclosure. If the request for an accounting is delivered directly to Business Associate, Business Associate shall within "0" days forward the request to the organization. The organization is responsible for preparing and delivering the accounting requested. Business Associate agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

k) Availability of Books and Records: Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, the organization available to the Secretary for purposes of determining the organization's and Business Associate's compliance with the Privacy Standards.

l) If the organization (covered entity) and the business associate are both governmental entities, additional implementation specifications must be addressed (See 45 CFR § 164.504(e)(3).

Security Rule Provisions (45 CFR § 164.314):

m) Implementation of Safeguards: Business associate agrees to implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, and transmits on behalf of the organization.

n) Agents and Subcontractors: Business associate agrees that any agent, including a

subcontractor, to which the business associate provides ePHI, agrees to implement reasonable and appropriate safeguards to protect the ePHI.

0) Security Incidents: Business associate agrees to report to the organization any security incident of which it becomes aware.

p) Termination: Business associate agreement authorizes termination of the contract by the organization, if the organization determines that the business associate has violated a material term of the contract.

q) If the organization chooses to terminate the arrangement with the business associate or the business associate chooses to terminate the arrangement with the organization, the agreement must be terminated as outlined in the provisions of the business associate agreement/addendum or contract.

r) Upon termination or expiration of the business arrangement between the BA and the organization, the BA shall either return or destroy all PHI received from the organization or created or received by BA on behalf of the organization that the BA still maintains in any form as outlined in the provisions of the business associate agreement/addendum or contract.

Other Provisions: (optional)

s) The organization may want to seek legal counsel guidance prior to entering into a BAA that includes language addressing:

i) Insurance responsibilities.

ii) Indemnification requirements.

8. The organization must respond to reported privacy breaches and security incident events should they occur and take reasonable steps to cure any potential breach or end the violation. Confirm that first sentence is true and its source

9. The organization may serve as a BA to another covered entity and may be asked to review and sign that covered entity's external BA agreement/addendum or contract. As a BA, the organization should:

a) Forward the external information to the Privacy Officer1to review the submitted BA agreement to ensure that the provisions outlined are consistent with those set forth in this

policy or as documented on the attached (See Addendum 2).

b) If the BA agreement is not consistent with this policy or contains additional provisions or provisions that are inconsistent with the privacy regulation, the Privacy Officer may recommend to the following alternatives.

(1) Agree to the additional provisions and sign the agreement.

(2) Refer the agreement to legal counsel to determine appropriateness before signing.

(3) Refuse to agree

to the provisions and notify the covered entity to establish a

resolution.

10. To meet the documentation requirements of the Security Rule, the responsible individual/team shall maintain a file/electronic spreadsheet business associate agreements/addendums/contracts. This file shall include the following information, and shall be available for review as needed:

a) Date BAA need identified/received by responsible individual/team.

b) Name of Individual/organization which forwarded the agreement/identified need.

c) Name of organization for which BAA is needed.

d) Description of organization's operations that the BA is involved with.

e) Initiation date of original contract (if applicable).

f) Term of contract.

g) Date BAA signed by responsible individual.

h) Location of BAA.

i) Any additional notes.

11 . All BAA documentation shall be maintained for a period of six years beyond the date of when the BAA relationship is terminated.

12. The BAA shall be effective for the length of the relationship between the BA and the organization, unless otherwise terminated under the provisions outlined in the agreement.

---

1 The Privacy Officer may wish to involve the Security Officer, legal counsel, or other Administrative leaders in this process.