
# HIPAA PRIVACY AND SECURITY POLICIES AND PROCEDURES

# COVERING GROUP HEALTH PLANS OF THE COUNTY OF MONROE, MICHIGAN

**ADOPTED BY THE MONROE COUNTY BOARD OF COMMISSIONERS**

**TUESDAY, APRIL 24, 2012**

**TABLE OF CONTENTS**

## ARTICLE I
## INTRODUCTION

**THE COUNTY OF MONROE, MICHIGAN** (the "Employer") sponsors and maintains the following group health benefits:

- County of Monroe Health Care and Prescription Drug Medical Program (offering self-funded medical and prescription drug benefit options for Eligible Active Employees and eligible dependents);

- County of Monroe Dental Program (offering self-funded dental benefit options for Eligible Active Employees and eligible dependents);

- County of Monroe Vision Program (offering self-funded vision benefit options for Eligible Active Employees and eligible dependents);

- County of Monroe Health Care Spending Account Program (self-funded through employee pre-tax contributions to pay for certain health care expenses of eligible Active Employees and eligible dependents); and

- County of Monroe Retiree Health Care, Prescription Drug Medical Program, Dental Program and Vision Program (offering self-funded medical, prescription drug benefit, dental and vision options for Eligible Retirees and eligible dependents);

Members of the Employer's workforce may have access to individually identifiable health information of Plan Participants for purposes of performing administrative functions on behalf of the Plan. The Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing privacy and security regulations (collectively referred to as "HIPAA") restrict the Employer's and Plan's ability to use and disclose certain health information known as "protected health information" ("PHI") and may require the Plan and the Employer to implement security measures with respect to electronic protected health information ("EPHI").

While the Plan's and Employer's policy is to fully comply with HIPAA, the Plan, through the Employer, has entered into third party administrative and business associate agreements with Business Associates to perform administrative functions on behalf of the Plan, including HIPAA compliance. As a result, member's of the Employer's workforce generally will not receive, use, maintain, disclose or transmit PHI or EPHI on behalf of the Plan. The Employer, in its capacity as the employer, typically will have access only to certain enrollment and disenrollment information regarding the Plan's participants (including participant name, social security number and election amount under the Plan) and to Summary Health Information. To the extent that the Employer (and/or members of its workforce) actually receive, use, maintain, disclose or transmit PHI or EPHI, then the Employer will implement the administrative, technical and other safeguard policies and procedures described in this document to ensure compliance with HIPAA.

Throughout this document, various terms are used repeatedly. These terms have specific and definite meanings and generally have been capitalized throughout this document. Whenever

capitalized terms appear, they shall have the meanings specified in Article V or as specified in HIPAA. Where necessary or appropriate to the context, the masculine shall include the feminine, the singular shall include the plural and vice versa.

## ARTICLE II
## PLAN'S AND EMPLOYER'S RESPONSIBILITIES

**Section 2.1** **HIPAA Privacy Officer and Contact Person**. The Employer has appointed Aundrea L. Armstrong, Deputy Director of Human Resources, 125 East Second Street, Monroe, Michigan 48161, Telephone number (734)-240-7298, as the Privacy Officer. The Privacy Officer is responsible for developing and implementing policies and procedures, and adherence to them, to ensure compliance with HIPAA and for appointing a Contact Person. The Privacy Officer also will be available to assist with the applications, interpretation and implementation of and compliance with the Plan's policies and procedures and the HIPAA Rules.

Plan Participants will be notified of any change to the contact information for or designation of the Privacy Officer. The Plan will maintain a written or electronic record of its designations of a Privacy Officer and will retain such designations for a period of six years after an initial or any subsequent designation.

At this time, the Privacy Officer has appointed Julie Hegyi, Benefits Specialist, 125 East Second Street, Monroe, Michigan 48161, Telephone number (734)-240-7253 as the Contact Person. The Contact Person is available to answer Participants' questions, concerns or complaints about the privacy of their PHI and to carry out any other duties assigned to her by the Privacy Officer or pursuant to these Privacy Policies and Procedures.

**Section 2.2** **HIPAA Security Officer**. The Employer has appointed the Colleen Hinzman, 125 East Second Street, Monroe, Michigan 48161, Telephone number (734)-240-7267, as the Security Officer**.** The Security Officer is responsible for developing and implementing policies and procedures to ensure compliance with HIPAA's security rules.

**Section 2.3** **Access to PHI.** Access to PHI is limited to the following employees of or positions within the Employer:

- Privacy Officer;
- Contact Person;
- Security Officer;
- Human Resources Personnel or designee;

These employees with authorized access to PHI or EPHI are referred to as Authorized Employees. No other persons shall have access to PHI or EPHI. Authorized Employees who have authorized access to PHI or EPHI only shall use and disclose PHI or EPHI to the extent necessary to perform the plan administration functions that the Employer performs for the Plan. The Employer will ensure that the adequate separation provisions required under this Section 2.3

will be supported by reasonable and appropriate security measures to the extent the persons designated above create, receive, transmit or maintain EPHI on behalf of the Plan.

**Section 2.4 Workforce Training**. The Privacy Officer, Contact Person and/or Security Officer will provide special HIPAA training to Authorized Employees to the extent that the Employer is receiving, using, disclosing or maintaining PHI on behalf of the Plan. HIPAA training will include developing training schedules and programs so that Authorized Employees receive the training necessary and appropriate to permit them to carry out their functions with respect to the Plan in a manner that complies with HIPAA and these Privacy and Security Policies and Procedures. If training is necessary, then:

(a) This document shall serve as the training materials and the Privacy Officer may develop any additional materials deemed necessary to train Authorized Employees on compliance with the requirements of this Policy and the standards, implementation specifications and other requirements of the HIPAA Rules. The Privacy Officer shall maintain a copy of any such training materials.

(b) Any new designated Authorized Employees shall complete HIPAA training within 30 days of becoming an Authorized Employee. Material changes in these HIPAA Policies will necessitate retraining within 90 days of the material change.

(c) All training will be documented by a signed copy of an Employee Confidentiality Agreement. The Employee Confidentiality Agreement is available from the Privacy Officer and will be retained for at least six (6) years in the employee file.

**Section 2.5 Technical and Physical Safeguards and Firewall**. The Employer and Authorized Employees will take reasonable steps to protect PHI in any form (paper, electronic, etc.) from unauthorized use, access or disclosure. The following technical and physical safeguards are established to prevent PHI or EPHI from intentionally or unintentionally being used or disclosed in violation of HIPAA and these Policies and Procedures:

(a) Personnel Security. The Privacy Officer will maintain a record of the names of all Authorized Employees.

(b) Computer System Management. To the extent that the Employer, on behalf of the Plan, transmits or maintains any EPHI, then the specific security measures outlined in Section 2.7 shall apply. Generally, there are various gate-keeping mechanisms on the Employer's computer system to maintain controlled access to PHI or EPHI and also to ensure the integrity of the information. They are as follows:

(1) *Virus Checking Software* - The Employer's computer network contains virus-checking software with the purpose of ensuring that information on the network will not be compromised and also prevents any security Breaches.

(2) *Firewalls* – The Employer depends on security software to secure its computer files and folders located on its network drives. Each employee creates a personal password in order to access the network. Employees are not to share network passwords with others and are required to periodically change their passwords to ensure security.

Employees also are instructed to logoff of the network or enable a password protected screensaver when stepping away from their workstations. The Employer instructs Authorized Employees to use the following standards to establish a complex password:

- At least six alphanumeric characters long.
- Contain characters from at least three (3) of the following four (4) groups; *upper case* (A-Z), *lower case* (a-z), *digits* (0-9), and *punctuation characters* (!@#$%^&*()_+|~-+\’{}[]:”;"<>?,./)(;).
- Not a word in any language, slang, dialect, or jargon.
- Not based on personal information such as family names.
- Do not use the same password for Employer accounts as use for Employee’s non-Employer accounts (personal ISP account, securities trading, benefits, etc.).
- Where possible, use different passwords for different Employer access needs.
- Do not reveal or share password(s) with anyone, including administrative assistants or secretaries. All passwords are to be treated as confidential Employer information.
- Do not use the “Remember Password” feature of applications (e.g., Outlook).
- Do not write passwords and store them in Employee’s office. Do not store passwords in any computer file, including Palm Pilots or similar devices, without encryption.

(c) WorkStation and Paper Records Security. Authorized Employees are instructed to lock all records and documents containing PHI in a security approved location before leaving the desk and to remove PHI from sight of non-authorized individuals immediately when approached. Each location/department shall make reasonable efforts to ensure that visual PHI is protected from unauthorized disclosure. This should include reasonable positioning of computer screens and other devices that display PHI to limit unauthorized view. Files and documents that are to be discarded should be placed in designated locked containers for shredding or shredded. The Authorized Employee shall make a reasonable effort to ensure that exchanges that contain PHI occur in private areas.

(d) Facsimiles and Printers. Authorized Employees are instructed to transmit and receive facsimiles or printing documents containing PHI in a manner which ensures the security and privacy of such PHI, including personally sending and/or receiving such facsimiles, promptly removing it from printers and facsimile machines and not leaving it on counter tops and desktops in unsecure areas. Printers and facsimile machines will be located in areas that minimize exposure of PHI to unauthorized persons.

(e) Internal Audit Procedures. At least once each year, the Privacy Officer will verify that no one other than Authorized Employees have access to electronic key cards, computer passwords, or file cabinet keys to areas containing PHI or EPHI. The Privacy Officer also will audit all authorization forms once each year to ensure validity. Those which are no longer valid, will be maintained in a separate file for six years.

(f) Authorized Employee Termination Procedures. When an Authorized Employee leaves the Employer, the Human Resources Department will meet with such Authorized

Employee on the last day and follow the termination checklist to deny future access to PHI. Items relevant to PHI on the checklist include:

- Information Technology Department removes the terminated employee's network access, e-mail access, and voice mail system access at the end of the last business day of employment; and

- The terminated employee turns in any electronic key cards and/or file cabinet keys on the last day of employment.

(g) Inquiry Procedure. Inquiries involving PHI from spouses, parents, providers and other individuals will be directed to the Contact Person. The Contact Person will require an Authorization form or power of attorney documentation before assisting an individual in his or her inquiries about a Participant's records containing PHI, unless such individual is the parent of a minor, dependent child. Once an Authorization form is completed, the Employer will keep it on file and it will remain in effect unless revoked.

Provider inquiries regarding verification of coverage and benefits relating to the release of a Participant's PHI generally will be directed to the applicable third party administrator for the Plan.

**Section 2.6 Security Risk Analysis**. The Plan has no employees. All of the Plan's functions, including creation and maintenance of its records, are carried out by the Authorized Employees of the Employer, insurers and/or by Business Associates. The Plan does not own or control any of the equipment or media used to create, maintain, receive and transmit EPHI relating to the Plan, or any facilities in which such equipment and media are located. Such equipment, media and facilities are owned or controlled by the Employer, insurers and/or Business Associates. Accordingly, the Employer, insurers and/or Business Associates create and maintain all of the EPHI relating to the Plan, own or control all of the equipment, media and facilities used to create, maintain, receive or transmit EPHI relating to the Plan and has control of its employees, agents and subcontractors that have access to EPHI relating the Plan. The Plan has no ability to access or modify any potential risks and vulnerability to the confidentiality, integrity and availability of EPHI relating to the Plan – that ability lies solely with the Employer, insurers and/or any appointed Business Associate.

Because the Plan has no access to or control over any EPHI relating to the Plan, the Plan will not directly implement most of the security standards (including the implementation specifications associated with them) established under HIPAA and set out in Subpart C of 45 CFR Part 164. However, the Plan, through the Employer, has implemented the following security measures:

(a) Appointed a Security Officer (see Section 2.2).

(b) Performed and documented this security risk analysis (as set forth in this Section 2.6 and Section 2.7).

(c) Entered into Business Associate Agreements that require the Business Associates to implement certain security standards with respect to EPHI maintained or transmitted by the Business Associate (see Section 3.5).

(d) Adopted a Plan Amendment under which the Employer certifies and agrees to implement certain security measures with respect to EPHI maintained or transmitted by the Employer, as plan administrator (see Sections 2.7 and 2.13).

(e) Instructed the Security Officer to periodically perform a security evaluation to determine whether there are any administrative, environmental or operational changes affecting the security of EPHI that would require a change in this security risk analysis.

**Section 2.7 The Employer's Security Obligations**. The Plan, through the Employer, has entered into third party administrative and business associate agreements with Business Associates and/or entered into fully-insured contracts with insurance carriers to perform all administrative functions on behalf of the Plan. As a result, the Authorized Employees of the Employer generally will not use, maintain, disclose or transmit PHI or EPHI on behalf of the Plan. The Employer, in its capacity as the employer, typically will have access only to certain enrollment and disenrollment information regarding the Plan's participants (including participant name, social security number and election amount under the Plan) and to Summary Health Information.

However, if the Employer maintains or transmits any EPHI in relation to administering the Plan, the Employer will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI, and it will ensure that any agents (or subcontractors) to whom it provides such EPHI agree to implement reasonable and appropriate security measures to protect the information. The Employer will report to the appointed Security Official any Security Incident of which it becomes aware and will implement reasonable and appropriate security measures to ensure that only Authorized Employees have access to EPHI. The Employer will satisfy its security obligations, if any, described in this paragraph by implementing those security standards and implementation specifications (as summarized in Attachment A and further set forth in HIPAA) that it deems reasonable and appropriate for the security of any EPHI that the Employer actually maintains or transmits on behalf of the Plan.

**Section 2.8 Complaint Procedures**. Any complaints regarding a violation of the HIPAA privacy standards should be reported to the Contact Person and any complaints regarding a violation of the security standards should be reported to the Security Officer. The complaint must be in writing and must describe the acts or omission the individual believes to have occurred, the date the act or omission occurred, the description of the PHI affected and how it was affected, and the name(s) of anyone who may have improperly been provided with the PHI. The complaint will be date-stamped upon receipt.

The Contact Person or Security Officer will investigate and resolve any such complaint within a reasonable time period (i.e. generally within thirty (30) days from receipt of the complaint, but if additional time is necessary, the individual generally will be notified of the delay and informed of the expected timeframe for completion of the review). All complaint investigations will be handled confidentially and involve only those individuals necessary to complete the investigation. Confidentiality of the person who discloses an alleged Breach of privacy or security standards will be maintained where possible, but cannot be guaranteed as the investigation may require discussion with witnesses or other involved individuals.

If there are no findings in the investigation to substantiate the complaint, the Contact Person or Security Officer will communicate this to the complainant in writing. However, if there are findings to support the complaint, the Contact Person or Security Officer will work to resolve the complaint in a manner consistent with these Policies and Procedures, including:

- Determining if performance or training needs to be improved, if a change in the departmental operation is needed, and if any sanction, mitigation efforts or reporting to other entities is required;
- Notifying appropriate administrative representative, staff or committees of the action needed; and
- Initiate employee discipline action as necessary in accordance with Section 2.9 below.

It is the Employer's intention to resolve all supported complaints in a timely and efficient manner.

**Section 2.9 Sanctions for Violations of Privacy or Security Standards**. Any individual who is found to use or disclose PHI or EPHI in violation of these HIPAA Privacy and Security Policies and Procedures will be disciplined in accordance with the Employer's Code of Conduct/Ethics Policy and or employees Collective Bargaining Agreement, which could include disciplinary notification placed in employee file, suspension, or immediate discharge of employment. The type of discipline issued will be determined based upon the factors of the situation to include the severity and impact of the violation or Breach of security.

For example, the Privacy or Security Officer may, in its discretion, take the following disciplinary action in response to the following Breaches:

- Sanction: Disciplinary notification placed in file if there is an inadvertent and inappropriate release of PHI within the Plan's Workforce or to a business associate or other covered entity.

- Sanction: Disciplinary notification placed in file and possible suspension if there is an inadvertent and inappropriate release of PHI to an external source other than a business associate or other covered entity.

- Sanction: Disciplinary notification placed in file, suspension, and possible discharge if there is a deliberate and inappropriate release of PHI.

- Sanction: Immediate discharge if there is a deliberate and inappropriate release of PHI with intent to harm the individual or intent of financial gain.

**Section 2.10 Mitigation of Inadvertent Disclosures**. The Employer will mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of any Participant's PHI or EPHI in violation of these HIPAA Privacy and Security Policies and Procedures. As a result, the Employer will instruct employees who become aware of a disclosure of PHI or EPHI, either by an employee of the Employer or an outside party, that is not in compliance with HIPAA to immediately contact the Privacy or Security Officer so that the

appropriate steps to mitigate the harm to the Participant can be taken. Mitigation of any harmful effects known to the Plan is at the discretion of the Privacy Officer but may involve:

- Apologies;
- Requests to other entities for special safeguards;
- Requests to other entities for retrieval of PHI; and/or
- Financial penalties.

**Section 2.11 Notification Requirements in the case of Breach of Unsecured PHI**.

(a) To the extent required by ARRA, the Plan (through the Privacy Officer) shall undertake certain notification obligations upon discovering a Breach of Unsecured PHI. These notification obligations under ARRA will apply to Breaches that have occurred on or after 30 calendar days from the publication of the DHHS interim final regulations issued on August 24, 2009 (i.e. September 23, 2009).

(b) If the Plan undertakes steps to secure PHI through the use of technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals, then the Plan will not be required to satisfy the notification obligations upon a Breach of secured PHI. On August 24, 2009, DHHS issued guidance regarding the securing of PHI, which can be found at http://www.hhs.gov/ocr/privacy (or Federal Register Vol. 74, No. 162, page 42740, Aug. 24, 2009) and will be annually updated by HHS.

(c) In the case of a Breach of Unsecured PHI, the Plan must provide notice to the affected individuals without unreasonable delay and in no case later than 60 days after discovery of the Breach of Unsecured PHI. A Breach shall be treated as discovered by the Plan as of the first day on which such Breach is known to the Plan, or, by exercising reasonable diligence, would have been known, to the Plan. The Plan will be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach) who is a workforce member or agent of the Plan.

(d) The Plan's notice of the Breach to the affected individual must be written in plain language and include:

(1) A brief description of the events surrounding the Breach, including the date of Breach and the date of discovery of the Breach, if known;

(2) A description of the types of information involved (such as full name, social security number, date of birth, home address, account number, disability code, or other types of information that were involved);

(3) Any steps individuals should take to protect themselves from the potential harm arising from the Breach;

(4) A description of the steps the Plan is taking to investigate and mitigate the harm and to protect against further Breaches; and

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

(e) The notice must be delivered using a method consistent with ARRA and additional guidance by ARRA, including:

(1) Written notice to the individual at the last known address of the individual by first-class mail (or by electronic mail if specified or agreed to by the individual);

(2) If the Plan knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification to the next of kin or personal representative.

(3) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, a substitute form of notice that is reasonably calculated to reach affected individuals must be provided (e.g. by phone or other means).

(4) In the case in which of 10 or more individuals for which there is insufficient contact information, then substitute notice must either be in the form of a conspicuous posting (for a period of 90 days) on the home page of the website of the Employer, or notice in a major print or broadcast media in geographical areas where the individuals affected by the Breach are likely to reside. Such notice must include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be affected by the Breach.

(5) In the case deemed by the Plan to require urgency because of possible imminent misuse of the Unsecured PHI, the Plan may provide the notice by telephone or other means, as appropriate, in addition to providing the written notice referenced above.

(f) If the Breach of Unsecured PHI involves less than 500 individuals, the Plan must maintain a log and annually submit such log not later than 60 days after the end of each calendar year to the DHHS in the manner specified on the DHHS Website.

(g) If the Breach of Unsecured PHI is reasonably believed to affect more than 500 individuals, notice also must be provided to prominent local media outlets for publication within the State or jurisdiction in which the affected individuals reside. The Plan must notify the media without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach. The Plan also must, contemporaneously with the written notice provided to the affected individuals, also notify the DHHS in the manner specified on the DHHS Website. (Media and DHHS notification may be delayed under certain law enforcement delay requests as set forth in 45 CFR §164.412). DHHS will establish a website listing such Breaches.

**Section 2.12** **No Retaliation or Waivers**. The Employer may not intimidate, threaten, coerce, discriminate against or take other retaliatory action against individuals for exercising their rights,

filing a complaint, participating in an investigation or opposing any improper practice under HIPAA.

No individual will be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

**Section 2.13 Notice of Privacy Practice**.

(a) The Employer, on behalf of the Plan, will develop and maintain a Notice of Privacy Practices that includes:

- The header language required by the HIPAA Rules.
- A description of the types of Uses and Disclosures the Plan is permitted to make for Treatment, Payment and Health Care Operations with an example of each.
- A description of each of the other purposes for which the Plan is permitted or required to use PHI without individual authorization.
- A description of any more stringent law that might prohibit or materially limit Use and Disclosure as described in the Notice.
- Sufficient detail to place the individual on notice of allowable and required Uses and Disclosures.
- A statement that all other Uses and Disclosures may be made only with individual authorization and the individual's right to revoke authorization.
- A description of the individual's rights with respect to PHI and how to exercise those rights.
- A statement that the Plan is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI.
- A statement that the Plan is required to abide by the terms of the Notice currently in effect.
- A statement of the Plan's right to change the terms of the Notice and how individuals will be notified of a change.
- A statement of how the individual may complain to the Plan and to the Secretary.
- The name, title, telephone number of the person or office to contact for further information.

- The effective date of the Notice.

- A statement that the Plan may disclose PHI to the Plan Sponsor.

(b) The Notice will be individually delivered to all Participants and may be included with other information or mailings sent to the Participants. It may be included with paychecks, newsletters, enrollment materials, or SPDs; however, it may not be included or combined with a privacy Authorization form. It is not necessary to deliver a notice to all covered dependents as delivery to a covered employee is effective for all his or her dependents.

To the extent other employment notices are electronically posted, the Employer also will electronically post the Notice of Privacy Practices at the same location. This is not, however, a substitute for the required, individually delivered notice, and any individual who is the recipient of an electronic Notice retains the right to obtain a paper copy of the Notice upon request. The Notice of Privacy Practice will be sent to Participants as follows:

- To all Participants in the Plan no later than April 14, 2003;

- To any new Participant who enrolls in the Plan after the date that the Notice was initially provided to all Plan Participants; and

- To all Participants within 60 days after a material change to the Notice.

The Employer also will inform Participants of the availability of this Notice of Privacy Practices at least once every three years.

(c) Revisions to the Notice must be approved by the Privacy Officer. The Privacy Officer will evaluate whether a revision is material and whether the Notice must be redistributed.

**Section 2.14 Plan Document and Employer Certification**. The Plan may disclose PHI to the Employer only after the Employer has adopted a HIPAA Privacy Plan Amendment that incorporates the following provisions and under which the Employer expressly agrees to:

- Not use or further disclose PHI other than as permitted by the Plan or as required by law;

- Ensure that any agents, including a subcontractor, to whom it provides PHI agree to the same restrictions and conditions that apply to the Employer with respect to such PHI;

- Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Employer;

- Report to the Privacy Officer any use or disclosure of the PHI that is inconsistent with the uses or disclosures for which the PHI was provided of which it becomes aware;

- Make available to an individual PHI about the individual, as required by law;

- Make PHI available for amendment by the individual and incorporate amendments requested by the individual, as required by law;

- Make available the information needed to account for disclosures of PHI;

- Make available to the Secretary its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan for purposes of determining the Plan's compliance with the privacy standards of HIPAA;

- If feasible, return or destroy all protected health information received from the Plan that the Employer still maintains in any form and retain no copies of such PHI when it is no longer needed for the purpose for which it was disclosed, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make it unfeasible to return or destroy the PHI;

- Ensure that there is adequate separation between the Plan and the Employer in order to comply with these restrictions on the use or disclosure of PHI or the security of EPHI; and

- To the extent that the Employer creates, receives, maintains or transmits any EPHI on behalf of the Plan, the Employer will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI, and it will ensure that any agents (including subcontractors) to whom it provides such EPHI agree to implement reasonable and appropriate security measures to protect the information.

**Section 2.15 Amendment or Termination of Policies or Procedures**. The Employer reserves the right to amend, change or terminate these Policies or Procedures at any time without notice. No third party rights (including but not limited to Plan Participants, beneficiaries or Business Associates) are intended to be created by these Policies and Procedures. To the extent these Policies and Procedures establish requirements and obligations above and beyond those required by HIPAA, the Policies and Procedures will be aspirational and will not be binding upon the Employer.

**Section 2.16 Documentation and Record Retention**. The Employer, on behalf of the Plan, implements these HIPAA Privacy and Security Policies and Procedures to document its compliance efforts with HIPAA. The Privacy Officer will periodically review and update these policies and procedures as necessary in response to environmental or operational changes affecting the privacy or security of PHI or EPHI or changes in applicable law; the Privacy Officer will promptly document any such changes. If a communication is required by the HIPAA Rules or the Plan's policies and procedures to be in writing, the Privacy Officer shall maintain or cause to be maintained such writing, or an electronic copy as documentation. If the Plan is required by the HIPAA Rules or the policies and procedures to document an action,

activity or designation, the Privacy Officer shall maintain or cause to be maintained a written or electronic record of such action, activity or designation. The Privacy Officer also will follow the Documentation Procedure, as defined in Article V below. Any documentation may be maintained in written or electronic form.

The Employer will maintain a record of these HIPAA Privacy and Security Policies and Procedures and all other HIPAA documentation (including the HIPAA Plan Amendment, Notice of Privacy Practices, Business Associate Agreements, Authorizations, complaints, and any required documentation of certain uses or disclosures of PHI) for a period of at least six years from the date of creation or the date last in effect, whichever is later. These policies and procedures will be made available to any person responsible for implementing the procedures to which the documentation pertains, including the Privacy or Security Officer, any Authorized Employee or any Business Associate.

## ARTICLE III
## POLICIES ON USE AND DISCLOSURE OF PHI

**Section 3.1** **General Policy**. The Employer intends to comply fully with HIPAA and to require all members of the Employer's workforce to comply with these HIPAA Privacy and Security Policies and Procedures. Reference to PHI throughout this Article III will include a reference to EPHI to the extent any EPHI is transmitted or maintained by the Employer on behalf of the Plan. Access to PHI will be limited to those members of the Employer's workforce who as part of their job responsibilities need to have access to PHI for Plan administrative purposes. These workforce members are named in Section 2.2 above and are referred to as Authorized Employees.

**Section 3.2** **Permitted Uses or Disclosures of PHI**.

(a) Plan Administration Functions.

(1) An Authorized Employee may use and disclose a Plan Participant's PHI to perform the Plan's own payment, operation, audit or other administration activities. Permitted disclosures pursuant to these activities include:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- Risk adjusting based on enrollee status and demographic characteristics;
- Billing, claims management, collection activities, payment activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;
- Reviewing health plan performance;
- Underwriting and premium rating;

- Business planning and development; and

- Business management and general administrative activities.

(2) PHI also may be disclosed to another covered entity (e.g. a health care provider) for purposes of the other covered entity's payment activities, quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the Participant and the PHI requested pertains to that relationship.

(b) Mandatory Disclosures of PHI. A Participant's PHI must be disclosed in two situations:

(1) The individual who is the subject of the PHI requests disclosure of PHI. Prior to any disclosure under this paragraph, the Employer will follow the procedures outlined in Section 4.1 regarding a Participant's request for access to PHI.

(2) The Department of Health and Human Services (DHHS) requests disclosure of PHI for purposes of enforcing the provisions of HIPAA. Prior to any disclosure to DHHS, the Employer will follow the Verification Procedure.

(c) Permissive Disclosures of PHI. A Participant's PHI may be disclosed for the following reasons:

(1) Disclosures may be made about victims of abuse, neglect, or domestic violence (i) if the individual agrees to the disclosure or (ii) the disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or the victim), or the individual is incapacitated and unable to agree, and the PHI will not be used against the individual and is necessary for any imminent enforcement activity. With respect to sub-paragraph (ii), the individual will be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

(2) For judicial and administrative proceedings in response to (i) an order of a court or an administrative tribunal or (ii) a subpoena, discovery request or other lawful process, not accompanied by a court or administrative order, 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.

(3) To a law enforcement official for law enforcement purposes, under the following conditions:

- Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.

- Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.

- Information about a suspected victim of a crime (i) if the individual agrees to disclosure; or (ii) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.

- Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

- Information that constitutes evidence of criminal conduct that occurred on the Employer's premises.

(4) To Appropriate Public Health Authorities for Public Health Activities.

(5) To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

(6) 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.

(7) For Cadaveric Organ, Eye or Tissue Donation Purposes, 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.

(8) For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

(9) To Avert a Serious Threat to Health or Safety, 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.

(10) For Specialized Government Functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.

(11) For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

(d) Minimum Necessary Standard, Documentation Procedure and Privacy Officer Approval. Any use or disclosure of PHI permitted or required under this Section 3.2 will satisfy the Minimum Necessary Standard and follow the Documentation Procedure. An Authorized Employee will receive the Contact Person's approval prior to the use or disclosure of PHI under any of the circumstances specified in Section 3.2(a)(2), (b) and (c).

**Section 3.3** **Use or Disclosure for Purposes of Non-Health Benefits**. Generally, a Participant's PHI may not be used for purposes of payment, operation or other administrative functions of the non-healthcare components of the Plan and the Employer's other non-health benefit plans (e.g. disability and life insurance, etc), or of any other non-Plan activity such as employment related decisions, unless each of the following requirements are satisfied:

(a) An Authorization is received;

(b) The Privacy Officer approves the use or disclosure for non-Plan purposes;

(c) The disclosure satisfies the Minimum Necessary Standard; and

(d) The Documentation Procedures are followed.

**Section 3.4** **Disclosures of PHI Pursuant to an Authorization**. PHI may be used or disclosed for any purpose if the Participant provides an Authorization. If the Employer uses or discloses PHI pursuant to an Authorization, the following policy or procedure will apply:

(a) The Employer will use or disclose PHI only in a manner that is consistent with the terms and conditions set for in the Authorization.

(b) The Employer will verify that the Authorization form is valid. An Authorization is valid only if each of the following conditions are satisfied:

(1) The form is properly signed and dated by the individual or the individual's authorized representative;

(2) The form contains an expiration date which is a specific date (e.g. January 1, 2005), 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 (e.g. for the duration of the individual's Plan coverage);

(3) The form is not expired or revoked;

(4) The form contains a description of the PHI to be used or disclosed;

(5) The form contains the name of the entity or person authorized to use or disclose PHI;

(6) The form contains a statement regarding the individual's right to revoke the Authorization and the procedures for revoking Authorizations; and

(7) The form contains a statement regarding the possibility for a subsequent re-disclosure of PHI.

(8) A statement to the effect that the Plan may condition enrollment in the Plan or eligibility for benefits from the Plan on provision of an authorization requested by the Plan prior to an individual's enrollment in the health plan, if the authorization

sought is for the Plan's eligibility or enrollment determinations relating to the individual or for the Plan's underwriting or risk rating determinations and the authorization is not for a use or disclosure of psychotherapy notes.

(c) The Employer will follow the Verification and Documentation Procedures for each Authorization.

**Section 3.5 Disclosures of PHI to Business Associates**.

(a) The Plan may contract with individuals or entities known as Business Associates to perform various functions or to provide certain types of services on the Plan's behalf. In order to perform these functions or provide these services, the Business Associates will receive, create, maintain, transmit, use and/or disclose a Participant's PHI or EPHI. HIPAA requires that all Business Associates agree in writing with the Plan to comply with HIPAA's privacy and security rules in connection with any PHI or EPHI.

The Privacy Officer will identify all Business Associates and ensure that a Business Associate Agreement has been executed between the Plan (or the Employer, on behalf of the Plan) and the applicable Business Associate. The Business Associate Agreement will contain the following terms:

(1) Limit the Business Associate's uses and disclosures to solely those uses and disclosures that would be allowed for the Plan under HIPAA, and prohibit the Business Associate from disclosing such information further;

(2) Require the Business Associate to implement safeguards to prevent the improper use and disclosure of PHI;

(3) Require the Business Associate to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI that the Business Associate creates, receives, maintains or transmits on behalf of the Plan;

(4) Require the Business Associate to report to the Plan (through the Privacy or Security Officer) any improper use or disclosure of PHI, or any Security Incident of which the Business Associate becomes aware.

(5) Require the Business Associate to notify the Plan of any Breach of Unsecured PHI without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach. A Breach shall be treated as discovered by a Business Associate as of the first day on which such Breach is known to the Business Associate, or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach) who is an employee, officer or other agent of the Business Associate. The Business Associate's notice to the Plan under this paragraph shall, to the extent possible, include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to

have been, accessed, acquired, used or disclosed during the Breach and provide any other available information to the Plan to enable the Plan to satisfy its Breach notification obligations under Section 2.11 above.

(6) Require the Business Associate to impose the same requirements on all of the Business Associate's subcontractors;

(7) Require the Business Associate to make available PHI in compliance with the individuals' rights to access, amend and receive an accounting related to PHI;

(8) Require the Business Associate to make its internal books and records available to DHHS for purposes of determining the covered entity's compliance with HIPAA;

(9) Require the Business Associate to return or destroy PHI or EPHI, if feasible, upon the termination of the relationship between the Business Associate and the Plan; and

(10) Authorize the Plan to terminate the Business Associate Agreement if the Business Associate has violated a material term of the Agreement, or if termination of the Agreement is not feasible, the Plan may report the Business Associate's violation of HIPAA to DHHS.

(b) Before providing any PHI or EPHI to a Business Associate, an Authorized Employee will:

(1) Contact the Privacy Officer and verify that a business associate agreement is in place;

(2) Disclose PHI in a manner that is consistent with the applicable Business Associate Agreement; and

(3) Satisfy the Minimum Necessary Standard and follow the Documentation Procedure.

(c) Privacy Violations by a Business Associate

(1) If a Plan employee or other staff personnel knows or has reason to believe that a Business Associate of the Plan is inappropriately using or disclosing PHI, whether the PHI was received by the Plan or not, the employee or other staff personnel is required to notify the Privacy Officer immediately regarding the suspected violation.

(2) Upon receiving notice of an alleged or actual violation of a Business Associate Agreement from any source, including notice obtained through individual complaints and reports from Plan personnel, the Privacy Officer will initiate a review of the conduct or activities at issue.

(3) If the Privacy Officer determines that the complaint, report or other form of notice contains substantial and credible evidence of violations by a Business Associate, the Privacy Officer will commence a formal investigation into the conduct or activities of the Business Associate.

- If the investigation reveals that a Business Associate has violated its agreement with the Plan, the Privacy Officer shall notify legal counsel immediately.

- If the Privacy Officer and/or legal counsel determine that the Business Associate has committed a material Breach or violation of its obligations under the Business Associate Agreement, the Privacy Officer, with the assistance of legal counsel, must take reasonable steps to remedy the Breach or terminate the contract of a Business Associate when feasible. If termination of the contract is not feasible, the Plan must report the problem to the Secretary of DHHS.

**Section 3.6 Requests for Disclosure of PHI from Family Members or Friends**. The Plan and Employer will not disclose PHI to family and friends of a Participant except as follows:

(a) The spouse, family member or personal friend is either the parent of the Participant who is a minor child or the personal representative of the Participant, **and** the Verification Procedure and the procedures outlined in Section 4.1 regarding a Participant's request for access to PHI are followed.

(b) All other requests from a third party to access PHI of a Participant requires an Authorization.

**Section 3.7 Disclosures of De-Identified Information**. The Plan and the Employer may freely use and disclose De-identified Information. Prior to any use or disclosure, the Privacy Officer or Contact Person will verify that the information qualifies as De-identified Information.

It is the policy of the Plan to consider requests for production and sharing (pursuant to a data use agreement) of limited data sets for the purpose of research, public health or health care operations. The Plan retains complete discretion as to whether to disclose a limited data set.

**Section 3.8 Limited Data Sets.**

It is the policy of the Plan to consider requests for production and sharing (pursuant to a data use agreement) of limited data sets for the purpose of research, public health or health care operations. The Plan retains complete discretion as to whether to disclose a limited data set.

The Plan may use PHI to create a limited data set that meets the requirements of §164.514(e)(2) of the HIPAA Rules or disclose PHI only to a business associate for such purpose.

(a) Limited data sets must meet the requirements of §164.514(e)(2) and (e)(3) of the HIPAA Rules.

(b) The recipient of a limited data set must enter into a data use agreement that meets the requirements of §164.514(e) of the HIPAA Rules.

(c) If we know of a pattern of activity or practice of the limited data set recipient that constitutes a Breach of the data use agreement, we must take reasonable steps to cure by placing the recipient on written notice of the Breach and specifying a cure period.

(d) If any Breach remains uncured, we will discontinue the data use agreement and make a report to the Secretary.

**Section 3.9 Hybrid Entity Election.** The Employer's Welfare Benefit Plan offers a healthcare component and a non-healthcare component. As a result, HIPAA may treat such Plan as offering a healthcare component and a non-healthcare component and consequently, it may be considered a "hybrid entity" as defined under Section 45 CFR 164.103 of HIPAA. The healthcare component of the Welfare Benefit Plan consists solely of the Group Health Plans mentioned on the first page of these policies. The non-healthcare component of the Plan consists of all other benefits under the Welfare Benefit Plan, including Dependent Care Spending Account, Life Insurance/Accidental Death and Dismemberment, and Disability Plans. The Employer intends to comply with HIPAA with respect to only the healthcare component of the Plan and to ensure adequate separation between the healthcare component and the non-healthcare component as if such healthcare component and non-healthcare component were separate and distinct plans. In this regard and to the extent required by HIPAA, the Employer will ensure compliance with the safeguard requirements set forth in 45 CFR 164.105(a) relating to hybrid entities, including ensuring that:

(a) The healthcare component does not disclose PHI to the non-healthcare components.

(b) The healthcare component protects the security of electronic PHI from the non-healthcare component.

(c) Any Business Associate of the healthcare component complies with the requirements of subparagraphs (a) and (b) above.

If an Authorized Employee performs duties for both the healthcare component and non-healthcare component, such Authorized Employee will not use or disclose PHI created or received in the course or incident to the Authorized Employee's work for the healthcare component in a manner prohibited by HIPAA (e.g. for purposes of administering or making benefit determinations for the non-healthcare component).

## ARTICLE IV
## POLICIES AND PROCEDURES ON INDIVIDUAL RIGHTS

**Section 4.1 Access to PHI**. Under HIPAA, each Participant has the right to access and obtain copies of his or her own PHI that the Plan (or the Plan's Business Associates) maintains in Designated Record Sets. A Participant (or the minor Participant's parent or Participant's personal representative) may request access to PHI by providing the Contact Person with a

written request for access to PHI and must specify the designated record set requested, in whole or in part, as:

- Medical records
- Billing records
- Enrollment information
- Payment information
- Claim adjudication records

The Employer (on behalf of the Plan) may charge a reasonable fee for copying, mailing, or summarizing the requested PHI. Upon receipt of a written request to access PHI, the Contact Person will take each of the following steps:

(a) The Contact Person will follow the Verification Procedure.

(b) The Contact Person will review and verify that the requested PHI is held in the Participant's Designated Record Set. If the requested information is not within the Designated Record Set, the Contact Person may deny the request.

(c) The Contact Person will review the request to determine if an exception to the disclosure exists. Circumstances under which access may be denied and no review of the denial request is required by HIPAA include:

- The information requested is psychotherapy notes;
- The information requested is compiled in anticipation of or for the use in a legal proceeding;
- The disclosure would violate the HIPAA Privacy Rule; or
- The information was obtained by someone other than a health care provider under a promise of confidentiality and access would be reasonably likely to reveal the source of information.

Access to an individual's PHI also may be denied under the following conditions:

- A licensed health care professional (LHCP) has determined that the access is reasonably likely to endanger the life or physical safety of the individual or another person;
- The information requested makes reference to another person and a LHCP has determined that the access is reasonably likely to cause substantial harm to the other person; or
- The request is made by the individual's personal representative and the LHCP has determined that the access is reasonably likely to cause substantial harm to the individual or another person.

In these cases, the individual has the right to have the denial reviewed by a LHCP appointed by the Employer who did not participate in the original decision to deny access. An appeal of denial of access to PHI will be addressed to the Contact Person.

(d) The Contact Person will respond to the request by providing the requested PHI or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the Participant within the original 30- or 60-day period of the reasons for the extension and the date by which the Employer will respond.

(e) Any denial of a request for access to PHI will first be approved by the Privacy Officer. A denial of a request to access PHI will include:

- The basis for the denial;
- A statement of the individual's right to request a review of the denial, if applicable; and
- A statement of how the individual may file a complaint concerning the denial.

(f) Before honoring a request to access PHI, the Contact Person will advise the individual of any cost associated with the provision of PHI. If the individual agrees to pay for the cost, the Contact Person will provide the requested PHI in the form of format requested by the individual, if readily producible in such form. Otherwise, the Contact Person will provide the requested PHI in a readable hard copy or such other form as is agreed to by the individual. Generally, the requested PHI may be mailed or e-mailed to the requesting party or inspected at the Contact Person's office, and to the extent required by ARRA, the individual shall have the right to receive any Electronic Health Records in an electronic format selected by the Plan.

(g) The Contact Person will follow the Documentation Procedure.

**Section 4.2** **Right to Amend PHI**. Under HIPAA, each Participant has the right to request an amendment to his or her own PHI that the Plan (or the Plan's Business Associates) maintains in Designated Record Sets. A Participant (or the minor Participant's parent or Participant's personal representative) may request to amend PHI by providing the Contact Person with a written request to amend PHI, which includes the reason to support the requested amendments. Upon receipt of a written request to amend PHI, the Contact Person will take each of the following steps:

(a) The Contact Person will follow the Verification Procedure.

(b) The Contact Person will respond to a request for amendment within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If a determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the Participant within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.

(c) A request for amendment may be denied if:

- The PHI was not created by the Plan, unless the originator of the PHI is no longer available to act on the requested amendment;
- The PHI is not part of the Designated Record Set;
- The PHI is otherwise unavailable for inspection under HIPAA (for the reasons specified in Section 4.1(c) above); or
- The PHI is accurate and complete.

(d) The denial of a Participant's request to amend PHI will include:

- The basis for denial;
- The Participant's right to submit a written statement disagreeing with the denial and how to file such a statement;
- The Participant's right to request that the request for amendment and the denial be included in future disclosures of PHI; and
- A statement of how the individual may file a complaint concerning the denial.

(e) If a request for amendment or correction has been denied, the Plan will permit the Participant to submit a statement disagreeing with the denial and the basis for the denial. A written rebuttal to the Participant's statement of disagreement may be prepared and a copy of the rebuttal will be provided to the Participant.

(f) When an amendment is accepted, the Contact Person will make the change in the Participant's Designated Record Set and provide appropriate notice to the requesting party and all persons or entities listed on the requesting party's request for amendment form, if any, and also provide notice of the amendment to any person who is known to have the particular record and who may rely on the uncorrected information to the detriment of the Participant.

(g) All requests for amendment or correction, denials, statements of disagreement, and rebuttals become part of the Designated Record Set maintained by the Plan.

**Section 4.3** **Request for an Accounting of Disclosure of PHI**. Under HIPAA, a Participant has the right to obtain an accounting of certain disclosures of his or her own PHI. Upon receiving a request from a Participant (or the parent of a minor-child Participant or the Participant's personal representative) for an accounting of disclosures, the Contact Person will take each of the following steps:

(a) The Contact Person will follow the Verification Procedure.

(b) The Contact Person will determine if the Participant requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request. Second and subsequent requests in a 12-month period will be subject to actual fees related to preparing, copying, and mailing such requests. When second and subsequent requests are received, the Contact Person will notify the Participant of the cost and provide an opportunity to withdraw the request.

(c) The Contact Person will respond to an accounting request within 60 days. If the accounting cannot be provided within 60 days, the deadline may be extended for 30 days by providing notice to the Participant within the original 60-day period of the reasons for the extension and the date by which the Employer will respond.

(d) The accounting will include disclosures (but not uses) of the requesting Participant's PHI made by the Plan and any of its Business Associates during the period requesting by the Participant up to six years prior to the request. The accounting will not include disclosures made:

- Prior to April 14, 2003 (i.e. HIPAA's compliance date);
- To carry out treatment, payment, or health care operations;
- To the Participant about his or her own PHI;
- Incident to an otherwise permitted use or disclosure;
- Pursuant to an Authorization;
- For purposes of creation of a facility directory or to persons involved in the Participant's care or other notification purposes;
- As part of a limited data set (as defined by HIPAA); or
- For other national security or law enforcement purposes.

(e) If any Business Associate of the Plan has the authority to disclose a Participant's PHI, then the Contact Person will coordinate with the Business Associate to obtain an accounting of the Business Associate's disclosures.

(f) The accounting will include the following information for each reportable disclosure of a Participant's PHI:

- Date of the disclosure,
- The name of the receiving party,
- A brief description of the information disclosed, and
- A brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

(g) The Contact Person will follow the Documentation Procedure.

(h) Disclosures to carry out treatment, payment or health care operations generally do not have to be included in an accounting. However, ARRA creates an exception to this general rule and provides that an accounting of disclosures to carry out treatment, payment or health

care operations is required if the Plan uses Electronic Health Records (EHR). There is a delayed effective date for such accounting provisions under the ARRA, such that it will apply sometime between January 1, 2011 and January 1, 2014, depending on the circumstances set forth in ARRA. The Plan will comply with such EHR accounting requirements only to the extent applicable to it under ARRA.

**Section 4.4 Request for Confidential Communications**. Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, Participants may ask to be called only at work rather than at home. The Employer will accommodate such a request if the Participant clearly provides information that the disclosure of all or part of that information could endanger the Participant.

An individual requesting alternative communication means or locations must submit the request in writing to the Contact Person. Upon receipt of a request for alternative communications or locations, the Contact Person will take each of the following steps:

(a) The Contact Person will follow the Verification Procedure.

(b) The Contact Person or the Privacy Officer will make a determination as to whether or not the request will be accommodated.

(c) The Contact Person will notify the individual making the request within 60 days as to whether the request will be honored. If the request is denied, the Contact Person will notify the individual in writing as to why the request is being denied.

(d) All requests for alternative communication means or locations that are approved will be tracked and reviewed before any disclosures are made.

(e) All approved requests will be communicated to the appropriate third-party administrator to ensure compliance with the approved request.

(f) All requests and their disposition will be documented to include:

- Date of request for alternative communication means or locations;
- A description of the reason for alternative communication means or locations; and
- A statement of the disposition of the request.

**Section 4.5 Request for Restrictions on Uses and Disclosures of PHI**. An individual, parent of a minor child, or personal representative has the right to request additional privacy protections for:

- Uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations; and

- Disclosures permitted for the involvement of another person in the individual's care and for notification purposes.

The Plan will consider each of these requests, however, the Plan is not required to agree to such restrictions, except in the limited case of self-payment. Effective on and after February 1, 2010, the Plan will honor an individual's request for restriction to the extent required under ARRA when the disclosure is to the Plan for the purpose of carrying out payment or health care operations (and is not for purposes of carrying out treatment) and the PHI pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full by such requesting individual.

Other than this self-payment exception under ARRA, approvals of such requests will be made only in limited circumstances as authorized by the Contact Person or the Privacy Officer.

An individual choosing to request additional privacy protections must submit the request in writing to the Contact Person. Upon receipt of a request for restrictions, the Contact Person will take each of the following steps:

(a) The Contact Person will follow the Verification Procedure.

(b) The Contact Person or the Privacy Officer will make a determination as to whether or not the request will be accommodated.

(c) The Contact Person will notify the individual making the request within 60 days as to whether the request will be honored. If the request is denied, the Contact Person will notify the individual in writing as to why the request is being denied.

(d) All requests for restrictions that are approved will be tracked and reviewed before any disclosures are made.

(e) All approved requests for restrictions will be communicated to the appropriate third-party administrator to ensure compliance with the approved request.

(f) All requests and their disposition will be documented to include:

- Date of request for restriction;
- Description of the reason for restriction; and
- A statement of the disposition of the request.

(g) The Plan may terminate its agreement to restriction, if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or

- The Plan informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to created or received after it has so informed the individual.

## ARTICLE V
## DEFINITIONS

Throughout this document, various terms are used repeatedly. These terms have specific and definite meanings and generally have been capitalized throughout this document. Whenever these terms appear, they will have the meanings set forth below or in HIPAA.

**Section 5.1** **ARRA**. The Health Information Technology for Economic and Clinical Health Act which is part of the American Recovery and Reinvestment Act of 2009 and related regulations or guidance promulgated thereunder.

**Section 5.2** **Authorization**. A Participant's written authorization for the use or disclosure of his or her PHI, which satisfies the requirements specified in Section 3.4(b) above.

**Section 5.3** **Authorized Employee**. Any member of the Employer's workforce who has been authorized access to PHI or EPHI by the Employer. The Employer's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. The term "employee" includes all of these types of workers. The Authorized Employees who have been designated as such by the Employer are listed in Section 2.3.

**Section 5.4** **Breach**. An unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information For these purposes:

- An acquisition, access, use or disclosure is "unauthorized" if there is an impermissible use or disclosure of PHI under HIPAA.

- The security or privacy of PHI is compromised if the acquisition, access, use or disclosure of such PHI poses a significant risk of financial, reputational or other harm to the individual.

Notwithstanding the foregoing, a Breach shall not include acquisition, access, use or disclosures of PHI made under any one of the following situations:

(1) The unauthorized acquisition, access, disclosure or use of PHI is unintentional and made by a workforce member or individual acting under authority of the Plan or its Business Associate if such acquisition, access or use was made in good faith and within the scope of authority of the Plan or Business Associate and does not result in further use or disclosure in a manner not permitted under HIPAA.

(2) Any inadvertent disclosure occurs by a person who is authorized to access PHI within the Plan or at the Business Associate to another person authorized to access PHI within the same Plan or at the same Business Associate, and the information

received as a result of such disclosure is not further used or disclosed in a manner not permitted by HIPAA.

(3) A disclosure of PHI where the Plan or Business Associate has a good faith belief that an unauthorized person to whom such PHI is disclosed would not reasonably have been able to retain such information.

(4) The acquisition, access, use or disclosure of PHI involved a limited data set that excludes the 16 direct identifiers listed in HIPAA regulations §164.514(e)(2), and the dates of birth and zip codes.

**Section 5.5 Business Associate**. A person or an entity that:

(a) Performs or assists in performing a Plan function or activity involving the use or disclosure of PHI (including claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, underwriting, etc.); or

(b) 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.

**Section 5.6 Contact Person**. The individual designated in Section 2.1 to assist the Privacy Officer with HIPAA compliance.

**Section 5.7 DHHS**. The United States Department of Health and Human Services.

**Section 5.8 De-identified Information**. Information that has had 18 specific identifiers removed prior to disclosure and use. The 18 identifiers are as follows:

(a) Names;

(b) All geographic subdivisions smaller than a state, aggregated to the level of a five-digit zip code;

(c) All elements of dates (except year) for dates directly related to an individual, including date of birth (DOB); admission date; discharge date; 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;

(d) Telephone numbers;

(e) Fax numbers;

(f) E-mail addresses;

(g) Social Security numbers;

(h) Medical record numbers;

(i) Health plan beneficiary numbers such as addresses and social security numbers;

(j) Account numbers;

(k) Certificate/license numbers;

(l) Vehicle identifiers and serial numbers, including license plates;

(m) Device identifiers and serial numbers;

(n) Web Universal Resource Locators;

(o) Internet Protocol addresses;

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

(q) Full-face photographic images and any comparable images; and

(r) Any other unique identifying numbers, characteristics, or codes.

**Section 5.9** **Designated Record Set**. A group of records maintained by or for the Plan that includes:

(a) The enrollment, payment, claims adjudication and case or medical management record of a Participant;

(b) Other PHI used, in whole or in part, to make decisions about the Participant.

**Section 5.10** **Documentation Procedure**. When certain uses or disclosures are required to be documented under these Policies and Procedures, the documentation will include:

- The date of the use or disclosure;
- The name of the person who used or disclosed the PHI;
- The name of the entity or person who received the PHI;
- The address of the entity or person who received the PHI;
- A description of the PHI disclosed;
- A statement of the purpose of the disclosure; and
- Any other documentation required by these Policies and Procedures.

**Section 5.11** **Electronic Health Records or EHR**. An electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. The Plan can have EHR if such records are consulted or managed by health care staff working for the Plan who perform activities such as utilization review, disease management and similar health-related activities.

**Section 5.12** **Employer**. **The County of Monroe** and any of its affiliates and subsidiaries who are authorized in writing to participate in the Plan by **The County of Monroe** (collectively referred to as "Employer"), provided, however, that whenever the Plan indicates that the Employer may or shall take any action under the Plan, **The County of Monroe** shall have sole authority to take such action for itself and as agent for any such participating employer.

**Section 5.13** **EPHI or Electronic Protected Health Information**. PHI that is transmitted by or maintained in electronic media. Electronic media is defined as (i) electronic storage media (including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card); or (ii) transmission media used to exchange information already in electronic storage media (e.g. internet, extranet, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage) (but certain transmissions via facsimile or voice mail will not be considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission).

**Section 5.14** **HIPAA**. The Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing privacy and security regulations (see 45 CFR Parts 160 and 164).

**Section 5.15** **Minimum Necessary Standard**. When using or disclosing PHI or when requesting PHI from another Covered Entity, the Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. To that end, the Contact Person will take each of the following steps:

(a) Comply with any new restrictions on the minimum necessary standards under ARRA.

(b) The Contact Person will identify recurring uses or disclosures and identify the information that is necessary for the purpose of the requested use or disclosure and create a policy that limits each use or disclosure to the minimum amount necessary to accomplish the purpose of the use or disclosure. Authorized Employees will then follow such procedures before any use or disclosure is made.

(c) For all other types of uses or disclosures which are not recurring, the Contact Person will review the request for use or disclosure to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of use or disclosure. Among the factors that may be considered in making such a determination are:

- What is the purpose of the disclosure? This could be relevant if the disclosure is not covered by the minimum necessary standard.

- What is the minimum amount of PHI that can be disclosed to accomplish the purpose of the disclosure?

- Are there standards in other industries or among health care providers as to what amount of information is sufficient to fulfill the intended purpose of the disclosure?

- To what extent would the disclosure increase the number of persons with access to the PHI?
- What is the likelihood of further disclosures?
- Can substantially the same purpose be achieved using de-identified information?
- Is there technology available to limit the amount of PHI disclosed?
- What is the cost, financial or otherwise, of limiting the disclosure?

(d) The Minimum Necessary Standard does not apply to any of the following types of uses or disclosures:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual;
- Uses or disclosures authorized by the individual;
- Disclosures made to the Secretary;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

**Section 5.16 Participant**. Any employee of the Employer, his or her covered dependents and any other individual who are or were participating in the Plan.

**Section 5.17 PHI or Protected Health Information**. Information that:

(a) is created or received by the Plan;

(b) relates to (i) the past, present or future physical or mental health or condition of a Participant, (ii) the provision of health care to a Participant, or (iii) the past, present or future payment for the provision of health care to a Participant; and

(c) identifies the Participant or for which there is a reasonable basis to believe the information can be used to identify the Participant.

Protected health information includes information of persons living or deceased.

**Section 5.18 Plan**. The group health plans identified on the first page of this document.

**Section 5.19 Privacy Officer**. HIPAA requires that the Employer appoint a Privacy Officer to ensure compliance with HIPAA. Section 2.1 names the Privacy Officer and describes his or her responsibilities.

**Section 5.20** **Security Incident**. Any attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system, with respect to EPHI.

**Section 5.21** **Security Officer**. HIPAA requires that the Employer appoint a Security Officer to ensure compliance with HIPAA. Section 2.2 names the Security Officer and describes his responsibilities.

**Section 5.22** **Unsecured PHI**. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of DHHS. On August 24, 2009, DHHS issued guidance regarding the securing of PHI, which can be found at http://www.hhs.gov/ocr/privacy (or Federal Register Vol. 74, No. 162, page 42740, Aug. 24, 2009) (which HHS will update annually).

**Section 5.23** **Use and/or Disclosure of PHI**. The use of PHI means sharing, employment application, utilization, examining or analysis of PHI by any person working for or within the Employer or by a Business Associate of the Plan. The disclosure of PHI means any release, transfer, provision of access to or divulging in any other manner of PHI to persons not employed by or working within the Employer.

**Section 5.24** **Verification Procedure**. Authorized Employees will take steps to verify the identity of individuals who request access to PHI. They also will 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 Participant, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access, and under some circumstances, phone verification may be acceptable.

(a) Request Made by a Participant. When a Participant requests access to his or her own PHI, each of the following steps should be followed:

- The Authorized Employee will request a form of identification from the Participant (e.g. a valid drivers license, passport or other photo identification issued by a government agency).

- The Authorized Employee will verify that the identification matches the identity of the individual requesting access to the PHI. If there is any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, the Contact Person or Privacy Officer will be contacted.

- The Authorized Employee will make a copy of the identification provided by the individual and file it with the individual's Designated Record Set.

- Disclosures will be documented in accordance with the Documentation Procedure.

(b) Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor, unemancipated child, each of the following steps should be followed:

- The Authorized Employee will seek verification of the person's relationship with the child. The Plan will treat a custodial parent or the legal guardian of the minor as the personal representative of the minor without the necessity of the Affidavit or documentation unless contradictory information is provided by another parent, guardian or person acting in loco parentis. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.

- Disclosures will be documented in accordance with the Documentation Procedure.

(c) Request Made by Personal Representative. When a personal representative requests access to a Participant's PHI, each of the following steps should be followed:

- The Authorized Employee will request that an Affidavit of Personal Representation (the "Affidavit") be completed along with satisfactory documentation of the personal representation. Satisfactory documentation means:

- A statement appointing a personal representative completed by the adult or emancipated minor who is the subject of the Affidavit;

- A court order; or

- Any other documentation or designation deemed satisfactory by the Privacy Officer.

- If there are any questions about the validity of this documentation, the Contact Person or Privacy Officer will be contacted.

- The Authorized Employee will make a copy of the documentation provided and file it with the Participant's Designated Record Set.

- Disclosures will be documented in accordance with the Documentation Procedure.

(d) Request Made by Personal Representatives of Deceased Individuals. It is the policy of the Plan to protect the PHI of a deceased individual to the same extent as all other PHI. An executor or administrator or other person who under applicable law has authority to act on behalf of a deceased individual or the estate of the individual will be recognized by the Plan as a personal representative of such deceased individual or estate upon completing the Affidavit and attaching acceptable documentation. Acceptable documentation will be considered a court order appointing the person as executor or administrator, letters testamentary or similar evidence

of authority. The Privacy Officer will approve the acceptability of the Affidavit and other documentation from an executor, administrator or similar individual. Once approved, the Affidavit and related documentation will be filed by the Privacy Officer. Disclosures will be documented in accordance with the Documentation Procedure.

(e) Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth in Sections 3.2(b) or (c) regarding mandatory or permissive disclosures of PHI, each of the following steps should be followed to verify the official's identity and authority:

- If the request is made in person, the Authorized Employee will request presentation of an agency identification badge, other official credentials, or other proof of government status. The Authorized Employee will make a copy of the identification provided and file it with the individual's Designated Record Set.

- If the request is in writing, the Authorized Employee will verify that the request is on the appropriate government letterhead.

- If the request is by a person purporting to act on behalf of a public official, the Authorized Employee will 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 official.

- The Authorized Employee will request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, the Authorized Employee will contact the Legal Department.

- The Authorized Employee will obtain approval for the disclosure from the Contact Person or Privacy Officer.

- Disclosures will be documented in accordance with the Documentation Procedure.

(f) Phone Verifications. PHI disclosure may be made by phone. However, Authorized Employees must use judgment in reasonably relying on representations of authority, as follows:

(1) If a caller is the individual who is the subject of the PHI, her or his identity should be verified by SSN and validated by confirmation of other identifying elements from the individual's records (e.g., date of birth,

street address, ZIP code, etc.) For personal representatives, refer to the Personal Representative Affidavit Form.

(2) For callers who are spouses, disclosure should only be made to an enrolled spouse for their own PHI or the PHI of unemancipated children, unless an authorization or Affidavit of Personal Representation is completed.

(3) For callers who are requesting PHI on emancipated children, an Affidavit of Personal Representation must be completed by the emancipated child.

(4) For unemancipated children under the age of 18, the Authorized Employee cannot release PHI except to a parent or legal guardian/personal representative.

(5) For callers requesting PHI on decedents, the Authorized Employee must check for a Personal Representative Affidavit and verify identity.

(6) The Authorized Employee must use judgment to ensure his or her reliance on the caller's identity is reasonable. If the Authorized Employee refuses to release PHI, he or she may tell the caller any steps he or she can take to obtain the PHI (i.e. file an Affidavit of Personal Representation, obtain an authorization, put their request in writing for further information).

(7) Any request for written information from a caller should be put in writing and approved by the Privacy Officer before disclosure.

(8) Claim status, claim inquiry or benefit inquiry calls from health care providers should first be referred to the appropriate third party administrator. If the third party administrator is unable to assist the SSN of the participant should be verified and validated by confirmation of two other identifying elements (e.g., date of birth, street address, ZIP code, etc.)

(9) If the Authorized Employee is aware of the caller's identity and authority to access PHI, via their status as a covered entity, a Business Associate or subcontractor, he or she may disclose PHI in the "ordinary course of business." "Ordinary course of business" means a disclosure, in accordance with the Minimum Necessary Standard, of that type of PHI ordinarily exchanged with the Covered Entity, Business Associate or subcontractor who is known to the Authorized Employee. If the caller is requesting PHI that the Authorized Employee would not ordinarily, on a routine and reoccurring basis, share with the caller, the Authorized Employee should ask for the request to be made in writing along with the purpose for the request, and their authority to make the request.

**Original Effective Date for Privacy Rules: April 14, 2003**
**Original Effective Date for Security Rules: April 21, 2005**
**Restatement Effective Date: February 17, 2009**
**Updated: February 24, 2012**

# ATTACHMENT A
# HIPAA SECURITY STANDARDS

HIPAA security regulations require that a covered entity (e.g. a group health plan) satisfy (i) administrative, (ii) physical, (iii) technical, (iv) organizational and (v) policies and procedures and documentation requirements with respect to any ePHI maintained or transmitted by a covered entity. This Attachment A sets forth the Security Standards and Implementation Specifications under HIPAA's Security Regulations that a covered entity must (or under limited circumstances, may) implement to satisfy its security obligations with respect to EPHI.[1]

## Administrative Safeguards

The following security standards for administrative safeguards require certain administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect EPHI and also to manage the conduct of the covered entity's workforce in relation to the protection of that information.

### *Standard: Security Management Process*

This standard requires the covered entity to implement policies and procedures to prevent, detect, contain, and correct security violations.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Risk Analysis | Required | Make an accurate and thorough assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability of EPHI held by the covered entity. |
| Risk Management | Required | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. |
| Sanction Policy | Required | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. |
| Information System Activity Review | Required | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. |

[1] The implementation specifications under the HIPAA security regulations are identified as required or addressable. If an implementation specification is designated as required, then a covered entity must implement it with respect to EPHI that is maintained or transmitted by the covered entity. If an implementation specification is designated as addressable, then the covered entity must determine whether the specification is a reasonable and appropriate safeguard in its particular security framework. The security regulations sets out a very specific process that a covered entity must follow before it can decide not to implement an addressable implementation specification. See 45 CFR 164.306 for more detail.

### *Standard: Assigned Security Responsibility*

This standard requires the covered entity to identify the security official who is responsible for the development and implementation of the required policies and procedures.

### *Standard: Workforce Security*

This standard requires the covered entity to implement policies and procedures to ensure that all members of the covered entity's workforce have appropriate access to EPHI and to prevent those workforce members who should not have access to EPHI from obtaining access.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Authorization and/or Supervision | Addressable | Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or who work in locations where it might be accessed. |
| Workforce Clearance Procedure | Addressable | Implement procedures to determine that a workforce member's access to EPHI is appropriate. |
| Termination Procedures | Addressable | Implement procedures to terminate access to EPHI when the employment of a workforce member ends, or when it is determined that it is not appropriate for a certain workforce member to have access to EPHI. |

### *Standard: Information Access Management*

This standard requires the covered entity to implement policies and procedures for authorizing appropriate access to EPHI.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Isolate Health Care Clearinghouse Functions | Required | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the rest of the organization. |
| Access Authorization | Addressable | Implement policies and procedures to grant access to EPHI, for example, through access to a workstation, transaction, program, process or other mechanism. |

| | | |
|---|---|---|
| Access Establishment and Modification | Addressable | Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process. |

### *Standard: Security Awareness and Training*

This standard requires the covered entity to implement a security awareness and training program for all members of the covered entity's workforce (including management).

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Security Reminders | Addressable | Implement procedures to distribute periodic security updates. |
| Protection from Malicious Software | Addressable | Implement procedures to guard against, detect, and report malicious software. |
| Login Monitoring | Addressable | Implement procedures to monitor login attempts and to report discrepancies. |
| Password Management | Addressable | Implement procedures to create, change, and safeguard passwords. |

### *Standard: Security Incident Procedures*

This standard requires the covered entity to implement policies and procedures to address security incidents.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Response and Reporting | Required | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. |

### *Standard: Contingency Plan*

This standard requires the covered entity to establish (and implement as needed) policies and procedures to respond to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems that contain EPHI.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Data Backup Plan | Required | Establish and implement procedures to create and maintain retrievable, exact copies of EPHI. |
| Disaster Recovery Plan | Required | Establish (and implement as needed) procedures to restore any loss of data. |
| Emergency Mode Operation Plan | Required | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode. |
| Testing and Revision Procedures | Addressable | Implement procedures for periodic testing and revision of contingency plan. |
| Applications and Data Criticality Analysis | Addressable | Assess the relative criticality of specific applications and data in support of other contingency plan components. |

### *Standard: Evaluation*

This standard requires the covered entity to perform a periodic technical and nontechnical evaluation of security, based initially on the standards implemented under the security rule and, subsequently, in response to environmental or operational changes that effect the security of EPHI, to establish the extent to which the covered entity's security policies and procedures comply with the requirements of the security rule.

### *Standard: Business Associate Contracts and Other Arrangements*

Under this standard, a covered entity may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information in accordance with the applicable provisions of the security rule.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Written Contract or Other Arrangement | Required | Document the business associate's satisfactory assurances through a written contract or other arrangement that meets the requirements of the security rule. |

## Physical Safeguards

The following security standards for physical safeguards require physical measures, policies and procedures to protect a covered entity's electronic information systems, and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

### *Standard: Facility Access Controls*

This standard requires a covered entity to implement policies and procedures to limit physical access to the covered entity's electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Contingency Operations | Addressable | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operation plan. |
| Facility Security Plan | Addressable | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. |
| Access Control and Validation Procedures | Addressable | Implement procedures based on a person's role or function to control and validate his or her access to facilities, including visitor control and control of access to software programs for testing and revision. |
| Maintenance Records | Addressable | Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). |

### *Standard: Workstation Use*

This standard requires the covered entity to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access EPHI.

### *Standard: Workstation Security*

This standard requires the covered entity to implement physical safeguards for all workstations that access EPHI to restrict access to authorized persons.

### *Standard: Device and Media Controls*

This standard requires the covered entity to implement policies and procedures to govern a facility's receipt and removal of hardware and electronic media that contain EPHI and the movement of these items into, out of, and within the facility.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Disposal | Required | Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored. |
| Media Re-Use | Required | Implement procedures for removal of EPHI from electronic media before the media are made available for re-use. |
| Accountability | Addressable | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. |
| Data Backup and Storage | Addressable | Create a retrievable, exact copy of EPHI, when needed, before movement of equipment. |

## Technical Safeguards

The following security standards for technical safeguards address the policies and procedures for the use of technology in a manner that protects EPHI and controls access to EPHI.

### *Standard: Access Control*

This standard requires the covered entity to implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Unique User Identification | Required | Assign a unique user name and/or number for identifying and tracking user identity. |
| Emergency Access | Required | Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency. |
| Automatic Logoff | Addressable | Implement electronic procedures that terminate an electronic session after a pre-determined time of inactivity. |
| Encryption and Decryption | Addressable | Implement a mechanism to encrypt and decrypt EPHI. |

### *Standard: Audit Control*

This standard requires the covered entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

### *Standard: Integrity*

This standard requires the covered entity to implement policies and procedures to protect EPHI from improper alteration or destruction.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Mechanism to Authenticate EPHI | Addressable | Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. |

### *Standard: Person or Entity Authentication*

This standard requires the covered entity to implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

### *Standard: Transmission Security*

This standard requires the covered entity to implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Integrity Controls | Addressable | Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection. |
| Encryption | Addressable | Implement a mechanism to encrypt EPHI whenever it is deemed appropriate. |

## Organizational Requirements

The following security standards establish what a covered entity is required to do if it will allow a business associate to create, receive, maintain, or transmit EPHI, and what a group health plan must do if it will allow the plan sponsor to create, receive, maintain, or transmit EPHI.

### *Standard: Business Associate Contracts or Other Arrangements*

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Business Associate Contracts or Other Arrangements | Required | Covered entity may not permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf without a business associate contract (or, in limited cases, another arrangement) |

### *Standard: Requirements for Group Health Plans*

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Administrative, Physical, and Technical Safeguards; Agents and Subcontractors; Adequate Separation; Report | Required | A group health plan may not disclose EPHI to the plan sponsor unless the plan document has been amended to require that the sponsor implement certain safeguards and take certain other steps |

## Policies and Procedures and Documentation

### *Standard: Policies and Procedures*

This standard requires the covered entity to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the security rule.

### *Standard: Documentation*

This standard requires the covered entity to maintain the policies and procedures implemented to comply with the security rule in written form (which may be electronic) and, if an action, activity, or assessment is required by the security rule to be documented, the covered entity must maintain a written record (which may be electronic) of the action, activity, or assessment.

| Implementation Specification | Required or Addressable | Description |
|---|---|---|
| Time Limit | Required | Retain documentation required by this standard for six years from the date of its creation or the date it was last in effect, whichever is later. |
| Availability | Required | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains |
| Update | Required | Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of the EPHI |