SMG Operating Company, LLC

and

Advanced Medical Management, Inc.

HIPAA Business Associate Privacy and Security Policy

As amended August 28, 2024

TABLE OF CONTENTS

SMG Operating Company, LLC and Advanced Medical Management, Inc.
HIPAA Business Associate Privacy and Security Policy

INTRODUCTION

This HIPAA Business Associate Privacy and Security Policy (the "Policy") has been adopted by each of SMG Operating Company, LLC, and Advanced Medical Management, Inc., a wholly owned subsidiary of SMG Operating Company, LLC. SMG Operating Company, LLC and Advanced Medical Management, Inc. are each referred to herein as the "Company".

The Health Insurance Portability and Accountability Act of 1996, including its regulations implementing certain privacy requirements (the "Privacy Rule"), certain breach notification requirements (the "Breach Notification Rule"), and certain security requirements regarding electronic media (the "Security Rule"), each as amended from time to time (collectively "HIPAA"). HIPAA imposes certain health information obligations, to the extent applicable, on the Company. These obligations concern the privacy and security of individually identifiable health information the Company receives in its capacity as a "Business Associate," as such term is defined under HIPAA. Generally, HIPAA restricts the Company's ability to use and disclose certain individually identifiable health information that is termed "protected health information" or "PHI."

Protected Health Information. For purposes of this Policy, protected health information means information that would be considered "protected health information" under the Privacy Rule, including information that is created or received by or on behalf of the Company in its capacity as a Business Associate of a Covered Entity and: (1) relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to these individuals; or the past, present, or future payment for the provision of health care to these individuals; *and* (2) that identifies these individuals, or for which there is a reasonable basis to believe the information can be used to identify these individuals. PHI includes information of persons living or who have been deceased for 50 years or less.

By way of background, HIPAA applies, in different ways, to "Covered Entities," as such term is defined under HIPAA, and to Business Associates (which HIPAA generally defines as a person or entity that performs certain functions or activities on behalf of a Covered Entity involving the use or disclosure of the Covered Entity's protected health information). If a Covered Entity, such as a health benefit plan or health care provider, engages a Business Associate (or a Business Associate engages a subcontractor Business Associate to help it provide such services), HIPAA has numerous requirements that apply to how the Business Associate may use or disclose that protected health information, and how the Business Associate must protect the privacy and security of that protected health information.

In particular, HIPAA requires the Covered Entity to have a written business associate contract or other arrangement with the Business Associate (a "Business Associate Agreement"), and that Business Associate Agreement must contain certain terms and conditions required under HIPAA. Also, if a Business Associate engages a subcontractor to perform certain functions or activities that involve the use or disclosure of protected health information of Covered Entities on behalf of the Business Associate, HIPAA also deems such subcontractor a Business Associate, and requires

the Business Associate that engages the subcontractor Business Associate to have a Business Associate Agreement with such subcontractor Business Associate.

In addition to these Business Associate Agreement contractual obligations, Business Associates are also directly responsible and liable for compliance with certain provisions of HIPAA, and so subject to direct enforcement actions by government authorities for noncompliance, such as regarding complying with the Security Rule, timely providing breach notifications to a Covered Entity or, as applicable, to another Business Associate under the Breach Notification Rule, and using and disclosing PHI in compliance with HIPAA. (*See* HHS Guidance – "Direct Liability of Business Associates").

This Policy describes the policies and procedures of the Company that are intended to comply with the HIPAA obligations found in its Business Associate Agreements, as well as in the provisions of HIPAA that directly regulate the Company as a Business Associate. For convenience, references in this Policy to HIPAA, the Privacy Rule, the Breach Notification Rule and the Security Rule are intended to incorporate Business Associate Agreement obligations of the Company that reflects these statutory and regulatory requirements.

Please note that not every Business Associate Agreement will contain the same rights and duties applicable to the Company regarding the use and disclosure of the PHI it addresses. For example, not every Business Associate Agreement will authorize the Company to de-identify PHI, to use and disclose PHI for the Company's proper management and administration (as distinguished from performing a function on behalf of the applicable Covered Entity), or to provide Data Aggregation services relating to the Health Care Operations of the Covered Entity (as such terms are defined under HIPAA). Also, unique timing, notice, and other requirements set forth in Business Associate Agreements may apply with respect to other matters covered under HIPAA, such as data breach notifications or responding to individual requests concerning access to PHI. In all cases, compliance is required with the specific terms and conditions of the applicable Business Associate Agreement. Workforce members must consult the Privacy Officer with any questions regarding the unique requirements of applicable Business Associate Agreements.

It is the Company's policy to comply fully with applicable HIPAA requirements. To that end, all members of the Company's workforce (the "Workforce") who have access to PHI to carry out their duties must comply with this Policy. For purposes of this Policy, the Workforce includes individuals who would be considered part of the Company's workforce under the Privacy Rule, such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company.

No third-party rights (including but not limited to rights of patients, clients or their family members, or subcontractors) are created by this Policy. Each Company independently reserves the right to adopt an alternative HIPAA Business Associate policy, and to amend or change this Policy as it applies to such Company at any time (and even retroactively) without notice.

The use of this same Policy by SMG Operating Company, LLC, and Advanced Medical Management, Inc., respectively, is for convenience, and any sharing of PHI between SMG Operating Company, LLC, and Advanced Medical Management, Inc. (e.g, regarding the

maintenance of records or otherwise) shall be pursuant to a basis permitted under HIPAA, such as pursuant to a subcontractor Business Associate Agreement.

To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy will be aspirational and will not be binding upon the Company, nor will it give rise to a violation of HIPAA. This Policy does not address requirements under other federal laws or under state laws, is not to be deemed to constitute a contract under any applicable law, and individuals may not bring a private cause of action based on this Policy.

In addition to this Policy, each Company maintains other policies that pertain to the privacy and security of personal information, including, but not limited to, health information. For any questions regarding these additional policies or this Policy please contact the Privacy Officer for SMG Operating Company, LLC, and Advanced Medical Management, Inc. by mail at SMG Companies, ATTN: Chief Compliance Officer, 5000 Airport Plaza Dr., Ste.150, Long Beach, CA 90815; or by email at CorporateCompliance@AMM.CC; or by telephone at 562-512-3752.

Part A of this Policy addresses the Privacy Rule and Breach Notification Rule.

Part B of this Policy addresses the Security Rule.

PART A.

HIPAA PRIVACY AND BREACH NOTIFICATION

I. Privacy and Security Officer and Contact Person

The Company has designated an officer to serve as the privacy officer under HIPAA. That individual is the Company's Privacy Officer. The same individual may serve as the Privacy Officer and as the Security Officer, as such term is defined in Part B of these Policies. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to the HIPAA Privacy Rule and Breach Notification Rule, including but not limited to as set forth in this Policy. The Privacy Officer will also serve as the Company's contact person who is responsible for receiving complaints regarding the Company's compliance with the Privacy Rule, the Breach Notification Rule, and this Policy, including, as applicable, providing further information about matters covered by Covered Entity Notices of Privacy Practices. Wherever this Policy refers to the Privacy Officer such reference will include any person delegated by the Privacy Officer, whether such delegation is oral or written.

II. Workforce Training

A. Policy

The Privacy Officer is charged with developing training schedules and programs so that all Workforce members receive the training necessary and appropriate to permit them to carry out their functions for the Company.

B. Procedures

(i) All current Workforce members shall be trained regarding the Privacy Rule, the Breach Notification Rule, and applicable procedures;

(ii) All new Workforce members will be trained within a reasonable time after joining the Workforce;

(iii) If this Policy is materially changed, the Privacy Officer will perform a new training session for the Workforce members whose functions are affected by a material change in this Policy or the Privacy Rule or Breach Notification Rule within a reasonable time after the new Policy takes effect.

(iv) The Privacy Officer shall document that all training has been provided as required (such as through training rosters that show training dates, the subject of the training, and the names of attendees) in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

III. Administrative, Technical and Physical Safeguards

A. Policy

The Company has established and shall implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. This shall include that the Company shall reasonably safeguard PHI from any intentional or unintentional use or disclosure of PHI that violates the Privacy Rule's requirements and shall reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

B. Procedures

Following are examples of specific procedures for protecting PHI, which shall be reasonably tailored as needed (in compliance with HIPAA), and in accordance with other Company information technology policies, for applicable circumstances:

(i) While working on a document or file, take reasonable measures to prevent others from viewing it, such as keeping documents containing PHI inside folders or face down;

(ii) When Workforce members are away from their workstations during the day, such as breaks and lunch, appropriately secure PHI, such as in a drawer;

(iii) Reasonably limit the number of photocopies of PHI;

(iv) Follow office policies regarding encryption or other protections regarding e-mails or mobile devices containing PHI;

(v) Before speaking to any client or patient about his or her PHI, Workforce members must verify the individual's identity in accordance "Verification of Identity of Those Requesting PHI" in Part A, Section XXIII of this Policy;

(vi) When on the telephone, take reasonable measures to prevent others from overhearing conversations regarding PHI;

(vii) Properly secure documents and files containing PHI in office premises;

(viii) Properly secure documents with PHI information, which are distributed internally, such as in properly sealed envelopes;

(ix) Shred papers containing PHI in accordance with Company policy;

(x) Follow appropriate password security; e.g., maintaining the confidentiality of passwords;

(xi) Appropriately secure computers when a Workforce member leaves the workstation; and

(xii) Reasonable steps must be taken to avoid exposing unauthorized persons to PHI.

IV. Disclosures of PHI - With Authorization

A. Policy

The Company may make disclosures of PHI not otherwise permitted under the Privacy Rule when properly authorized, in writing, by the individual whose PHI will be disclosed (or by the personal representative of the individual). Generally, PHI may be disclosed for any purpose if an authorization that satisfies all of the Privacy Rule's requirements for a valid authorization is provided. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

In accordance with Part A, Section IV of this Policy, in no event will the Company use or disclose PHI that is "genetic information" for "underwriting" purposes, and no authorization can be relied on to permit such use or disclosure of PHI.

In accordance with the Privacy Rule, in no event will the Company use or disclose PHI for paid marketing activities or sell PHI without a valid authorization (unless expressly permitted by the Privacy Rule), and any such authorization must be tailored to state that remuneration is involved and otherwise satisfy HIPAA requirements. In the event a Workforce member knows or suspects that any arrangement involving the Company, or a Business Associate of the Company, includes or will include any sale of PHI, or involves or will involve payments or other remuneration to promote items or services using PHI, the Workforce member must immediately notify the Privacy Officer.

B. Procedures

Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required may be made pursuant to an individual authorization. In addition, except for certain narrow exceptions permitted by law (such as legal defense), the Company, in compliance with the Privacy Rule, will not use or disclose PHI that is a mental health professional's psychotherapy notes (discrete notes that document the contents of conversation during counseling sessions) without prior authorization, and will not use or disclose PHI for any paid marketing activities, or sell PHI without prior authorization.

If an authorization is requested, the following procedures will be followed:

(i) Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting PHI" (Part A, Section XXIII);

(ii) Prior to any use or disclosure of information pursuant to an authorization, the Privacy Officer shall verify that the authorization form is valid in accordance with the Privacy Rule. Generally, valid authorization forms are those that:

(a) Are properly signed and dated by the individual or the individual's representative;

(b) Are not expired or revoked. The expiration date of the authorization form must be a specific date or a specific time period (*e.g.*, one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure;

(c) Contain a description of the information to be used or disclosed;

(d) Contain the name of the entity or person authorized to use or disclose the PHI;

(e) Contain the name of the recipient of the use or disclosure;

(f) Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and

(g) Contain a statement regarding the possibility for a subsequent re-disclosure of the information.

(iii) A copy of the authorization should be provided to the authorizing individual unless the individual indicates on the authorization form that he/she does not want a copy;

(iv) All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization;

(v) A copy of each verified and signed authorization shall be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII);

(vi) If the authorization is revoked or expired, subsequent uses and disclosures only permitted by an authorization should cease until a new authorization is executed.

V. Disclosure Requests for PHI From Spouses, Domestic Partners, Family Members, and Friends

A. Policy

The Company intends to protect the privacy of an individual's PHI by disclosing it only as permitted under the Policy or the Privacy Rule or as otherwise authorized.

Workforce members may not disclose PHI to family and friends of an individual except as required or permitted by the Privacy Rule, and in many cases an authorization is required before another party, including spouse, family member or friend, will be able to access PHI. However, in certain cases, in accordance with the Privacy Rule, this Policy permits and, in some cases, requires, an individual's PHI to be disclosed to such persons without an authorization.

B. Procedures

Disclosures may be made to the spouse, domestic partner, relative, friend or other person identified by the individual in the following four circumstances, to the extent permitted by the Privacy Rule. Workforce members should consult with the Privacy Officer with any questions regarding specific requests:

(i) Subject to certain safeguards, including certain requirements of applicable state and other laws, disclosures must be made to the parent of a minor child or to someone who is the authorized personal representative of the individual (in accordance with state or other applicable law). These persons, if authorized to access PHI on this basis, are generally treated as standing in the shoes of the individual whose PHI is maintained by the Company. If a Workforce member receives a request for disclosure of an individual's PHI and the person requesting the information is either (1) the parent of the individual and the individual is a minor child; or (2) the authorized personal representative of the individual, then the Workforce member should follow the procedure for "Verification of Identity of Those Requesting PHI" (Section XXIII). Once the identity of a parent or authorized personal representative is verified, then follow the procedure for "Access to PHI and Requests for Copies or Amendment" (Part A, Section XII);

(ii) If the individual whose PHI is maintained by the Company is present and consents, or is provided with the opportunity to object and does not express an objection, or the Workforce member reasonably infers from the circumstances - based on the exercise of professional judgment - that the individual does not object to the disclosure (and there is no known prior objection by the individual to the disclosure), then the Workforce member may disclose to the individual's spouse, domestic partner, family member or close friend, PHI that is directly relevant to that person's involvement with the individual's health care or payment related to the individual's health care. For example, if the individual calls a Workforce member with another person on the telephone and asks the Workforce member to discuss his or her PHI with the other person, the Workforce member may discuss such PHI with the other person;

(iii) If the individual whose PHI is maintained by the Company is not present, or an opportunity to agree or object to a use or disclosure is not practicable (e.g. the individual is incapacitated or there is an emergency situation, or the individual is deceased), and if there is no known prior objection by the individual to the disclosure, then the Workforce member may disclose to the individual's spouse, domestic partner, family member or close friend who is involved in the individual's health care or payment related to the individual's health care (or, if the individual is deceased, was so involved prior to the individual's death), PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care, but only (if the individual is living) the disclosure is determined in the exercise of professional judgment to be in the best interests of the individual. For example, if a patient's spouse calls the Company to assist their hospitalized spouse to inquire about a claim and verifies prior knowledge regarding the claim by giving the provider's name and date of service and asks about the claim status, the Workforce member may tell the spouse whether the claim has been paid, denied or is under review. However, the Workforce member may not provide additional information, such as treatment information, diagnostic codes or information related to other claims; and

(iv) All other requests from spouses, domestic partners, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures of PHI -With Authorization" (Part A, Section IV);

VI. Disclosures of De-Identified Information – Without Authorization

A. Policy

Information that has been de-identified in accordance with the Privacy Rule is no longer considered to be PHI subject to HIPAA. Generally, de-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe

that the information can be used to identify an individual. There are two ways to determine that information is de-identified: either by professional statistical analysis, or by removing the following specific identifiers. Workforce members should consult with the Privacy Officer with any specific questions regarding the de-identification of PHI in accordance with the Privacy Rule. Generally, the identifiers that must be removed are as follows:

(i) Names;

(ii) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;

(iii) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(iv) Telephone numbers;

(v) Fax numbers;

(vi) Electronic mail addresses;

(vii) Social security numbers;

(viii) Medical record numbers;

(ix) Health Plan beneficiary numbers;

(x) Account numbers;

(xi) Certificate/license numbers;

(xii) Vehicle identification and serial numbers, including license plate numbers;

(xiii) Device identifiers and serial numbers;

(xiv) Web Universal Resource Locators (URLs);

(xv) Internet Protocol (IP) address numbers;

(xvi) Biometric identifiers, including finger and voice prints;

(xvii) Full face photographic images and any comparable images; and

(xviii) Any other unique identifying number, characteristic, or code.

B. Procedures

(i) Obtain approval from the Privacy Officer for the disclosure. The Privacy Officer will verify that the information is de-identified.

(ii) The Company may use and disclose de-identified information without regard to HIPAA, since de-identified information is not PHI.

VII. Disclosures For Treatment, Payment and Health Care Operations – Without Authorization

A. Policy

Subject to the terms of this Policy and the Privacy Rule, the Company may use or disclose PHI for treatment, payment and health care operations purposes without the individual's authorization.

(i) *Treatment*. Treatment means the provision, coordination, or management of health care and related services by one or more health care providers. This includes, for example, the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

(ii) *Payment*. Payment means activities undertaken to obtain or provide reimbursement for health care. This includes, for example:

(a) Eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

(b) Risk adjusting based on enrollee status and demographic characteristics;

(c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;

(d) Review of health care services with respect to medical necessity, health plan coverage, appropriateness of care, or justification of charges; and

(e) Utilization review activities; including pre-certification and pre-authorization of services, concurrent and retrospective review of services.

(iii) *Health Care Operations*. Health care operations mean such operations as defined in the Privacy Rule, for example:

(a) Conducting quality assessment and improvement activities;

(b) Reviewing performance and the competency of health care professionals;

(c) Premium rating and similar activities;

(d) Conducting or arranging for medical review, legal services and auditing functions;

(e) Business planning and development;

(f) Business management and general administrative activities;

(g) Management activities relating to HIPAA compliance;

(h) Certain customer service activities, such as data analyses for Covered Entities;

(i) Resolution of internal grievances; and

(j) De-identification of PHI.

B. Procedures

(i) *Treatment Purposes*. PHI may be used or disclosed for treatment activities of a health care provider.

(ii) ***Uses and Disclosures for the Covered Entity's Own Payment Activities or Health Care Operations.*** PHI may be used or disclosed to perform a Covered Entity's own payment activities or health care operations, where the Company serves as that Covered Entity's (or its Business Associate's) Business Associate.

(iii) ***Disclosures for Another Entity's Payment Activities.*** PHI may be disclosed to another Covered Entity (or its Business Associate) or health care provider to perform the other entity's payment activities, where the Company does not serve as such Covered Entity's (or its Business Associate's) Business Associate.

(iv) ***Disclosures for Health Care Operations.*** PHI may be disclosed to a Covered Entity (where the Company does not serve as its Business Associate), or such Covered Entity's Business Associate, for a purpose listed in paragraph (1) or (2) in the Privacy Rule's definition of "health care operations" (e.g., for purposes of the receiving entity's quality assessment

and improvement, and case management), or for the purpose of health care fraud and abuse detection or compliance, but only if the Covered Entity for which the Company serves as a Business Associate, and the receiving entity has (or had) a relationship with the individual who is the subject of the PHI and the PHI requested pertains to that relationship. A Covered Entity that participates in an organized health care arrangement ("OCHA") may disclose PHI about an individual to other participants in the OCHA for any health care operations activities of the OCHA. An OCHA is defined under HIPAA, and includes, among other things, an organized system of health care in which more than one Covered Entity participates and in which the participating Covered Entities 1) hold themselves out to the public as participating in a joint arrangement, and 2) participate in joint activities that include at least one of the following: utilization review, quality assessment and improvement activities, or payment activities.

(v) *Minimum Necessary Rule.* The foregoing uses and disclosures for payment or health care operations are subject to the Policy's "Minimum Necessary Standards" (Part A, Section XI).

(vi) *No Use of Genetic Information for Underwriting Purposes.* The foregoing uses and disclosures for payment, or health care operations are subject to the requirement that in accordance with the Privacy Rule the Company shall not use or disclose PHI that is genetic information for underwriting purposes. Workforce members should consult with the Privacy Officer with any specific questions regarding the application of this requirement in accordance with the Privacy Rule. In addition, for purposes of this requirement:

(a) "Underwriting purposes" means: (A) determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the applicable health plan, coverage or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (B) the computation of premium or contribution amounts, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (C) the application of any pre-existing condition exclusion under the applicable health plan, coverage or policy; (D) other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits. Underwriting purposes does not include determination of medical appropriateness where an individual seeks a benefit under an applicable health plan, coverage or policy.

(b) "Genetic information" means, with respect to an individual, information about the individual's genetic tests, the genetic tests of family members (as defined by HIPAA) of the individual, the manifestation of a disease or disorder in family members of an individual, or any request for, or receipt of, genetic services (e.g., genetic tests, counseling or education), or participation in clinical research which includes genetic services, by the individual or any family member of the individual. Genetic information concerning an individual or family member of an individual includes the genetic information of a fetus carried by such individual who is a pregnant woman, and any embryo legally held by such individual utilizing an assisted reproduction technology. Genetic information excludes information about the sex or age of any individual.

(c) "Genetic test" means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder or pathological condition.

VIII. Mandatory Disclosures of PHI to the Individual and to the Department of Health and Human Services – Without Authorization

A. Policy

The Company intends to facilitate disclosures required by the Privacy Rule. To assure compliance, the requirements include prior approval of the Privacy Officer. An individual's PHI must be disclosed as required by the Privacy Rule in two situations:

(i) The disclosure is to the individual who is the subject of the information; or

(ii) The disclosure is made to the U.S. Department of Health and Human Services ("HHS") for purposes of enforcing the Privacy Rule.

B. Procedures

(i) Upon receiving a request from an individual for disclosure of the individual's own PHI, the Workforce member response would include the following steps:

(a) Follow the procedures for verifying the identity of the individual, as set forth in "Verification of Identity of Those Requesting PHI" (Part A, Section XXIII); and

(b) Follow the procedure for "Access to PHI and Requests for Copies or Amendment" (Part A, Section XII).

(ii) Upon receiving a request from an HHS officer for disclosure of PHI, the Workforce member response would include the following steps:

(a) Follow the procedures for verifying the identity of a public officer set forth in "Verification of Identity of Those Requesting PHI" (Part A, Section XXIII);

(b) Inform the Privacy Officer of the request and obtain approval from the Privacy Officer; and

(c) Disclosures must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

IX. Disclosures of PHI for Legal and Public Policy Purposes – Without Authorization

A. Policy

The Company may make disclosures for legal and public policy purposes under circumstances permitted by the Privacy Rule. PHI will generally be disclosed in the following situations without an individual's authorization, when specific requirements are satisfied. Specific requirements must be met before these types of disclosures may be made. With respect to disclosures for legal and public policy purposes, the requirements include prior approval of the Privacy Officer.

B. Procedures

Disclosures are made under the following procedures:

(i) A Workforce member who receives a request for disclosure of an individual's PHI that appears to be a disclosure for legal or public policy purposes must contact the Privacy Officer, and the disclosure must be approved by the Privacy Officer;

(ii) Disclosures must comply with the "Minimum Necessary Standard" (Part A, Section XI);

(iii) Disclosures must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII);

(iv) With respect to disclosures about victims of abuse, neglect or domestic violence:

(a) The disclosure may be made if: (1) the disclosure is required by law; or (2) the individual agrees with the disclosure; or (3) the disclosure is expressly allowed (but not required) by statute or regulation and (A) the Company believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious harm to the individual (or other potential victims), or (B) the individual is incapacitated and unable to agree and information will

not be used against the individual and is necessary for an imminent enforcement activity.

(b) The individual must be promptly informed of any such disclosure unless the Company believes, in the exercise of professional judgment, that: (1) this would place the individual at risk of serious harm; or (2) if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence, that informing such person would not be in the best interests of the individual.

(v) Disclosures may be made for judicial and administrative proceedings only in response to:

(a) An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or

(b) A subpoena discovery request or other lawful process, not accompanied by a court order or administrative tribunal, but only upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

(vi) Disclosures may be made to a law enforcement officer for law enforcement purposes under any of the following circumstances:

(a) As required by law;

(b) Pursuant to a legal process, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and de-identified information could not reasonably be used;

(c) In response to a law enforcement officer's request for information needed to identify or locate a suspect, fugitive, material witness or missing person, or about an individual who is or suspected to be a victim of a crime;

(d) The PHI concerns a deceased individual and there is suspicion that the individual's death resulted from criminal conduct; or

(e) The PHI constitutes evidence of criminal conduct that occurred on Covered Entity premises.

(vii) Disclosures may be made to appropriate public health authorities for public health activities, such as regarding the prevention of diseases, injuries or disability, and (with appropriate permission, such as from a parent of a

minor child, or from an adult student) to schools to provide proof of student immunizations;

(viii) Disclosures may be made to a health oversight agency for health oversight activities, as authorized by law;

(ix) Disclosures may be made to a coroner or medical examiner about decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law;

(x) Disclosure may be made for certain limited research purposes;

(xi) Disclosures may be made to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation;

(xii) Disclosures may be made upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public;

(xiii) Disclosures may be made for specialized government functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officers for the conduct of national security activities;

(xiv) Disclosures may be made for workers' compensation purposes to the extent necessary to comply with laws relating to workers' compensation or similar programs.

X. Disclosures of PHI to Subcontractor Business Associates – Without Authorization

A. Policy

Workforce members may disclose PHI to the Company's subcontractor Business Associates, and may allow the Company's subcontractor Business Associates to create or receive PHI on its behalf, subject to certain safeguards, including the execution of a subcontractor Business Associate Agreement that satisfies Privacy Rule requirements.

Under HIPAA, a Business Associate is an individual or entity that, on behalf of a Covered Entity (and not as a member of the Covered Entity's Workforce):

(i) creates, receives, maintains, or transmits PHI for a function or activity subject to the Privacy Rule, such as claims processing or administration, data analysis, utilization review benefit administration, etc.; or

(ii) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

A Business Associate also includes a subcontractor of a Business Associate that generally has been engaged to perform a service provided by such Business Associate, directly or indirectly for a Covered Entity, if that subcontractor has access to the Covered Entity's PHI in the performance of such service. An entity that offers a personal health record to individuals on behalf of the Company is also considered to be a Business Associate.

B. Procedures

(i) All uses and disclosures by a Company subcontractor Business Associate must be made in accordance with a valid Business Associate Agreement between the Company and the Business Associate, except that the Business Associate is responsible for entering into valid Business Associate Agreements with its own subcontractors who are also Business Associates. The Privacy Officer maintains a list of Business Associates to whom PHI may be disclosed, and a form Business Associate Agreement to be used with Business Associates. Before providing PHI to a subcontractor Business Associate, Workforce members must verify that the Business Associate is on such list.

(ii) The following additional procedures must be satisfied:

(a) Disclosures must be consistent with the terms of the Business Associate Agreement;

(b) Disclosures must comply with the "Minimum Necessary Standard" (Part A, Section XI).

(iii) Evidence of the Business Associate's Agreement to safeguard PHI must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

(iv) If a Workforce member becomes aware of an incident, pattern of activity or practice that may be a material breach or violation of the subcontractor Business Associate's obligations under its Business Associate Agreement, this Policy or the Privacy Rule, the Workforce member should notify the Privacy Officer. The Privacy Officer will assess the situation and in particular determine if there has been a material breach or violation of the Business Associate's obligations under its Business Associate Agreement, and take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, the Privacy Officer, will take any additional reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, the Company will terminate the Business Associate Agreement, if feasible. In addition, further appropriate action will be taken, for example, determining if the violation falls within the "Breaches of Unsecured PHI" policy (Part A, Section XVI).

XI. Complying With the "Minimum Necessary Standard"

A. Policy

The Privacy Rule generally requires that when the Company uses or discloses PHI, or when the Company requests PHI from a Covered Entity or a Business Associate, the Company must make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request.

B. Procedures

(i) Workforce members may reasonably rely on a requested disclosure of PHI as the minimum necessary for the stated purpose if: (a) the PHI is requested by a professional who is a member of the Workforce or is a Business Associate for the purpose of providing professional services to or on behalf of a Covered Entity for which the Company serves as Business Associate; (b) the PHI is requested by a Covered Entity; or (c) the PHI is requested by a public officer (as permitted under Part A, Section IX of this Policy). For all other requests for disclosures of PHI, Workforce members must determine that the amount of information disclosed is the minimum necessary to accomplish the intended purpose of the disclosure. If a Workforce member has a question regarding whether a use or disclosure of PHI meets the minimum necessary standard, he or she is required to consult with the Privacy Officer, who shall assist in making the determination.

(ii) The minimum necessary standard does not apply to any of the following:

(a) Disclosures made to the individual;

(b) Uses or disclosures made pursuant to an individual authorization;

(c) Disclosures made to HHS;

(d) Uses or disclosures required by law;

(e) Uses or disclosures required to comply with HIPAA; and

(f) Disclosures to a health care provider for treatment purposes.

(iii) If a Workforce member requests PHI from a Covered Entity or another Business Associate, such request must be limited to the minimum necessary for the requested purpose;

(iv) The Privacy Officer shall, in accordance with the standards of this Section XI identify those persons or classes of persons, if any, and as appropriate, that are Workforce members and who accordingly need access to PHI to carry out their duties; and for each such person or class of persons, the category or categories of PHI to which access is needed and any

conditions appropriate to such access. Documentation of these determinations shall be retained pursuant to Part A, Section XXII ("Documentation").

XII. Access to PHI and Requests for Copies or Amendments

A. Policy

The Privacy Rule gives individuals the right to access and obtain copies of their PHI that are maintained by or on behalf of Covered Entities in "Designated Record Sets" (as such term is defined in the Privacy Rule). The Privacy Rule also provides that individuals may request to have their PHI amended. The Company will, in accordance with the Company's obligations under applicable Business Associate Agreements, address requests for access or amendments.

***A Designated Record Set*,** for purposes of this Policy, is defined as in the Privacy Rule, and generally consists of a particular group of "records" maintained by or for a Covered Entity, where the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity, and such records are: (i) the medical records and billing records about individuals maintained by or for a health care provider that is a Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan that is a Covered Entity; or (iii) records used, in whole or in part, by or for a Covered Entity to make decisions about individuals. If a Workforce member has a question regarding whether a given record is part of a Designated Record Set, they are required to consult with the Privacy Officer, who shall assist in making the determination.

B. Procedures

(i) Requests for Access to and/or Copy of PHI

Upon receiving a written request from an individual (or a minor's parent or an individual's authorized personal representative under applicable law) for access to such individual's PHI held in a Designated Record Set, the Workforce member must first assess relevant requirements in the applicable Business Associate Agreement and respond in compliance with such requirements. Where, for example, the Company is responsible for directly responding to the request, the following steps apply:

(a) Follow the procedures for verifying the identity and, as applicable, the authority of the requester, as set forth in "Verification of Identity of Those Requesting PHI" (Part A, Section XXIII).

(b) Review the disclosure request, including by consulting and coordinating with Business Associates, as applicable. This will include a review to determine whether the PHI at issue is held in a Designated Record Set. It will also include review to determine whether an exception to the disclosure requirement might exist under the Privacy Rule; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a

legal proceeding, certain requests by inmates, information compiled during research when the individual has denied access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. All Workforce member determinations to approve or deny access must be reviewed and approved by the Privacy Officer.

(c) Respond to the request, including by consulting and coordinating with Business Associates, as applicable. This will include providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may, in some cases, be extended for no more than 30 days by providing written notice to the individual within the original 30-day period of the reasons for the extension and the date by which the Company will respond.

(1) A denial notice must comply with Privacy Rule requirements, including by containing: (i) the basis for the denial; (ii) a statement of the individual's right to request a review of the denial, if applicable; and (iii) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer.

(2) If the request is approved, provide the information requested, in the form and format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form and format as is agreed to by the individual, except that if the requested PHI is maintained electronically, and the request is made for an electronic copy, the Company must provide the PHI in the electronic form and format requested, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Company and the individual. Individuals have the right to receive a copy directly by mail or come in and pick up a copy. Individuals also have the right to come in and inspect the information.

(3) If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information (including agreeing in advance to the fees imposed, if any, by the Company, for the summary and explanation), prepare such summary and explanation of the information requested, and make it available to the individual in the form or format requested by the individual. All such statements must be reviewed and approved by the Privacy Officer.

(4) If the individual's request for access directs the Company to transmit the PHI directly to another person designated by the individual, the Workforce member shall provide the copy to the person designated by the individual. This designation must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI. Any such requests shall be reviewed and approved by the Privacy Officer.

(d) Charge a reasonable cost-based fee for copying, postage, and preparing a summary, which shall include the costs for supplies for electronic media if the individual requests that the electronic copy be provided on portable media. The calculation of this fee may include consulting and coordinating with Business Associates, as applicable. The fee for preparing a summary must be agreed to in advance by the individual.

(e) Disclosure requests and associated matters must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

(ii) **Request to Amend PHI**

Upon receiving a written request from an individual (or a minor's parent or an individual's authorized personal representative under applicable law) for amendment of such individual's PHI held in a Designated Record Set, the Workforce member must first assess applicable requirements in the applicable Business Associate Agreement, and respond in compliance with such requirements. Where, for example, the Company is responsible for directly responding to the request, the following steps apply:

(a) Follow the procedures for verifying the identity, and as applicable, the authority of the requester as set forth in "Verification of Identity of Those Requesting PHI." (Part A, Section XXIII).

(b) Review the request for amendment, including by consulting and coordinating with Business Associates, as applicable. This will include determining whether the PHI at issue is held in a Designated Record Set. It will also include reviewing the request for amendment to determine whether the amendment is appropriate under the Privacy Rule, including regarding whether the PHI was created by or on behalf of an applicable Covered Entity, the Company or subcontractor Business Associate; would be available for access and inspection by the individual under subparagraph (i), above; and is accurate and complete without the amendment. All Workforce member determinations to approve or deny an amendment request must be reviewed and approved by the Privacy Officer.

(c) Respond to the request, including by consulting and coordinating with Business Associates, as applicable. This will include responding within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for no more than 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Company will respond.

(1) When an amendment is accepted, make appropriate changes and notations in the applicable Designated Record Set in accordance with Privacy Rule requirements. All such notations and changes must be reviewed and approved by the Privacy Officer.

(2) With respect to all approved amendments, in accordance with Privacy Rule requirements, and within the time period specified in subparagraph (c), above, provide appropriate notice to the individual of the amendment, and obtain the individual's identification and agreement regarding persons who have received the applicable PHI and require the amendment. Also, the Company shall make reasonable efforts to identify and notify within a reasonable time other persons/entities who are known to have the particular record (*e.g.* Business Associates) and who may rely on the uncorrected information to the detriment of the individual.

(3) When an amendment request is denied, the following procedures apply:

(A) A denial notice must comply with Privacy Rule requirements, including by containing (i) the basis for the denial; (ii) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (iii) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for reamendment and its denial be included in future disclosures of the information; and (iv) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer; and

(B) The Privacy Officer shall be responsible for assuring that the Company complies with all Privacy Rule requirements regarding any individual's statement of

disagreement and shall coordinate any rebuttal/response to such statement of disagreement, including, without limitation, all record-keeping requirements with respect to such matters.

(d) Amendment requests and associated matters must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

XIII. Requests for Alternative Communication Means or Alternative Locations

A. Policy

Individuals may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home.

The Company will accommodate reasonable requests by individuals if the request states that the disclosure of all or part of that information could endanger the individual. The Company may condition an accommodation on, when appropriate, information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.

B. Procedures

(i) All requests must be in writing.

(ii) The Workforce member receiving the request should follow the procedures for verifying the identity, and as applicable, the authority of the requester as set forth in "Verification of Identity of Those Requesting PHI." (Part A, Section XXIII).

(iii) The Workforce member should determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual and shall otherwise evaluate the appropriateness of providing an accommodation in accordance with this Policy. All Workforce member determinations regarding such requests must be reviewed and approved by the HIPAA Compliance Officer.

(iv) If a request will not be accommodated, the Workforce member must contact the individual in writing to explain that the request will not be accommodated.

(v) All confidential communication requests that are approved must be notated on the individual's file clearly so that all Workforce members who have access to such individual's PHI are made aware of the communication instructions. Business Associates who communicate directly with the individual must be notified of such communication requirements.

(vi) Requests and their dispositions must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

XIV. Requests for Restrictions on Uses and Disclosures of PHI

A. Policy

An individual may request restrictions on the use and disclosure of the individual's PHI with respect to uses or disclosures of PHI to carry out treatment, payment or health care operations, and with respect to disclosures to family members, friends and other persons identified by the individual that are involved with the individual's health care or payment related to health care, as described in Part A, Sections V and VI, above. The Company, in its sole discretion, may accommodate or not accommodate the request.

B. Procedures

(i) All requests for restrictions must be in writing;

(ii) The Workforce member receiving the request should follow the procedures for verifying the identity, and as applicable, the authority of the requester as set forth in "Verification of Identity of Those Requesting PHI." (Part A, Section XXIII).

(iii) The Workforce member should present the request to the Privacy Officer to determine whether the Company will honor the request. While the Company will consider reasonable requests, the Company is not required to honor a request. The Privacy Officer may decide not to honor the request for any reason, including without limitation the feasibility of accommodating the request and/or the additional costs to the Company.

(iv) If the request will not be accommodated, the Workforce member must contact the individual, in writing, to notify the individual.

(v) If a request will be accommodated, the Workforce member must contact the individual, in writing, to explain that the request will be accommodated, including, among other things, the circumstances concerning any termination of the restriction. This notice shall be reviewed and approved by the Privacy Officer. Further, such limitations must be notated in the individual's file clearly so that all Workforce members who have access to such individual's PHI are made aware of the restriction, including Privacy Rule exceptions regarding emergency treatment, and the scope of the restriction (e.g., its non-application to certain disclosures required by law). Such notation shall be reviewed and approved by the Privacy Officer.

(vi) All Business Associates that may have access to the individual's PHI must be notified by the Privacy Officer of any agreed-to restrictions.

(vii) Requests and their dispositions must be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

XV. Accounting for Disclosures

A. Policy

An individual has the right to request an accounting of certain disclosures of his or her PHI by or on behalf of a Covered Entity (e.g., by its Business Associate), including disclosures for purposes other than treatment, payment, health care operations and other exceptions specified in the Privacy Rule. Requests involving the Company may be made orally or in writing (and Workforce members must promptly document all oral requests), and generally cover all applicable PHI disclosures, regardless of whether the PHI was in a Designated Record Set. Under HIPAA, a disclosure means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information.

The accounting must be in writing and include the applicable disclosures of the requesting individual's PHI made by the Company and the Company's subcontractor Business Associates in the six years prior to the date on which the accounting is requested, or a period of time less than six years from the date of the request, if requested by the individual.

The Privacy Officer shall have supervisory responsibility for overseeing the Company's response to requests for accounting for disclosures, including regarding the adequacy of the Company's mechanisms to track disclosures of PHI that are subject to an accounting request. This shall include assuring that the Company's records regarding disclosures of PHI that may be subject to an accounting request include all information that must be included in the accounting provided to an individual under Part A, Section XVB(i)(f), below.

B. Procedures

(i) Upon receiving a request from an individual (or a minor's parent or an individual's authorized personal representative under applicable law) for an accounting of disclosures, the Workforce member must first assess relevant requirements in the applicable Business Associate Agreement and respond in compliance with such requirements. Where, for example, the Company is responsible for directly responding to the request, the following steps apply:

(a) Follow the procedures for verifying the identity, and as applicable, the authority of the requester as set forth in "Verification of Identity of Those Requesting PHI." (Part A, Section XXIII).

(b) If the individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, conduct a prompt preliminary review of the request in order to determine the fee (which shall be a reasonable, cost-based fee) that will be charged to the individual for processing the accounting request. To calculate the fee, the

Workforce member should consult and coordinate with Business Associates, as applicable. When the fee has been determined, the Workforce member should prepare a written notice to the individual informing him or her that a fee for processing the accounting shall be charged, and the amount of that fee. The notice should provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee. Such notice shall be reviewed and approved by the Privacy Officer.

(c) Respond to the request within 60 days by providing the accounting or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60-day period, the deadline may be extended for up to 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Company will respond.

(d) The disclosures to be reported in the accounting shall only exclude those disclosures not required to be reported in the accounting under Privacy Rule requirements, which may include disclosures made:

(1) To carry out treatment, payment and health care operations (as described in Part A, Section VII of this Policy);

(2) To the individual about his or her own PHI (as described in Part A, Section VIII of this Policy);

(3) Incident to an otherwise permitted use or disclosure;

(4) Pursuant to an individual authorization (as described in Part A, Section IV of this Policy);

(5) To the spouse, domestic partner, relative, friend and other persons identified by the individual (as described in Part A, Section V of this Policy)

(6) For national security or intelligence purposes;

(7) To correctional institutions or law enforcement when the disclosure was permitted without an authorization; or

(8) As part of a limited data set.

(e) The disclosures to be reported in the accounting shall include all disclosures not excluded from the accounting under the Privacy Rule, all of which must be documented and tracked by the Company, including, without limitation, the following:

(1) Disclosures for public health activities;

(2) Disclosures about victims of abuse, neglect or domestic violence;

(3) Disclosures for health oversight activities;

(4) Disclosures for judicial and administrative proceedings;

(5) Disclosures to coroners and funeral directors about decedents;

(6) Disclosures for cadaver organ, eye, or tissue donation;

(7) Disclosures for research purposes;

(8) Disclosures to avert a serious threat to health or safety;

(9) Disclosures for military and veteran activities, protective services for the President of the U.S., and medical suitability determinations; and

(10) Disclosures required by law for workers' compensation programs.

(f) The accounting must include the information required by the Privacy Rule for each reportable disclosure of the individual's PHI, and the adequacy of such information shall be reviewed and approved by the Privacy Officer prior to providing the accounting to the requesting individual. This information includes, as required by the Privacy Rule:

(1) The date of disclosure;

(2) The name (and if known, the address) of the entity or person to whom the information was disclosed;

(3) A brief statement of the PHI disclosed; and

(4) A brief statement explaining the purpose for the disclosure that reasonably informs the individual of the basis for the disclosure. As permitted by the Privacy Rule, for certain disclosures the statement of purpose may be accomplished by providing a copy of the applicable written request for the disclosure (e.g., where the disclosure was required by law).

(g) If the Company receives a written statement from a health oversight agency or a law enforcement officer stating that notice to the

individual of disclosures of PHI to such agency or officer would be reasonably likely to impede the agency's or officer's activities, and specifying the time for which a suspension is required, the Company shall suspend an individual's right to receive an accounting of the applicable disclosures for the applicable time period. If a Workforce member receives an oral request of this type, the Company shall document the statement, including the identity of the agency or officer, and temporarily suspend the accounting of disclosures subject to the statement for no more than 30 days, unless a compliant written statement is provided during such period. Workforce members must promptly contact the Privacy Officer of any oral or written requests of these types from health oversight agencies or law enforcement officers, and all actions taken in response to such requests shall be require the review and approval of the Privacy Officer.

(ii) Accountings must be documented in accordance with the Policy's procedure under "Documentation" (Part A, Section XXII).

XVI. Breaches of Unsecured PHI

A. Policy

To the extent the Company maintains, accesses, stores, destroys, and otherwise uses and discloses unsecured PHI, the Company, in accordance with the requirements of the Breach Notification Rule, will notify applicable Covered Entities and others if any of their unsecured PHI has been, or reasonably believed to have been, accessed, acquired or otherwise compromised as a result of a Breach of the Company's system or by the Company's Business Associate. For purposes of this Policy a "Breach" is as defined in the Breach Notification Rule and, as further defined below, generally means the acquisition, access, use or disclosure of PHI in a manner that is not permitted by the Privacy Rule and which compromises the security or privacy of the PHI. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of certain technologies or methodologies according to guidance from the HHS. (*See*: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html).

The Company will investigate all suspected or actual unauthorized uses and disclosures of PHI to the extent the Company becomes aware of such suspected or actual wrongful uses or disclosures, and such investigation will be coordinated by the Privacy Officer. Upon determining that a Breach of Unsecured PHI has occurred, the Company's Privacy Officer will arrange for all notifications as required by applicable law.

B. Procedures

(i) Procedures for Determination of a Breach of Unsecured PHI:

(a) Any Workforce member, the Company's Business Associate or any other person who becomes aware of an actual or suspected

unauthorized use or disclosure of PHI held by the Company or any of their Business Associates, or any other actual or suspected unauthorized use, disclosure, loss, theft or alteration of PHI by or on behalf of the Company must notify the Privacy Officer immediately.

(b) The Privacy Officer, as appropriate involving attorneys for the Company, will immediately undertake an investigation to determine if the unauthorized use or disclosure constitutes a "Breach of Unsecured PHI" under HIPAA. All such investigations and assessments of suspected or actual Breaches by the Company will be documented, and maintained on file by the Privacy Officer, for at least six (6) years from the date of the incident, in accordance with the Policy's procedure under "Documentation" (Part A, Section XXII).

(c) A Breach does not include:

(1) Any unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of the Company or their Business Associate, if made in good faith and within the scope of authority, which does not result in further use or disclosure in a manner not permitted under the Privacy Rule;

(2) Any inadvertent disclosure by a person who is authorized to access PHI at the Company or their Business Associate to another person authorized to access PHI at the Company or same Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or

(3) Any disclosure of PHI where the Company or their Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Any such finding shall be reviewed and approved by the Privacy Officer, who may consult with attorneys for the Company to make such finding.

(d) Except for the exclusions listed in subparagraph (c), above, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach unless the Company or its Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

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

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

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

Any such finding of low probability of compromise shall be reviewed and approved by the Privacy Officer, who may consult with attorneys for the Company to make such finding.

(ii) **Notification of Breach.**

(a) In the event the Privacy Officer, including, as applicable, in consultation with attorneys for the Company, concludes that a Breach of Unsecured PHI has occurred, the Privacy Officer will be responsible for arranging for sending out all requisite notifications in compliance with the Breach Notification Rule (including applicable Business Associate Agreement requirements), including as to recipients (e.g., Covered Entities, and, as applicable individuals, government officers and media outlets), timing and content requirements. The Privacy Officer will typically consult with attorneys for the Company as to the form and substance of all such notifications.

(b) The Privacy Officer will maintain a log of all Breaches of Unsecured PHI.

(c) For Breaches of Unsecured PHI affecting 500 or more individuals, an appropriate public notice should be arranged; and

(d) Records of all such notifications must be maintained on file by the Privacy Officer for at least six (6) years from the date of the incident, in accordance with the Policy's procedure under "Documentation" (Part A, Section XXII).

(iii) Mitigation and Remediation of Breaches. The Privacy Officer, typically in consultation with attorneys for the Company, will be responsible for determining what steps should be taken to mitigate the effects of any Breaches (e.g., credit monitoring, retraining of relevant Workforce members), and what remedial steps should be taken to avoid similar future events (e.g., retraining of staff, instituting new procedures, engaging alternative Business Associates). All such mitigation and remedial steps must be documented by the Privacy Officer and maintained on file for at least six (6) years from the date of the incident, in accordance with the Policy's procedure under "Documentation" (Part A, Section XXII).

(iv) Records regarding Breaches of Unsecured PHI, including, without limitation, any notifications and any mitigation and remedial steps, must be

documented in accordance with the Policy's procedure under "Documentation" (Part A, Section XXII).

XVII. Certain Considerations Applicable to Company Business Associate Agreements with Covered Entities

A. Policy

As a Business Associate's authority to use or disclose PHI derives from the Covered Entity, and since a Covered Entity may only use an individual's PHI for certain purposes without the individual's prior consent, the Company, as a Business Associate, shall comply with the restrictions on use and disclosure of PHI as set forth in the applicable Business Associate Agreement with a Covered Entity, and as set forth in the Privacy Rule. To the extent the Business Associate Agreement between the Company and a Covered Entity permits the Company, as a Business Associate, to do so, the Company may engage in the following activities only as specified and authorized in and subject to restrictions in the applicable Business Associate Agreement and the Privacy Rule:

(i) Engage in "data aggregation" services relating to the health care operations of the Covered Entity, wherein *data aggregation* services means, with respect to PHI created or received by the Company in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Company with the PHI received by the Company in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities, but which in no event shall permit the use of such PHI by the Company for its own purposes;

(ii) "De-identify" PHI, wherein de-identification follows the processes set forth by the Privacy Rule at either 45 C.F.R. §§ 164.514(a) or (b). As, the process of de-identifying PHI constitutes a use of PHI, the Company may only de-identify PHI it has on behalf of a Covered Entity to the extent that the applicable Business Associate Agreement authorizes the Company to do so; however, once PHI is properly de-identified, it is no longer considered PHI and may be used and disclosed by the Company for any purpose (subject to any other applicable laws); and

(iii) to use and disclose PHI for the Company's own "proper management and administration" and to "carry out [its own] legal responsibilities," as such terms are defined under HIPAA, and subject to applicable HIPAA requirements, such as with respect to disclosures, obtaining reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person (see, 45 C.F.R. §164.504(e)(4)).

In each such case, as applicable, the Company may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth in subsections (i), (ii) and (iii), above.

B. Procedures

Prior to the Company engaging in any activity permitted under Part A, Section XVII (A) (i)-(iii), above, the Privacy Officer shall review the applicable Business Associate Agreement pertaining to the Covered Entity whose PHI is to be used and shall assure that the Company's proposed use of PHI comports with the terms and conditions of the applicable Business Associate Agreement and the Privacy Rule.

XVIII. Complaints

A. Policy

The Privacy Officer will be the Company's contact person for receiving complaints about this Policy, and the Company's compliance with this Policy or the requirements of the Privacy Rule or Breach Notification Rule, and for handling such complaints.

B. Procedures

(i) The Privacy Officer will review and handle complaints in accordance with the Company's procedures;

(ii) The Privacy Officer will document complaints received and their resolutions in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

XIX. Sanctions for Violations of Privacy Policy

A. Policy

Sanctions against Workforce members for using or disclosing PHI in violation of this Policy, or the requirements of the Privacy Rule or the Breach Notification Rule (subject to protections afforded to whistleblowers, and in compliance with applicable anti-retaliation requirements) will be imposed in accordance with the Company's discipline policy.

B. Procedures

(i) During training, The Workforce members are informed that sanctions may be imposed if the Policy is violated;

(ii) Appropriate sanctions will be determined based on the nature of the violation, its severity, and whether it was intentional or unintentional. Such sanctions may include, without limitation, verbal counseling, written warnings, probationary periods and/or termination of employment;

(iii) Application of any sanctions will be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII).

XX. Mitigation of Inadvertent Disclosures of PHI

A. Policy

The Company will mitigate, to the extent practicable, any harmful effects that become known to the Company of a use or disclosure of PHI in violation of this Policy or the requirements of the Privacy Rule by the Company or its Business Associates.

B. Procedures

If a Workforce member becomes aware of a disclosure of PHI, either by a Workforce member of the Company or an outside consultant/contractor or other Business Associate that is or is suspected to be not in compliance with this Policy or the Privacy Rule, the Workforce member must **immediately** contact the Privacy Officer so that the appropriate steps to mitigate the harm can be taken.

XXI. No Intimidating or Retaliatory Acts; No Waiver of the Privacy Rule

A. Policy

The Company, in compliance with HIPAA, shall not and no Workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person: (i) for the exercise of any right established, or for participation in any process provided for by the Privacy Rule or Breach Notification Rule, or (ii) for filing a complaint under HIPAA, or (iii) for testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under HIPAA, or (iv) for opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Rule. In addition, the Company shall not require individuals to waive their rights under HIPAA to make a complaint to the Secretary of HHS, or any right under the Privacy Rule or the Breach Notification Rule, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

B. Procedure

If a Workforce member or other person becomes aware of a violation of the foregoing prohibitions against intimidation, retaliation, etc. the Workforce member or other person will **immediately** notify the Privacy Officer.

XXII. Documentation

A. Policy

The Company's privacy policies and procedures are documented and maintained for at least six years from the later of the date of creation or when it was last in effect, whichever is later. Policies

and procedures are changed as necessary and appropriate to comply with changes in the law, including the standards, requirements and implementation specifications of the Privacy Rule or Breach Notification Rule. Any changes to policies or procedures are promptly documented.

B. Procedures

(i) The Privacy Officer maintains copies of all of the following items:

(a) When a disclosure of PHI is made that is subject to the accounting rules (Part A, Section XV), the following information regarding the disclosure will be documented:

(1) The date of the disclosure;

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

(3) A brief description of the PHI disclosed;

(4) A brief statement of the purpose of the disclosure;

(5) Any other documentation required under this Policy.

(b) Privacy and breach notification policies and procedures and revisions to them;

(c) Records of training;

(d) Sanctions applied to Workforce members who violate the Policy;

(e) Business Associate Agreements and lists of Business Associates, as well as applicable documentation pertaining to Covered Entities (e.g., applicable Notices of Privacy Policies, Minimum Necessary Requirements, etc.);

(f) Complaints and resolutions;

(g) Records regarding Workforce member access to PHI;

(h) Records regarding Breaches of Unsecured PHI;

(i) Individual authorizations;

(j) Agreed to restrictions on PHI;

(k) Requests for access or amendments to PHI;

(l) Requests for alternative communication means or alternative location;

(m) Any documentation authorizing an individual's personal representative to be treated as the individual for purposes of this Policy and the Privacy Rule.

The documentation of the foregoing may be maintained in either written or electronic form.

XXIII. Verification of Identity of Those Requesting PHI

A. Policy

The Company must verify the identity and authority of individuals requesting PHI before providing such PHI.

B. Procedures

Workforce members must take steps to verify the identity of individuals who request PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI for his or her minor child, an authorized personal representative under applicable law, or a public officer. Similarly reasonable steps should be taken to verify the identity of personnel from Covered Entities that seek access to the Covered Entity's PHI.

(i) When an individual requests access to his or her own PHI, the following steps must be followed:

(a) If the individual requests PHI in person, Workforce members must request a form of identification. Workforce members may rely, for example, on a valid driver's license, passport or other photo identification issued by a government agency;

(b) If the individual requests PHI over the telephone, the Workforce member must verify the individual's identity by requesting all of the following information: i) address, ii) date of birth, and iii) Social Security number, or other unique identifier as appropriate;

(ii) When a parent requests access to the PHI of the parent's minor child, seek reasonable verification of the person's relationship with the child. However, applicable state or other laws may, in select circumstances, limit parental access to a minor's PHI for certain sensitive services where a minor is authorized to personally consent to treatment without parental consent (e.g., regarding HIV/AIDS treatment, or treatment for sexually transmitted illness) and the Privacy Officer should be consulted regarding parental inquiries with respect to these types of services;

(iii) When a personal representative requests access to an individual's PHI, the following steps should be followed:

(a) Require a copy of a valid power of attorney or other officer documentation that authorizes the individual to access the requested PHI under applicable state or other law (such as court-appointment as a guardian or trustee, appointment under a power of attorney or health care proxy, or appointment as executor of an estate). With respect to a living individual, the documentation must grant the personal representative the authority to act on behalf of the individual in making decisions related to health care, which would include decisions relating to payment for health care, and the personal representative may access the individual's PHI only to the extent that PHI is relevant to the matters on which the personal representative is authorized to represent the individual. For deceased individuals, a person may be a personal representative of a deceased individual if they have the authority to act on behalf of such individual or such individual's estate for any decision, not only decisions related to health care, and would generally be entitled to access all PHI. The Privacy Officer should be consulted to verify the authority of the individual to access the requested PHI as a personal representative under the documentation provided;

(b) A copy of the authorizing documentation provided shall be documented in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII);

(iv) If a public officer requests access to PHI, the following steps should be followed to verify the officer's identity and authority:

(a) If the request is made in person, request presentation of an agency identification badge, other officer credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set in accordance with the Policy's procedures under "Documentation" (Part A, Section XXII);

(b) If the request is in writing, verify that the request is on the appropriate government letterhead;

(c) If the request is by a person purporting to act on behalf of a public officer, request 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 officer;

(d) Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, other proof as appropriate;

(v) In accordance with the Privacy Rule, the Company reserves the right to not treat a personal representative as the individual, and to not provide a parent of a minor child with access to the minor child's PHI, if, in the exercise of professional judgment, the Company finds that doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative or parent, or that doing so would otherwise endanger the individual.

PART B.

HIPAA SECURITY

I. Introduction

Part B of this Policy contains policies and procedures for compliance with the HIPAA Security Rule (the "Security Rule"). It addresses PHI that is Electronic Protected Health Information (referred to as "ePHI" in this Part B) under the Security Rule, which is information transmitted by or maintained in Electronic Media. For purposes of this Policy:

Electronic Media means media that would be considered "electronic media" under HIPAA, including (1) electronic storage media on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and (2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, via facsimile, and voice via telephone, are not considered to be transmissions via Electronic Media if the information being exchanged did not exist in electronic form immediately before the transmission.

Certain words and phrases that are capitalized in Part B of this Policy, and not specifically defined when used, have special meanings under the Security Rule and are defined in Section VII, below ("Glossary"); provided that any capitalized term not specifically defined in this Policy shall have the same meaning as is set forth in HIPAA, and all words and phrases defined in Section VII, below that are also defined in HIPAA are intended to have the same meaning as is set forth in HIPAA.

Part B of this Policy consists of eight (8) sections.

Section I, this Introduction, describes the purpose of this Security Rule policy and the organization of this Part B of the Policy.

Section II describes the Company's overall policy for protecting ePHI.

Section III describes the Company's procedures for implementing Administrative Safeguards.

Section IV describes the Company's procedures for implementing Physical Safeguards.

Section V describes the Company's procedures for implementing Technical Safeguards.

Section VI describes required legal documents including Business Associate Agreements and the policies and procedures. This Section also includes a description of the Security Rule documentation requirements.

Section VII contains a Glossary of certain key terms used in this Part B of the Policy. These defined terms are capitalized in this Part B of the Policy.

Section VIII addresses complaints and non-retaliation.

II. Statement of Security Policy

The Company's will, to the extent applicable, secure ePHI in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is the Company's policy to:

- Ensure the Confidentiality, Integrity, and Availability of the Company's ePHI;
- Protect against any reasonably anticipated Threats or hazards to the security or Integrity of the ePHI;
- Protect against any reasonably anticipated uses or Disclosures that are not permitted by the HIPAA Privacy Rule; and
- Ensure Workforce compliance.

The Company will, to the extent applicable, maintain a security infrastructure containing Administrative, Physical, and Technical Safeguards for ePHI.

When ePHI is shared with a Business Associate providing services to the Company, the Company must have a Business Associate Agreement with that subcontractor Business Associate.

III. Administrative Safeguards

A. Overview

The Company maintains procedures to manage risks to ePHI it holds, to control Access to such ePHI, to train Workforce members regarding ePHI protections, to resolve Security Incidents that may be a Threat to its ePHI, and to protect ePHI during emergency situations. The Administrative Safeguards include the following sections of this Policy:

Section III-B - Security Management Process

The Company will maintain procedures to prevent, detect, and correct security violations. This process will include a risk analysis, ongoing risk management, enforcement of a sanction policy, and review of Information System activity.

Section III-C - Assigned Security Responsibility

The Company will designate a single individual who has overall responsibility for the development and implementation of the Policies and Procedures required by the Security Rule and this Policy for the security of its ePHI.

Section III-D - Workforce Security

The Company will maintain Workforce security measures to assure that all Workforce members with Access to ePHI have the appropriate Access authority and clearances, and to prevent Access by those who do not.

Section III-E - Information Access Management

The Company will define Access control for all Workforce members authorized to Access ePHI and maintain procedures for granting and modifying Access.

Section III-F - Security Awareness and Training

The Company will maintain a security awareness and training program for all Workforce members with Access to ePHI.

Section III-G - Security Incident Procedures

The Company will maintain procedures to handle Security Incidents, including identification and response plans, mitigation of incidents, and documentation of incidents and their outcomes.

Section III-H - Contingency Plan

The Company will maintain a contingency plan for responding to emergencies that affect applications and systems containing ePHI.

Section III-I - Evaluation

The Company will perform periodic technical and non-technical evaluations based on the requirements of the Security Rule, and in response to environmental or operational changes.

B. Security Management Process

As applicable, the Company maintains a security management process to prevent, detect, contain and correct security violations of applications and/or systems that contain ePHI.

(i) Risk Analysis

The Company conducts assessments of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of ePHI held by the Company periodically, as warranted by changes in environmental, technological, or operational conditions. To appropriately consider the potential vulnerabilities to the Company's ePHI, the Company uses the following risk analysis strategy:

- Identify and document all ePHI containing systems or applications (repositories);
- Identify the potential Threats or vulnerabilities to each repository;
- Assign a level of risk to each ePHI repository; and

- As appropriate, mitigate the risk to each ePHI repository.

An ePHI repository may be a database, spreadsheet, folder, storage device, document or other form of electronic information. The Company will perform periodic inventories at regular intervals to ensure that the risk analysis is up-to-date and accurate.

(ii) **Risk Management**

The Company manages risks to its ePHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Company;
- The Company's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and
- The criticality of the ePHI potentially affected.

The Company will perform a periodic technical and non-technical evaluation, based on the standards set forth in the Security Rule, to ensure that the Company's Policies and Procedures are updated as warranted by changes in the Company's environmental or operational conditions affecting the security of ePHI.

(iii) **Sanction Policy**

Sanctions against Workforce members for failing to comply with the policies and procedures of the Company set forth in this Policy (subject to protections afforded to whistleblowers, and in compliance with applicable anti-retaliation requirements) will be imposed in accordance with the Company's discipline policy.

During training, Workforce members will be informed that sanctions may be imposed if the policies and procedures of this Policy are violated. Appropriate sanctions will be determined based on the nature of the violation, its severity, and whether it was intentional or unintentional. Such sanctions may include, without limitation, verbal counseling, written warnings, probationary periods and/or termination of employment.

(iv) **Information System Activity Review**

The Company will appropriately review activity in ePHI-containing applications and/or systems in order to limit ePHI access to authorized purposes, including auditing and oversight tools permitting review of suspicious or unusual activity and vulnerabilities and adequate and prompt notice to the Security Officer.

(v) **Citations**

45 CFR § 164.308(a)(1)

C. Assigned Security Responsibility

The Company has designated an officer to serve as the security official under HIPAA. That individual is the Company's Security Officer, and, in the Company's discretion, may be the same individual who serves as the Privacy Officer. The Security Officer will be responsible for the development and implementation of policies and procedures relating to the HIPAA Security Rule, including but not limited to as set forth in this Policy. The Security Officer will also serve as the Company's contact person who is responsible for receiving complaints regarding the Company's compliance with the Security Rule, and this Policy. Wherever this Policy refers to the Security Officer such reference will include any person delegated by the Security Officer, whether such delegation is oral or written.

(i) Citations

45 CFR § 164.308(a)(2)

D. Workforce Security

The Company maintains Workforce security procedures to ensure that all Workforce members have appropriate Access to ePHI. These procedures also are intended to prevent those Workforce members who do not have appropriate Access to ePHI from obtaining such Access. As applicable:

(i) Authorization and/or Supervision

A record is maintained by the Company of those Workforce members who require Access to ePHI and the scope of such Access necessary to perform applicable functions. Workforce members who do not have Access to ePHI but who have a need to review records containing ePHI must be supervised in that activity by someone that has such Access and the technical skills to appropriately supervise said Workforce members.

(ii) Workforce Clearance Procedure

Workforce members that Access ePHI are subject to a background check and screening process to ensure that their Access is appropriate.

(iii) Termination Procedures

If a Workforce member who has Access to ePHI is terminated or resigns, the former Workforce members' computer accounts will be disabled, including any accounts used for database Access, dial-up, or Internet Access from a remote location.

(iv) Citations

45 CFR § 164.308(a)(3)

E. Information Access Management

As applicable, to ensure that appropriate Access to ePHI is consistent with the HIPAA Privacy Rule, the Company actively manages the rights of Workforce members to Access ePHI. To the extent that it is reasonable and appropriate, Access to ePHI is limited to Workforce members for purposes of performing applicable functions as permitted by the Privacy Rule and consistent with the Company's documents. As applicable:

(i) Access Authorization

The Company maintains a record of those Workforce members who require Access to ePHI and the scope of such Access necessary to perform Plan administrative functions.

(ii) Access Establishment and Modification

The Company will review who has Access to ePHI and whether such Access is limited to ePHI that is minimally necessary to perform applicable functions.

(iii) Citations

45 CFR § 164.308(a)(4)

F. Security Awareness and Training

The Company maintains security awareness and training for all Workforce members with Access to any ePHI repository. Workforce members will review the Company's HIPAA Security Policy, as appropriate, prior to receiving Access to any ePHI, and when changes to the Security Policy occur that are relevant to their job function. As applicable:

(i) Security Reminders

The Company will provide Workforce members with periodic security updates.

(ii) Protection from Malicious Software

The Company uses hardware and anti-virus software that scans email attachments and other downloadable files. Every Workstation will have anti-virus software installed and activated. Virus signature files will be routinely updated. Workforce members will be instructed not to open emails unless the message was expected in the course of business or was sent by a source known to the recipient.

(iii) Log-In Monitoring

The Company maintains procedures for monitoring log-in attempts and reporting discrepancies. Suspicious login activity will be reported and resolved in accordance with the Company's Security Incident Procedures.

(iv) Password Management

Workforce members with Access to the Company's ePHI will comply with the Company's password management policy.

(v) **Citations**

45 CFR § 164.308(a)(5)

G. Security Incident Procedures

The Company maintains procedures addressing Security Incidents that permit the Company to identify and respond to suspected or known Security Incidents, mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Company, and document Security Incidents and their outcomes.

(i) **Response and Reporting**

The user of any information technology device connected to or housing ePHI will report any suspected or known Security Incident promptly to the Security Officer, who will log all pertinent information regarding a Security Incident including date, time, people contacted, and ePHI applications or repositories affected. The Security Officer will promptly notify the Privacy Officer in the event of any such reports, and cooperate to address and resolve all such issues in compliance with HIPAA.

The Security Officer and the Privacy Officer shall cooperate to mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Company, and document Security Incidents and their outcomes, and as appropriate if the Security Incident constitutes a reportable data breach in violation of HIPAA Privacy Rules, and in accordance with HIPAA Breach Notification rules.

(ii) **Citations**

45 CFR § 164.308(a)(6)

H. Contingency Plan

The Company maintains a contingency plan that includes procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems and/or applications containing ePHI. As applicable:

(i) **Data Backup Plan**

The extent to which a backup is needed will be determined by the Company's periodic risk analyses.

(ii) **Disaster Recovery Plan**

The Company, as feasible, will restore lost, damaged or destroyed ePHI from regularly maintained backups, or other outside sources (e.g., third-party vendors).

(iii) Emergency Mode Operation Plan

The Company, as feasible, will permit Access control overrides during emergency situations, and continue, as feasible, other applicable security measures.

(iv) Testing and Revision Procedures

Testing, updates and revisions of applicable policies and procedures will be conducted as needed.

(v) Applications and Data Criticality Analysis

See Risk Management (Section III-B) for the Company's Applications and Data Criticality Analysis procedure.

(vi) Citations

45 CFR § 164.308(a)(7)

I. Evaluation

See Risk Management (Section III-B) for the Company's Evaluation procedure.

(i) Citations

45 CFR § 164.308(a)(8)

IV. Physical Safeguards

A. Overview

The Company maintains procedures to protect applications, systems and related facilities and equipment housing ePHI from natural and environmental hazards, unauthorized intrusion, and other Threats. Physical Safeguards include the following sections of this Policy:

IV-B Facility Access Controls: the Company will limit physical Access to electronic Information Systems and the facilities in which they are housed, while ensuring that properly authorized Access is allowed.

IV-C Workstation Use: the Company will specify the proper Workstation functions to be performed, the manner in which those functions are to be performed, and the characteristics of the physical surroundings of Workstations that can Access ePHI.

IV-D Workstation Security: the Company will use reasonable measures regarding entry to Workstations that can Access ePHI to authorized users.

IV-E Device and Media Controls: Procedures will govern the receipt and removal of hardware and Electronic Media that contain ePHI into and out of a Facility, and the movement of these items within the Facility. The security procedure address: (a) the final disposition of ePHI and/or the hardware or Electronic Media on which it is stored; (b) the removal of ePHI from Electronic Media

before the media are made available for re-use; and (c) the creation of retrievable, exact copies of ePHI when needed, before movement of equipment occurs. The Security Officer will assure that appropriate documentation is maintained to record the movement of hardware and Electronic Media and any person responsible therefor.

B. Facility Access Controls

The Company will maintain Facility Access control procedures to limit physical Access to its ePHI containing Information Systems and the Facility (or facilities) where they are housed, while ensuring that properly authorized Access is permitted. As applicable:

(i) Contingency Operations

When reasonable and practical, Workforce members and emergency personnel will be given Access to the Company to assist in the restoration of lost data. For additional related procedures see: Section III-H: Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan).

(ii) Facility Security Plan

The Company will safeguard the Company and its equipment from unauthorized physical Access, tampering and theft, using, among other things, appropriate physical security safeguards.

(iii) Access Control and Validation Procedures

The Company will control and validate a person's Access to the Company using appropriate Access controls, including, for example, with respect to visitor sign in upon arrival and supervision when on-premises, as appropriate.

(iv) Maintenance Records

The Company will maintain a log of material repairs and modifications to all physical security safeguards including hardware, locks, doors, and walls.

(v) Citations

45 CFR § 164.310(a)(2)

C. Workstation Use

Workforce members will limit their Access and use of ePHI-containing systems, applications, and/or Workstations to necessary and appropriate functions. In addition, as applicable, Workforce members will be prohibited from attempting to bypass security protections and must follow all relevant security measures including: Workstation Security (Section IV-D), Facility Access Controls (Section IV-B), Authorization and/or Supervision (Section III-D), Access Control (Section V-B), Audit Controls (Section V-C), Person or Entity Authentication (Section V-E), and Transmission Security (Section V-F).

(i) Citations

45 CFR § 164.310(b)

D. Workstation Security

The Company will impose security procedures for all Workstations that have Access to ePHI-containing systems or applications: See Facility Access Controls (Section IV-B).

(i) **Citations**

45 CFR § 164.310(c)

E. Device And Media Controls

The Company maintains procedures governing the receipt and removal of hardware and Electronic Media that contain ePHI, into and out of a Facility, and the movement of these items within the Facility.

(i) **Disposal and Media Re-Use**

The Company will ensure proper sanitation of all Electronic Media containing ePHI before it is transferred from the custody of its current custodian. The proper sanitization method depends on the type of media and the intended disposition of the media.

The Company will not use 'clearing data' as a method for sanitizing media. Clearing data (such as formatting or deleting information) removes information from storage media so that the information is unreadable. However, special utility software or techniques can be used to recover the cleared data.

Appropriate Plan method for sanitizing Electronic Media may include: Overwriting disk drives, Low-Level formatting and "Zeroing out the drive". CDs are shredded and destroyed.

(ii) **Data Backup and Storage**

As needed, the Company will create a retrievable, exact copy of the ePHI (e.g., using a tape back-up, imaging the hard drive, or copying the ePHI onto a network hard drive) to assure proper backup and storage.

(iii) **Citations**

45 CFR § 164.310(d)

V. Technical Safeguards

A. Overview

The Company, as applicable, maintains technology procedures to protect and control Access to ePHI. They are designed to guard against unauthorized Access to or alteration of ePHI that is

stored in an application or system or that is transmitted over a communications network. The Technical Safeguards include the following sections of this Policy. As applicable:

Section V-B Access Control

The Company will maintain procedures to grant and allow Access to Electronic Information Systems that contain ePHI to only those persons or software programs that have appropriate Access rights.

Section V-C Audit Controls

The Company will maintain procedural mechanisms and processes that record and examine activity in Information Systems that contain or use ePHI.

Section V-D Integrity

The Company will maintain procedures to protect ePHI from improper or unauthorized alteration or destruction.

Section V-E Person or Entity Authentication

The Company will verify that a person or entity seeking Access to ePHI is the one claimed.

Section V-F Transmission Security

The Company will guard against unauthorized Access to ePHI that is being transmitted over an electronic communications network.

B. Access Control

The Company will restrict Access to applications or systems that contain ePHI to those users that require Access to ePHI to carry out the Company's administrative functions by the following administrative policies and procedures: Sanction Policy (Section III-B), Information System Activity Review (Section III-B), Authorization and/or Supervision (Section III-D), Termination Procedures (Section III-D), and Information Access Management (Section III-E). As applicable:

(i) Unique User Identification

The Company will require user Authentication for all Workforce members seeking Access to network applications or systems containing ePHI. That Authentication will require a unique identifier (e.g., a log-in user ID) for each user. See also Person or Entity Authentication (Section V-E). Workforce members are instructed not to allow others to use their unique user ID and password, smart card, or Authentication information. Workforce members will make a reasonable effort to verify the Authentication of the person or entity receiving ePHI prior to transmission.

Anonymous users will not be permitted Access to ePHI. All vendor-supplied passwords will be changed when new software or hardware is added to an electronic Information System containing ePHI, or when new software or hardware has Access to such a system.

(ii) Emergency Access Procedure

The Company will use the following Contingency Plan procedures for obtaining necessary ePHI during an emergency (Section III-H):

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan

(iii) Automatic Logoff

Workforce members will log off and use reasonable measures to appropriately secure Workstations when not in use. In addition, the Company will impose the following requirements for all Workstations that have Access to ePHI containing systems or applications:

Facility Access Controls (Section IV-B) addresses additional Physical Safeguards that will be implemented to protect the security of Workstations.

(iv) Encryption and Decryption

As appropriate and consistent with guidelines established by the Security Officer, ePHI will be encrypted when stored and decrypted for use.

(v) Technical Perimeter Control

Appropriate Technical Safeguards will be used to protect ePHI - containing systems from unauthorized Access from outside the Company, and appropriate measures to ensure that system perimeter controls have been effectively configured.

See also Protection from Malicious Software (Section III-F)

(vi) Citations

45 CFR § 164.312(a)(2)

C. Audit Controls

Audit controls will be implemented to identify suspect data Access, assess the effectiveness of the Company's security program, and respond to potential weaknesses, including, as appropriate regarding:

- Successful Logins

- Failed Login Attempts
- File Accessed
- Security Incidents
- Port Scans
- User Identity
- Time and Date Access
- Scope of ePHI Data Being Accessed

See also Information System Activity Review (Section III-B), Log-in Monitoring (Section III-F) and Security Incident Procedures (Section III-G).

(i) **Citations**

45 CFR § 164.312(b)

D. Integrity

The Company maintains procedures to protect ePHI from improper alteration or destruction. As applicable:

(i) **Mechanism to Authenticate ePHI**

The Company will appropriately verify that ePHI has not been altered or destroyed in an unauthorized manner.

(ii) *Citations*

45 CFR § 164.312(d)

E. Person or Entity Authentication

The Company will require appropriate Authentication mechanism(s) to verify user identity of persons Accessing ePHI-containing applications/or systems.

(i) **Citations**

45 CFR § 164.312(d)

F. Transmission Security

The Company, as applicable, maintains transmission security procedures to guard against unauthorized Access to ePHI that is being transmitted over an electronic communications network.

The Company will use appropriate methodologies to secure ePHI when it is being transmitted over an open electronic network, and appropriately limit remote computer Access to ePHI to personnel who have demonstrated a need to Access ePHI from off-site locations.

(i) **Integrity Controls**

See above Section V-F, and also see Mechanism to Authenticate ePHI (Section V-D) for the Plan's integrity controls procedure.

(ii) **Encryption**

See above Section V-F for the Company's transmission Encryption procedure.

(iii) **Citations**

45 CFR § 164.312(e)

VI. Required Legal Documents

A. Overview

The Company will execute and retain copies of all necessary legal documentation as described in the following sections of this Policy:

Section VI-B Business Associate Agreements and Other Arrangements

The Company may permit a Business Associate to create, receive, maintain, or transmit ePHI on its behalf, only if the Company obtains a written contract or other documented arrangement with the Business Associate as required by HIPAA. The contract or documented arrangement must provide satisfactory assurances that the Business Associate will appropriately safeguard ePHI.

Section VI-C Policies and Procedures

This Policy is intended to comprise the policies and procedures to comply with the HIPAA Security Rule, which are reasonably designed and appropriate for the size and type of activities that relate to ePHI. Any organizational or technological changes may require updates to this Policy.

Section VI-D Documentation

If an action, activity, or assessment is required by the HIPAA Security Rule to be documented, the Company will also maintain a record of that action, activity, or assessment, in accordance with HIPAA requirements.

B. Business Associate Agreements and Other Arrangements

The Company will, in compliance with HIPAA, obtain Business Associate Agreements from all of its subcontractor Business Associates, and from all Covered Entities for which it is a Business Associate. In these Business Associate Agreements the Business Associates must, among other

things, agree to comply with the applicable requirements of the Security Rule. The Company will not disclose ePHI to a subcontractor Business Associate unless a Business Associate Agreement has been signed.

The Security Officer will monitor the ePHI that a Business Associate must return to the Company or destroy (or extend the protections of the Business Associate Agreement if the ePHI is not returned or destroyed) upon termination of the Business Associate Agreement.

If the Security Officer knows or suspects that a Business Associate is violating the terms of its Business Associate Agreement, the Security Officer will promptly notify the Privacy Officer, and the Security Officer and Privacy Officer will cooperate to determine if a breach has occurred, if the breach can be cured, and to take any other actions that are indicated under HIPAA and otherwise appropriate.

(i) Citations

45 CFR § 164.308(b), 45 CFR § 164.314(a)

C. Policies And Procedures

The Company will implement reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule, and such policies and procedures shall be set forth in this Policy. The Company may change its policies and procedures at any time and shall document such changes in this Policy, in accordance with Section VI-C of this Policy, and implement such changes in accordance with the Security Rule.

(i) Citations

45 CFR § 164.316(a)

D. Documentation

The Company will comply with the Security Rule requirements regarding documentation creation and retention. This includes that in the event the Company determines that it will not implement an "addressable" implementation specification or implement an alternative version of the implementation specification, it will document why it has decided not to or the alternative it will implement to address the specification.

(i) Document Retention

The Company will retain all documentation required by the HIPAA Security Rule for 6 years from the later of the date of its creation or the date when it was last in effect, whichever is later.

(ii) Availability

The Company will make documentation available to those persons responsible for implementing the procedures, set forth in this Policy, to which the documentation pertains. See also Security Awareness and Training (Section III-F).

(iii) **Updates**

The Company will periodically review HIPAA security documentation and update the documentation in response to environmental or operational changes affecting the security of the ePHI, as needed.

(iv) **Citations**

45 CFR § 164.316(b), 45 CFR § 164.306(d)(3)

VII. Glossary

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative Safeguards: Administrative actions and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the Workforce in relation to the protection of that information.

Audit: Safeguards dealing with ensuring activity involving Access to and modification of sensitive or critical files is logged, monitored, and possible security violations investigated.

Authentication: The corroboration that a person is the one claimed.

Availability: The property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility: The physical premises and the interior and exterior of a building(s).

HHS: The United States Department of Health and Human Services.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

Physical Safeguards: Physical measures, policies, and procedures to protect electronic Information Systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Technical Safeguards: The technology and the policy and procedures for its use that protect ePHI and control access to it.

Threat: A potential force or situation that may exploit (accidentally or intentionally) a specific weakness in the safeguards protecting ePHI.

Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and Electronic Media stored in its immediate environment.

VIII. Complaints; Non-Retaliation

A. Complaints

The Security Officer will be the Company's contact person for receiving and handling complaints about the policies and procedures set forth in this Policy, and the Company's compliance with this Policy or the requirements of the Security Rule, and for handling such complaints.

The Security Officer will document complaints received and their resolutions in accordance with the Policy's documentation procedures at Section VI-D.

B. No Intimidating or Retaliatory Acts

The Company, in compliance with HIPAA, shall not and no employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person: (i) for the exercise of any right established, or for participation in any process provided for by the Security Rule, or (ii) for filing a complaint under HIPAA, or (iii) for testifying, assisting or participating in an investigation, compliance review, proceeding or hearing under HIPAA, or (iv) for opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of ePHI in violation of the Privacy Rule. In addition, the Company shall not require individuals to waive their rights under HIPAA to make a complaint to the Secretary of HHS.

If an employee or other person becomes aware of a violation of the foregoing prohibitions against intimidation, retaliation, etc. the employee or other person will promptly (but not later than 24 hours) notify the Security Officer, who shall cooperate with the Privacy Officer in resolving the matter in compliance with HIPAA and this Policy.