HIPAA

(Health Insurance Portability and

Accountability Act of 1996)

Privacy & Security

Policies and Procedures for the

Xavier University

Organized Health Care Arrangements

Effective as of December 23, 2024

Table of Contents

PART I

A. Definitions ..... - 6 -
B. Compliance with HIPAA Rules ..... - 9 -
C. Privacy Officer ..... - 10 -
D. Security Officer ..... - 12 -
E. Training ..... - 15 -
F. Plan Documents ..... - 17 -
G. Business Associates ..... - 19 -
H. Breach Notifications ..... - 22 -

PART II

A. Permitted Uses and Disclosures of PHI ..... - 27 -
B. Disclosures to Plan Sponsor ..... - 37 -
C. Minimum Necessary Standard ..... - 38 -
D. Written Authorizations ..... - 42 -
E. Oral or Implicit Permission to Disclose PHI ..... - 44 -
F. Disclosures Requiring Attestation ..... - 46 -
G. De-Identified Information ..... - 49 -
H. Requests for Restrictions on Use or Disclosure of PHI ..... - 51 -
I. Requests for Confidential Communications ..... - 53 -
J. Right of Access to PHI ..... - 55 -
K. Right to Request Amendment of PHI ..... - 58 -
L. Right to Request an Accounting of Disclosures ..... - 61 -
M. Sanctions for Violating the Privacy Rule ..... - 63 -
N. Privacy Complaints ..... - 64 -
O. Mitigation of Harm Due to Improper Uses or Disclosures ..... - 66 -
P. No Retaliation or Intimidation ..... - 67 -
Q. No Waiver of Rights ..... - 68 -
R. Notice of Privacy Practices ..... - 69 -

PART III

A. Risk Analysis ..... - 71 -
B. Risk Management ..... - 72 -
C. Sanctions for Violating the Security Rule ..... - 73 -
D. User Access Management ..... - 75 -
E. Authentication & Password Management ..... - 78 -
F. Log-In Monitoring ..... - 79 -
G. Facility Access Controls ..... - 80 -
H. Workstation Use & Security ..... - 81 -
I. Portable Device & Media Controls ..... - 82 -
J. Transmission Security ..... - 85 -

K. Protection From Malicious Software ..... **- 86 -**
L. System Audits, Audit Controls & Activity Review ..... **- 87 -**
M. Response and Reporting ..... **- 88 -**
N. Contingency Plan ..... **- 90 -**

Introduction

The Plan Sponsor provides various group health benefits to its eligible employees and their eligible dependents. These benefits are provided under a group health plan or plans as identified from time to time by the Plan Sponsor that are "Covered Entities" as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Office of the Secretary of the Department of Health and Human Services (the "Secretary") has issued: (1) regulations providing Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Subparts A and E of Part 164 ("Privacy Rule"); (2) regulations providing Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Subpart C of Part 164 (the "Security Rule"); and (3) regulations modifying the Privacy Rule, Security Rule, Enforcement and Breach Notification Rules (collectively the "HIPAA Rules); and

The privacy and security provisions of HIPAA have been amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009, and any and all references herein to the "HIPAA Rules" shall be deemed to include the Privacy Rule, the Security Rule, HITECH, the Enforcement and Breach Notification Rules, and all existing and future implementing regulations, as they become effective.

These policies and procedures (the "Policies") apply to each self-funded group health benefit and to each fully-insured group health benefit, to the extent the Plan Sponsor receives protected health information for such benefit and is required to maintain policies and procedures under the HIPAA Rules.

These Policies outline the obligations of the Plan and the Plan Sponsor as well as the rights of employees and dependents participating in the Plan under the HIPAA Rules. The Plan and the Plan Sponsor intend to comply fully with the requirements under the HIPAA Rules with respect to Protected Health Information ("PHI") Used or Disclosed by the Plan. These Policies have been adopted by the Plan Sponsor for purposes of complying with the HIPAA Rules with respect to the Plan, but these Policies do not create third party rights for or with respect to Participants, Business Associates or otherwise.

PART I

DEFINITIONS & GENERAL POLICIES

A. Definitions

In applying the Policies (including Parts I through III), the following definitions shall apply. Any capitalized term not defined below shall have the meaning set forth in the HIPAA Rules.

1. "Breach" means an unauthorized acquisition, access, or use or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of such information. A Breach excludes the following:

    a. any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Rules;

    b. any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Rules; or

    c. a disclosure of PHI where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

2. "Business Associate" means any person who, on behalf of the Plan, and in a capacity other than as part of the workforce of the Plan Sponsor, either:

    a. creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA's administrative simplification rules, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or

    b. provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, if the performance of such services involves disclosure of PHI from the Plan, or from another business associate of the Plan, to the service provider.

3. "Designated Record Set" means a group of records maintained by or for the Plan that is:

    a. the medical and billing records about Participants maintained by or for a covered health care provider;

    b. the enrollment, payment, claims adjudication and care or medical management records systems maintained by or for the Plan; or

c. used, in whole or in part, by or for the Plan to make decisions about Participants.

The term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

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

5. "Electronic Media" means:

   a. Electronic storage material on which data is or may be recorded electronically, including, for example, 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

   b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, if the information being exchanged did not exist in electronic form immediately before the transmission.

6. "Electronic Protected Health Information" or "Electronic PHI" means PHI that is transmitted by or maintained in Electronic Media.

7. "Individually Identifiable Health Information" means health information that: (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (c) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

8. "Plan" means the health components of the Xavier University Medical Plan and Xavier University Flex Plan. Together these plans make up an Organized Health Care Arrangement.

9. "Plan Sponsor" means Xavier University ("University") and any affiliate which has adopted the Plan for the benefit of its employees.

10. "Policy" or "Policies" means the Plan's policies and procedures as described herein.

11. "Privacy Officer" means the Associate VP for Human Resources.

12. "Protected Health Information" or "PHI" means Individually Identifiable Health Information, but excludes employment records held in the role of an employer and information regarding a person who has been deceased for more than 50 years. Accordingly, PHI includes Individually Identifiable Health Information that is received or maintained by the Plan Sponsor in the performance of plan administration functions for the Plan, but PHI does not include information that is received or maintained by the Plan Sponsor in its capacity as the employer of a participant or beneficiary. PHI also includes genetic information.

13. Reproductive Health Care" means health care that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes which includes but is not limited to contraception, including emergency contraception; preconception screening and counseling; management of pregnancy and pregnancy-related conditions, including pregnancy screening, prenatal care, miscarriage management, treatment for preeclampsia, hypertension during pregnancy, gestational diabetes, molar or ectopic pregnancy, and pregnancy termination; fertility and infertility diagnosis and treatment, including assisted reproductive technology and its components (e.g., in vitro fertilization (IVF)); diagnosis and treatment of conditions that affect the reproductive system (e.g., perimenopause, menopause, endometriosis, adenomyosis); and other types of care, services, and supplies used for the diagnosis and treatment of conditions related to the reproductive system (e.g., mammography, pregnancy-related nutrition services, postpartum care products).

14. "Security Officer" means the Director of Information Security.

15. "Summary Health Information" means information that may be Individually Identifiable Health Information and that summarizes the claims history, claims expenses, or types of claims experience by participants in the Plan, provided that the 18 specific identifiers in 45 CFR § 164.514(b)(2)(i) are removed, except that geographic information need only be aggregated to the level of a five digit zip code.

16. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS.

B. Compliance with HIPAA Rules

POLICY:

The Plan will comply fully with the requirements of the HIPAA Rules. No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by these Policies. The Plan reserves the right to amend or change any of the Policies at any time (and even retroactively) without notice. To the extent that these Policies establish requirements and obligations above and beyond those required by HIPAA, the Policies shall be aspirational and shall not be binding upon the Plan. These Policies do not address requirements under state law or federal laws other than HIPAA.

PROCEDURES:

1. The Plan's Policies shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the privacy and security of PHI, and any changes to Policies will be documented promptly.

2. Except to the extent that they are carried out by the Plan Sponsor or Business Associates, the Plan shall document certain actions, activities, and assessments with respect to PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this Policy, for example).

3. Policies and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

4. The Plan will make its Policies and other documentation available to the Privacy Officer, Security Officer, Plan Sponsor, third-party administrators and other Business Associates or other persons responsible for implementing the procedures to which the documentation pertains.

C. Privacy Officer

POLICY:

The Plan's Privacy Officer is responsible for the development and implementation of the Plan's Policies related to privacy, as well as the Plan's maintenance of and adherence to those Policies.

PROCEDURES:

The Privacy Officer's responsibilities are as follows:

1. Take the lead role and assist in the formation, implementation, and maintenance of the Plan's Policies related to privacy.

2. Maintain and ensure proper distribution of the privacy notice.

3. Enforce the Minimum Necessary Standard for the Plan.

4. Perform periodic reviews of the uses and disclosures of the Plan's PHI.

5. Take a lead role and assist in drafting appropriate Business Associate agreement provisions, assist in identifying Business Associates, and develop appropriate monitoring under the Privacy Rule of Business Associate agreements.

6. Implement and oversee the administration of participant and beneficiary rights under the Privacy Rule, including the right to access, right to request amendment, right to an accounting, and the right to request privacy protections.

7. Implement a process for tracking all disclosures of PHI that must be tracked and accounted for (upon participant or beneficiary request) under the Privacy Rule.

8. Establish and administer a system for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Plan's Policies related to privacy or compliance with the Privacy Rule.

9. Monitor legal changes and advancements in technology to ensure continued compliance.

10. Maintain (or supervise the maintenance of) all documentation required by the Privacy Rule.

11. Establish sanctions for failure to comply with the Plan's Policies related to privacy.

12. Cooperate with the U.S. Department of Health and Human Services, Office of Civil Rights, and other legal entities in any compliance reviews or investigations.

13. Be the official contact and information source for all issues or questions relating to the Plan's privacy treatment of participant and beneficiary PHI.

14. Work with the Security Officer for the Plan to ensure appropriate coordination between the privacy and security programs, including compliance with the requirements of the HITECH Act to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of the Business Associates discover a Breach.

15. In cooperation with the Security Officer, develop and oversee the training of appropriate members of the Plan Sponsor's workforce regarding the Privacy Rule, as well as the Plan's Policies related to privacy.

16. Work with the Security Officer to investigate and resolve security Breaches involving Electronic PHI of the Plan, including Breaches reported by Business Associates.

17. Undertake any other activities relating to PHI that are necessary or desirable to comply with the HIPAA Rules.

D. Security Officer

POLICY:

The Plan's Security Officer is responsible for the development and implementation of the Plan's Policies relating to the Security Rule, as well as the Plan's maintenance of and adherence to those Policies.

PROCEDURES:

The Security Officer's responsibilities are as follows:

1. Perform initial and periodic written risk assessments related to security of Electronic PHI for the Plan.

2. Implement, oversee, and monitor risk management measures to address security risks and vulnerabilities identified by risk assessments performed for the Plan, including the development and updating of a comprehensive written risk management program for the Plan.

3. Apply the Plan's Policies related to security providing the framework and the measures to protect against reasonably anticipated threats or hazards to security or integrity of Electronic PHI of the Plan.

4. Apply the Plan's Policies related to security providing the framework and the measures to protect against reasonably anticipated unauthorized uses or disclosures of Electronic PHI of the Plan.

5. Facilitate the Plan Sponsor's and Plan's compliance with:

    a. the Security Rule; and

    b. all Policies related to security.

6. Oversee the development, implementation, and maintenance of appropriate Policies and for the Plan.

7. Oversee the development, implementation, and maintenance of appropriate documents and forms, including:

    a. security policies;

    b. Business Associate contracts; and

    c. other policies, forms, and documentation required by HIPAA.

8. Apply the Plan's Policies related to security to regularly review records of computer or information system activity relating to the Plan, such as audit logs, access reports and security incident tracking reports.

9. Review and maintain the Plan's Policies related to security to ensure that they address the security of Electronic PHI of the Plan, including:

    a. systems/processes to monitor, track and index Electronic PHI;

    b. information system access and activity (e.g. audit logs, access reports);

    c. appropriate administrative, technical, and physical security measures;

    d. compliance with the Security Rule; and

    e. the retention of all required documentation for at least six years.

10. Apply the Plan's Policies related to security for the authorization of Plan Sponsor's workforce members who have access to Electronic PHI and develop and implement PHI, and apply the Plan's Policies related to security to terminate access when the Plan Sponsor's workforce members are terminated or transferred to other positions at the Plan Sponsor in which their access to Electronic PHI would be inappropriate.

11. Apply the Plan's Policies related to security for granting access authorization to areas where Electronic PHI of the Plan is stored or used and for computers on which such Electronic PHI is stored or used, including password management and similar issues.

12. Apply the Plan's Policies related to security in cooperation with other Plan Sponsor employees, for data backup procedures, disaster recovery plans, and emergency mode plans for the Plan.

13. Apply the Plan's Policies related to security for physical and technical safeguards.

14. Work with Business Associates of the Plan on HIPAA security issues and concerns.

15. Conduct periodic review of the Plan's Policies related to security and update as needed in response to environmental or operational changes.

16. Work with legal counsel to ensure that Policies, forms, and other documents of the Plan comply with the Security Rule and that the appropriate amendments have been made to these documents.

17. Coordinate work of other Plan Sponsor departments on security issues relating to the Plan, such as IT and security departments.

18. Work with the Privacy Officer for the Plan to ensure appropriate coordination between the health privacy and security programs, including compliance with the requirements of the HITECH Act to provide notification to affected individuals, HHS,

and the media (when required) if the Plan or one of the Business Associates discover a Breach.

19. In cooperation with the Privacy Officer, develop and oversee the training of appropriate members of the Plan Sponsor's workforce regarding the Security Rule, as well as the Plan's Policies related to security.

20. Provide periodic security updates to remind and update workforce members on the Plan's Policies related to security.

21. Work with the Privacy Officer to investigate and resolve security Breaches involving Electronic PHI of the Plan, including Breaches reported by Business Associates.

22. Maintain awareness of changes in security risks, security measures, and computer systems relating to the Plan.

23. Work with senior management to oversee the implementation of a sanction policy and appropriate sanctions for violation of the security policies and practices of the Plan, or for violation of the Security Rule.

24. Cooperate with the Office for Civil Rights (OCR), or other appropriate entity, in any compliance review, audit or investigation of the Plans.

25. Undertake any other activities relating to the Plans that are necessary or desirable to comply with HIPAA Rules.

E. Training

POLICY:

Employees of the Plan Sponsor who are considered part of the Plan's "workforce" will be trained to understand and implement the Plan's Policies related to privacy and the Privacy Rule. Employees of the Plan Sponsor who access, receive, transmit or otherwise use Electronic PHI or who set up, manage or maintain systems and workstations that access, receive, transmit, or store Electronic PHI will be trained to understand and implement the Plan's Policies related to security and the Security Rule.

PROCEDURES:

1. The Privacy Officer and Security Officer have responsibility for implementation of this Policy for their respective organizations. They are responsible for conducting a training needs assessment and developing and approving a training strategy. They will monitor and periodically evaluate the training plan and modify as necessary.

2. Timing of Training.

    a. Within a reasonable time after becoming a workforce member.

    b. Within a reasonable time after material changes to the Plan's Policies.

    c. Whenever, in the determination of a Privacy Officer or Security Officer, additional training is necessary to ensure compliance with the Plan's Policies or the HIPAA Rules.

3. Plan Sponsor employees who require privacy training will be trained in the following areas:

    a. At the determination of the Privacy Officer, on all of the Plan's Policies, or, if appropriate, relevant Policies for any particular employee if his or her job responsibilities do not necessitate training in all of the Policies;

    b. Permissible uses and disclosures of PHI;

    c. Relevant provisions of the Privacy Rule; and

    d. The requirement that all employees report any potential violations of the Plan's Policies or the Privacy Rule, whether caused by a workforce member or a service provider, to the Privacy Officer.

4. Plan Sponsor employees who require security training will be trained in the following areas:

a. At the determination of the Security Officer, on all of the Plan's Policies, or, if appropriate, relevant Policies for any particular employee if his or her job responsibilities do not necessitate training in all of the Policies;

b. Confidentiality, integrity and availability;

c. Common security threats and vulnerabilities;

d. Relevant provisions of the Security Rule; and

e. Incident response and reporting procedures.

5. The Privacy Officer and Security Officer will maintain records indicating who has been trained, what training occurred, and the date of training, for six years following the date of the training. These documents will be maintained by the Plan.

F. Plan Documents

POLICY:

Before the Plan discloses any PHI to the workforce of the Plan Sponsor for plan administrative functions, the Plan Sponsor shall certify to the Plan that the Plan documents have been amended as required by the HIPAA Rules.

PROCEDURES:

1. For purposes of complying with the Privacy Rule, the certification should represent that the Plan documents require the Plan Sponsor to:

    a. Not use or further disclose PHI other than as permitted by the Plan or as required by law.

    b. Ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor.

    c. Not use or disclose PHI for employment-related actions.

    d. Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.

    e. Make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures.

    f. Make the Plan Sponsor's internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request.

    g. If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

2. For purposes of complying with the Security Rule, the certification should represent that the Plan documents require the Plan Sponsor to:

    a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Plan.

b. Ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the Plan Sponsor.

c. Ensure that agents to whom the Plan Sponsor provides Electronic PHI agree to implement reasonable and appropriate security measures to protect the Electronic PHI of the Plan.

d. Report to Security Officer any security incident of which the Plan Sponsor becomes aware.

G. Business Associates

POLICY:

Each Plan Sponsor has many contractual and business relationships, and has policies related to its contracts and business relationships. The Plan's relevant service provider contract will incorporate Business Associate contract language. However, not all contractors or business partners are "Business Associates" as defined by the HIPAA Rules. This policy only applies to contractors or business partners that come within the definition of a "Business Associate."

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions should be addressed, in the first instance, by the Privacy Officer.

2. Business Associate contracts.

    a. All of the Plan's service providers who are Business Associates under the Privacy Rule must have written contracts.

    b. The Privacy Officer will ensure that service provider contracts incorporate appropriate business associate language. The Privacy Officer may develop standard Business Associate contract language, but is not required to use such language in all situations.

    c. The Plan Sponsor will be the signatory on all Business Associate contracts.

3. The Business Associate agreements will obtain satisfactory assurances from all Business Associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA privacy and security regulations and specifically providing:

    a. The permitted uses and disclosures of PHI by the Business Associate.

    b. The prohibition of other uses and disclosures of PHI by the Business Associate.

    c. The Business Associate will make PHI available to satisfy the participant access, amendment and accounting provision standards.

    d. The Business Associate will make its records available to HHS for any investigation.

    e. The Business Associate will implement appropriate safeguards to prevent unauthorized disclosures of PHI.

f. The Business Associate will implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that the Business Associate creates, receives, maintains, or transmits on behalf of the Plan (the "Contract Electronic PHI").

g. The Business Associate will ensure that any agents or subcontractors to whom the Business Associate provides PHI agree to the same restrictions and conditions that apply to the Business Associate and that they implement reasonable and appropriate security measures to protect the Contract Electronic PHI.

h. To the extent the Business Associate is to carry out any of the Plan's obligations under the HIPAA Rules, the Business Associate will comply with the requirements of the Privacy Rule that apply to the Plan in the performance of such obligation.

i. The Business Associate will report to the Plan any security incident or disclosure of the information other than as provided for by the contract of which the Business Associate becomes aware.

j. The Business Associate will take required steps with respect to Breach notification requirements.

k. The Business Associate will return or destroy all PHI received from, or created or received by the Business Associate on behalf of the Plan or, if such return or destruction is infeasible, extend the protections of the contract to the information and limit further uses and disclosures.

l. The authorization of the termination of the contract by the Plan if the Plan determines that the Business Associate has violated a material term of the contract.

4. If the Plan learns of a service provider's potential violation of its Business Associate contract (either through a participant or beneficiary complaint, during a performance audit, or otherwise), it will take the steps outlined below.

a. The Privacy Officer will investigate all potential or alleged Business Associate contract violations and, in conjunction with legal counsel, will determine if there is an actual violation.

b. Upon determining that there is an actual Business Associate contract violation, the Privacy Officer will work with the Business Associate to end the violation or to cure any harm caused. Refer to Plan's Policy on Mitigation of Harm.

c. If the Privacy Officer determines that the Business Associate is unwilling to cure or end the violation, then the Privacy Officer, in consultation with legal

counsel, will determine if it is feasible to terminate the contract. It is feasible to terminate the contract if there is any other service provider who can supply the same services, even if the cost is higher.

H. Breach Notifications

POLICY:

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its Business Associates discovers a Breach of Unsecured PHI.

PROCEDURES:

1. The Privacy Officer will work with the Security Officer to investigate any impermissible use or disclosure of PHI to determine whether the PHI was Unsecured PHI and whether there was a Breach. Acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach, unless the Privacy Officer determines that there is a low probability that the privacy or security of the PHI has been or will be compromised.

2. The Privacy Officer's determination of whether a Breach has occurred must include the following considerations:

    a. Was PHI involved? If not, there was not a Breach.

    b. Was Unsecured PHI involved? If not, there was not a Breach.

    c. Was there unauthorized access, use, acquisition, or disclosure of PHI? If not, then there was not a Breach.

    d. Is there a low probability that privacy or security was compromised? In order to determine if there is a low probability that the PHI was compromised, the Privacy Officer must perform a risk assessment that considers at least the following factors:

        i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.

        ii. The unauthorized person who used the protected health information or to whom the disclosure was made. For example, does the unauthorized recipient of the protected health information have obligations to protect the privacy and security of the protected health

information, such as another entity subject to HIPAA or an entity required to comply with the Privacy Act of 1974 or the Federal Information Security Management Act of 2002, and would those obligations lower the probability that the recipient would use or further disclose the protected health information inappropriately? Also, was the protected health information impermissibly used within a covered entity or Business Associate, or was it disclosed outside a covered entity or Business Associate?

iii. Whether the protected health information was actually acquired or viewed. If there was only an opportunity to actually view the information, but the Privacy Officer determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer with was lost or stolen and subsequently recovered, and the Privacy Officer is able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.

iv. The extent to which the risk to the protected health information has been mitigated. For example, if the Plan can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

3. If the Privacy Officer determines that there was not a Breach, the Privacy Officer will document the determination in writing, keep the documentation on file, and not provide notifications.

4. If the Privacy Officer determines there was a Breach, the Privacy Officer will provide the required notification to affected individuals.

   a. The notice will be provided without unreasonable delay and in no event later than 60 days following the discovery of a Breach. A Breach is considered to be discovered on the earlier of (i) the date that a workforce member (other than a workforce member who committed the Breach) knows of the events giving rise to the Breach, or (ii) the date that a workforce member or agent of the Plan would have known of the event giving rise to the Breach by exercising reasonable diligence.

   b. The notice will be given by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically.

c. Notices will be mailed to parents of minor children and to next-of-kin or to a personal representative of a deceased individual.

d. Notice will be given by alternative means to individuals whose contact information is out of date. If there are 10 or more individuals with out-of-date contact information, substitute notice will be provided through either a conspicuous posting for a period of 90 days on the homepage of the Plan Sponsor's website or conspicuous notice in major print in the geographic area where the individuals affected by the breach likely reside. If there are fewer than 10 individuals with out-of-date contact information, substitute notice may be made by telephone, in writing, or by other means.

e. The notice will contain the following information:

i. A description of the Breach, including a brief description of the incident, the types of Unsecured PHI that were involved, the date of the Breach, and the date of the discovery of the Breach;

ii. The steps an individual should take to protect themselves from potential harm from the Breach;

iii. A description of what the Plan is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and

iv. Contact procedures for individuals to ask questions and obtain more information.

5. The Security Officer and Privacy Officer will provide the required notification to HHS and will maintain a log of all Breaches.

a. If the Breach affects fewer than 500 individuals, notice will be given to HHS no later than 60 days after the end of the calendar year in which the Breach was discovered.

b. If the Breach affects 500 or more individuals, notice will be given to HHS without unreasonable delay but in no event later than 60 days following the discovery of a Breach.

6. The Security Officer and Privacy Officer will provide notice to the proper media outlets for any Breach that affects 500 or more individuals in a state or jurisdiction. If 500 or more individuals were affected, but not more than 500 residents of any one state or jurisdiction were affected, no notice will be given to the media.

a. Notice will be provided in the form of a press release to prominent media outlets in any state or jurisdiction where 500 or more affected individuals reside.

b. Notice will be provided without unreasonable delay and in no event later than 60 days following the discovery of a Breach.

c. The press release will contain the same information as the information required in the notice to the affected individuals.

7. Unless agreed upon otherwise in a Business Associate Agreement, the Security Officer and Privacy Officer will be responsible for following the procedures outlined above if they are notified of a Breach of PHI in the possession of a Business Associate.

PART II

Privacy Policies

A. Permitted Uses and Disclosures of PHI

POLICY:

The uses and disclosures discussed in the procedures below are permitted by the Plan without the participant's or beneficiary's permission or request (written or otherwise), provided the particular requirements of these procedures and the Privacy Rule are met.

PROCEDURES:

1. The following uses and disclosures of the Plan's PHI for "payment" purposes are permitted:

   Billing and premium or claims payment
   Claims reporting
   Claims management and related health care data processing
   Utilization review, precertification and preauthorization
   Claims inquiries and resolution
   Eligibility reporting, enrollment and disenrollment activities
   Coverage determination
   Determination of cost sharing
   Coordination of benefits
   Subrogation
   Benefit elections

   a. Additional uses and disclosures may also fall within the Privacy Rule's definition of "payment." The Privacy Officer will determine on a case-by-case basis if a particular use or disclosure not listed above is a payment activity. If that activity is common or recurring, it shall be added to the list above.

   b. All uses and disclosures of PHI for payment activities will comply with the Plan's Minimum Necessary Standard.

2. The following uses and disclosures of the Plan's PHI for "health care operations" purposes are permitted:

   Legal review
   Cost management
   Quality assessment and rating provider and plan performance
   Population-based activities
   Audits and fraud and abuse detection
   Business planning
   General administration

   a. Additional uses and disclosures may also fall within the Privacy Rule's definition of "health care operations." The Privacy Officer will determine on a

case-by-case basis if a particular use or disclosure not listed above is a health care operations activity. If that activity is common or recurring, it shall be added to the list above.

b. All uses and disclosures of PHI for health care operations activities will comply with the Plan's Minimum Necessary Standard.

3. The Privacy Rule permits other additional uses and disclosures of the Plan's PHI. Those additional uses and disclosures, described in the remainder of these procedures, are:

a. To the Plan's Business Associates (provided a business associate agreement is in place).

b. To other covered entities that are members of the Plan's Organized Health Care Arrangement.

c. For the treatment and payment activities of another covered entity.

i. Upon request by a health care provider, the Plan will disclose PHI to a health care provider for that provider's treatment activities.

ii. Upon request by another covered entity or a health care provider, the Plan will disclose PHI for purposes of the requestor's payment activities.

iii. The Plan assumes the information requested by a provider or another covered entity is compliant with the Minimum Necessary Standard.

d. For the following health care operations activities of another covered entity. Upon request by another covered entity, the Plan will disclose PHI for purposes of the requestor's health care operations activities if the following conditions are met:

i. The other entity has or had a relationship with the participant or beneficiary who is the subject of the PHI.

ii. The health care operation activity is one of the following types of activities:

- Quality assessment and improvement;
- Population-based activities relating to improving health or reducing health care costs;
- Case management;
- Conducting training programs;

- Accreditation, certification, licensing, or credentialing; or
- Health care fraud and abuse detection or compliance.

iii. The Plan assumes that the information requested by a covered entity is compliant with the Minimum Necessary Standard.

e. As required by law.

i. The Plan will use or disclose PHI as required by law.

ii. The Privacy Officer, in conjunction with legal counsel, will determine on a case-by-case basis whether uses and disclosures are required by law.

iii. The Privacy Officer will ensure that uses or disclosures required by law will be limited to the requirements of the law. The Plan's Minimum Necessary Standard does not apply to uses or disclosures required by law.

iv. The following uses and disclosures required by law, as discussed below in these procedures, have additional requirements relating to:

- Victims of abuse, neglect, or domestic violence;
- Judicial or administrative proceedings;
- Disclosures for law enforcement purposes; and
- Disclosures related to Reproductive Health Care.

f. For public health activities. Uses or disclosures of PHI for public health activities will be rare. See the Privacy Officer for any uses or disclosures potentially falling within this category.

g. For health oversight activities. The Plan will disclose PHI for purposes of health oversight activities.

i. Health oversight activities are those relating to oversight of:

- The health care system;
- Government benefit programs for which health information is relevant to beneficiary eligibility;
- Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

- Entities subject to civil rights laws for which health information is necessary for determining compliance.

ii. The following are some of the health oversight agencies to whom the Plan may make health oversight disclosures:

- U.S. Department of Labor Employee Benefits Security Administration
- EEOC
- Federal offices of inspectors general
- Department of Justice
- Occupational Health and Safety Administration
- Defense Criminal Investigative Services
- Social Security Administration
- HHS Office for Civil Rights
- Food and Drug Administration
- State insurance agencies
- Medicaid fraud control units

iii. Disclosures will be made under the Plan's Policy for disclosures for law enforcement purposes if (a) the use or disclosure relates to a particular individual, and (b) the oversight activity is not directly related to the receipt of health care or qualification for public benefits related to health care.

iv. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.

v. The Plan assumes that information requested by a public official for health oversight activities compliant with the Minimum Necessary Standard.

h. Related to victims of abuse, neglect, or domestic violence.

i. If the Privacy Officer determines, based on PHI that legitimately came to his or her attention or to the attention of a Plan workforce member, that a participant or beneficiary is the victim of abuse, neglect, or domestic violence, then this information may be disclosed as follows:

- To a government authority authorized by law to receive reports of abuse, neglect, or domestic violence. The Privacy Officer will consult with legal counsel to determine the appropriate governmental authority.

- The disclosure must be required by another law. The Privacy Officer will consult with legal counsel to ensure that the disclosure is required by law.

- The Privacy Officer must notify the participant or beneficiary of the disclosure (unless the Privacy Officer determines notification would harm the participant or beneficiary, or if the appropriate disclosure would be to a personal representative, and it is the personal representative that is causing the abuse, neglect, or harm).

ii. If the Privacy Officer or other Plan workforce member suspects a participant or beneficiary is the victim of abuse, neglect, or domestic violence, and that suspicion is not based on information in the Plan records, the Privacy Rule and this Policy do not apply to any disclosure of those suspicions to the appropriate authorities.

i. For judicial or administrative proceedings.

i. All legal documents seeking PHI for judicial or administrative proceedings immediately should be directed to the Privacy Officer, who will determine the appropriate response based on these procedures, in consultation with legal counsel.

ii. Judicial orders and subpoenas. The Plan's PHI may be disclosed pursuant to a judicial order or valid subpoena from a court or an administrative tribunal.

- The disclosure must be limited to the information expressly authorized in the order or subpoena.

- The Plan's Minimum Necessary Standard does not apply to this type of disclosure.

iii. Discovery requests and non-judicial subpoenas. If the Plan receives a discovery request or subpoena that is not issued by a court or administrative tribunal, then the Privacy Officer, in consultation with legal counsel, will comply if one of the following conditions is met:

- The discovery request or subpoena is accompanied by a written statement showing that: (1) the requestor made a good faith attempt to provide written notice to the individual whose PHI is

requested; (2) the notice included enough information about the litigation such that the individual could raise an objection to the court/administrative tribunal; and (3) the time for the individual to raise objection has elapsed and no objections were filed or, if filed, have been resolved by the court.

- The discovery request or subpoena is accompanied by a written statement showing that there is either a stipulated or court issued protective order that prohibits the use or disclosure of the PHI outside the litigation, and requires that the PHI be returned to the covered entity or destroyed at the conclusion of the proceeding.

- If the discovery request or subpoena does not meet the requirements of either statement above, then the Privacy Officer, in consultation with legal counsel, may disclose the requested PHI by ensuring that the above requirements are met (that is, notify the individual as required or obtain a protective order).

iv. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.

j. For law enforcement purposes. The Privacy Officer, in consultation with legal counsel as appropriate, may disclose PHI to a law enforcement official (i.e., someone having authority to investigate potential violations of law, or to prosecute or conduct criminal, civil, or administrative proceedings arising from alleged violations of the law) in the following circumstances:

i. When the disclosure is required by law.

ii. Pursuant to a court order, warrant, subpoena, or summons issued by a judicial officer (including a grand jury subpoena).

iii. Pursuant to an investigative request from an administrative body, but only if the following additional conditions are met:

- The Privacy Officer determines that the information sought is relevant and material to a legitimate law enforcement inquiry;

- The request is specific and limited in scope in light of the purpose for which the information is sought; and

- De-identified information cannot reasonably be used.

iv. To identify or locate an individual, but only if officially requested. The PHI from Plan records that may be disclosed in such circumstances is strictly limited to:

- Name and address
- Social security number
- Type of injury
- A description of distinguishing physical characteristics, including height, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos
- Date and place of birth
- ABO blood type and rh factor
- Date and time of treatment
- Date and time of death, if applicable

Note: Information in the Plan Sponsor's non-group health plan records is not subject to the Privacy Rule.

v. About individuals who are suspected to be crime victims, but only if (1) the individual agrees orally or in writing to the disclosure, or (2) if the individual is unable to agree because of incapacity, in which case the Privacy Officer may determine that disclosure is appropriate, but only if the following conditions are met:

- The law enforcement official states that they need the information to determine whether another person has violated the law (and the information will not be used against the victim);
- The law enforcement official states that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
- In the Privacy Officer's professional judgment, the disclosure is in the potential crime victim's best interest.

vi. About a crime relating to the Plan.

vii. For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.

k. About decedents. The Plan will treat any person authorized to act as the personal representative of a participant or beneficiary that is deceased (e.g.,

an executor or administrator) as though the personal representative is the participant or beneficiary. The Plan will also disclose a decedent's PHI to a family member or others who were involved in the care or payment for care prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Plan.

l. To avert a serious threat to health or safety. The Privacy Officer will determine when a disclosure of PHI is necessary to avert a serious threat to health or safety. The following criteria apply to any such disclosure:

i. It must not conflict with other applicable law and standards of ethical conduct.

ii. It must be based on good faith.

iii. It must be necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

iv. It must be to a person or to people reasonably able to prevent or lessen the threat, including the target of the threat.

v. It must be limited to the following information:

- Name and address
- Social security number
- Type of injury
- A description of distinguishing physical characteristics, including height, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos
- Date and place of birth
- ABO blood type and rh factor
- Date and time of treatment
- Date and time of death, if applicable

m. Relating to national security and intelligence activities.

i. The Privacy Officer will, in consultation with legal counsel, disclose PHI to authorized federal officials for intelligence and other national security activities.

ii. Disclosures for national security and intelligence activities are not subject to the Plan's Policies on the right to Request an Accounting of Disclosures.

n. For workers' compensation. The Plan will disclose PHI in compliance with applicable state and federal workers' compensation laws (i.e., any state or federal law that has the effect of providing benefits for work-related injuries or illness without regard to fault).

o. To the personal representative of participant or beneficiary.

i. Adult or emancipated minor. The Plan will disclose PHI to an adult or emancipated minor's personal representative to the extent the PHI is relevant to the personal representation.

ii. Unemancipated minor. The Plan will disclose PHI to the parent, guardian, or other personal representative of an unemancipated minor only to the extent required, permitted, or prohibited by state law.

iii. Exceptions: The Plan will not disclose PHI to the personal representative of a participant or beneficiary if the Privacy Officer reasonably believes, and documents that belief, that:

- The participant or beneficiary has been or may be abused or neglected by the personal representative;
- The participant or beneficiary will be endangered if the personal representative relationship is recognized;
- The Plan, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative; or
- For disclosures that are potentially related to Reproductive Health Care, disclosures may only be made in accordance with the Plan's Policy for Disclosures Requiring Attestation.

4. The Privacy Rule prohibits or restricts the following uses and disclosures of the Plan's PHI:

a. Sale of PHI. The Plan will not sell PHI in a manner not permitted by the Privacy Rule without the authorization from any impacted individual.

b. Genetic Information. The Plan will not use or disclose genetic information for underwriting purposes.

c. Reproductive Health Care Information. The Plan will not use or disclose PHI for any of the following activities:

i. to conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care;

ii. to impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; or

iii. to identify any person for the purposes described above.

This Reproductive Health Care prohibition applies only when the Plan reasonably determines: (1) the Reproductive Health Care is lawful under applicable state or federal law under the circumstances in which it was provided; or (2) the Reproductive Health Care presumption applies.

B. Disclosures to Plan Sponsor

POLICY:

The Plan may only disclose PHI to the Plan Sponsor under the following conditions: (i) the disclosure is pursuant to a written authorization; (ii) the PHI is limited to Summary Health Information that has been requested by the Plan Sponsor for the purposes of obtaining premium bids, or amending or terminating the Plan; (iii) the PHI is enrollment, disenrollment or participation information; or (iv) the PHI is disclosed for plan administration functions.

PROCEDURES:

1. If the Plan is disclosing PHI for plan administrative functions, the Plan must determine that the Plan Sponsor has satisfied the Plan documentation requirements described in Part I of these Policies.

2. Plan administrative functions must be within the scope of payment or health care operations. Examples include disclosure for administrative review of claims and participant advocacy.

C. Minimum Necessary Standard

POLICY:

The Plan will use or disclose only the minimum necessary amount of PHI in order to achieve the purpose of the use or disclosure.

PROCEDURES:

1. The Minimum Necessary Standard does not apply in the following circumstances:

   a. The PHI is for use by or a disclosure to a health care provider for treatment purposes;

   b. The disclosure is to the participant or the participant's legally authorized representative;

   c. The disclosure is pursuant to a valid authorization, in which case, the disclosure will be limited to the PHI specified on the authorization;

   d. The disclosure is to the Secretary of Health and Human Services; or

   e. The disclosure is required by law.

2. Accessibility by workforce members. The following categories or titles of the Plan's workforce need access to the identified types of information, some of which is protected health information, to carry out their duties relating to the Plan.

Job Title or Category of Workforce Member	**Type of Protected Health Information Necessary to Carry Out Duties**
Human Resources Internal Auditing Personnel Benefit Committee Legal	Dependent status Dependent data Medicare eligibility Other insurance Claims history Coverage history Treatment history Treating provider Primary care physician Health Plan election Diagnosis Treatment code FSA election Cost of coverage
Payroll Personnel	Medicare eligibility Other insurance

Job Title or Category of Workforce Member	**Type of Protected Health Information Necessary to Carry Out Duties**
	Health Plan election FSA election Cost of coverage
Controller's Office	Dependent status Medicare eligibility Claims History Coverage History Health Plan election FSA election Cost of coverage
IT Personnel	Dependent status Dependent data Medicare eligibility Other insurance Coverage history Primary care physician Health Plan election FSA election Cost of coverage

3. Routine disclosures. The Privacy Officer will make reasonable efforts to limit the access of the Plan's workforce members identified above to their related types of protected health information by taking the following steps:

   a. Limit access to stored data relating to PHI; and

   b. Periodically monitor activities of Plan's workforce.

   The following are the minimum necessary information for "routine and recurring" uses and disclosures:

Use or Disclosure	**Minimum Necessary Data**
Claims inquiries and resolution Utilization review, precertification and preauthorization Legal review Audits and fraud and abuse detection Coordination of benefits Subrogation	Name Social Security Number Age and date of birth Marital status Sex Dependent status Dependent data Medicare eligibility Other insurance Home address Work location Claims history

Use or Disclosure	**Minimum Necessary Data**
	Coverage history Treatment history Treating provider Primary care physician Health Plan election Diagnosis Treatment code FSA election Cost of Coverage
Billing and premium or claims payment Claims reporting Claims management and related health care data processing Eligibility reporting, enrollment and disenrollment activities General administration	Name Social Security Number Age and date of birth Marital status Sex Dependent status Dependent data Medicare eligibility Other insurance Home address Work location Claims history Coverage history Primary care physician Health Plan election FSA election Cost of Coverage
Coverage determination Determination of cost sharing Benefits election	Name Social Security Number Age and date of birth Marital status Dependent status Dependent data Medicare eligibility Other insurance Home address Work location Health Plan election FSA election
Quality assessment and rating provider and plan performance	Claims history
Cost management Business Planning Population-based activities	Age and date of birth Marital status Dependent status Dependent data Medicare eligibility

Use or Disclosure	Minimum Necessary Data
	Other insurance Home address Work location Claims history Coverage history Health Plan election FSA election Cost of coverage

4. Non-routine disclosures. The Privacy Officer will review non-routine uses and disclosures on a case-by-case basis to determine the minimum necessary requirement.

5. Requests for PHI from another covered entity. When requesting PHI from another covered entity, the Plan must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are made on a routine and recurring basis the Plan shall take reasonable steps to insure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

6. Reliance on request for PHI. The Privacy Officer need not make a minimum necessary determination for requests of information by the following entities (and can, instead, assume that the requestor's statement of information needed is the minimum necessary amount):

    a. A public official when the disclosure is one that is permitted pursuant to the Plan's use and disclosure Policy (pursuant to law, for health oversight purposes, etc.);

    b. Covered entities;

    c. An employee if the individual represents that the information requested is the minimum necessary for the stated purpose; and

    d. The Plan's Business Associates, as long as the disclosure is for the purposes of carrying out the services under the service provider contract.

D. Written Authorizations

POLICY:

The Plan will obtain written authorizations for the use or disclosure of PHI not permitted under the Privacy Rule. The Plan will disclose PHI upon the request of another entity upon receiving a valid authorization. The Plan does not condition eligibility for enrollment in, or coverage under the Plan on, the receipt of any authorization from a participant or beneficiary.

PROCEDURES:

1. Written authorizations must be obtained from participants and beneficiaries before making the following uses or disclosures of their PHI:

    a. any PHI use or disclosure that this privacy Policy does not specifically require or permit;

    b. any communications for marketing purposes, unless an exception is provided for in the HIPAA Rules; or

    c. any use or disclosure of psychotherapy notes.

2. Content of authorizations. The Plan will use a standard authorization form for all authorizations except those initiated by other entities.

    a. Authorizations should be modified to specifically state the PHI to be used or disclosed, to whom it will be disclosed, and the purpose of the disclosure.

    b. The Privacy Officer will review each authorization or type of authorization to ensure it meets the requirements of the Privacy Rule.

    c. Multiple authorizations may be combined for uses or disclosures of PHI, except that an authorization may not be combined with any non-authorization document or with an authorization for the use or disclosure of psychotherapy notes.

3. Revocations. The Plan will honor all written revocations of authorization.

    a. All revocations should be sent to the Privacy Officer.

    b. The Privacy Officer will ensure that uses and disclosures previously authorized cease.

4. Refusal to sign an authorization does not affect a participant's or beneficiary's rights relating to eligibility for, enrollment in, or coverage under the Plan.

5. Authorizations initiated by participants, beneficiaries, or other entities.

a. The Plan may receive a request for information from another entity or a request from a participant or beneficiary to disclose his or her PHI to another entity.

b. The Privacy Officer must review all authorizations received from participants, beneficiaries, or other entities to ensure that the authorizations meet the requirements of the Privacy Rule. Disclosures will not be made if the authorizations are not sufficient under the Privacy Rule.

6. The Plan's Minimum Necessary Standard does not apply to uses or disclosures made pursuant to an authorization. The PHI used or disclosed will be consistent with the information authorized to be used or disclosed.

7. Documentation. Signed authorization forms and revocations will be maintained by the Plan for six years following the date last in effect.

E. Oral or Implicit Permission to Disclose PHI

POLICY:

The Plan will disclose PHI to a person who is involved in a participant's or beneficiary's health care or payment related to that health care when the participant or beneficiary orally or implicitly permits such a disclosure (as governed by the Privacy Rule). Such disclosures that are requested when the participant or beneficiary is not present will only be made to a member of the participant's or beneficiary's immediate family.

PROCEDURES:

1. This Policy applies to inquiries by a family member or friend about a participant's or beneficiary's status or benefits. This Policy does not apply to inquiries by family members who are the personal representative of another family member. Personal representatives are generally treated as the participant or beneficiary.

2. Phone or in person – participant or beneficiary present.

    a. If an individual contacts the Plan Sponsor regarding a participant's or beneficiary's status or benefits, the Privacy Officer should in all cases try to obtain oral agreement from the participant or beneficiary before communicating with the individual.

        i. If the inquiry is in person, and the participant or beneficiary is present, obtain the participant or beneficiary's verbal agreement that PHI may be shared with the inquiring individual.

        ii. If the inquiry is by phone, ask to speak with the participant or beneficiary, if available obtain the participant or beneficiary's verbal agreement that PHI may be shared with the inquiring individual.

    b. Once verbal agreement is obtained, the Privacy Officer may disclose the following categories of information:

        i. Confirm eligibility or enrollment information;

        ii. Provide general information regarding healthcare plan provisions; and

        iii. Provide assistance with claims resolution.

    c. Suggest to the participant or beneficiary that they may wish to give the Plan written authorization to disclose PHI to certain family members or friends involved in the participant's or beneficiary's health care. See the Plan's Policy on authorizations.

3. Phone, in person, or by correspondence (including e-mail) – participant or beneficiary not present.

   a. If a member of the participant's or beneficiary's immediate family contacts the Plan Sponsor regarding a participant's or beneficiary's status or benefits and the participant or beneficiary is not present at the time an inquiry is made on his or her behalf, the Privacy Officer should:

      i. Verify the identity of the individual and his or her immediate family relationship to the participant or beneficiary.

      ii. Review the participant's or beneficiary's records to ensure that there is no restriction or confidential communication request in place. (If there is, the Privacy Officer should not disclose any PHI to the individual.)

   b. The Privacy Officer should determine if the disclosure requested is in the best interests of the participant or beneficiary. If so, the disclosure should be limited as follows:

      i. Confirm eligibility or enrollment information;

      ii. Provide general information regarding healthcare plan provisions; and

      iii. Provide assistance with claims resolution.

   c. The PHI disclosed must be limited to that directly relevant to the inquiring individual's involvement in the participant's or beneficiary's health care.

F. Disclosures Requiring Attestation

POLICY:

The Plan will obtain an attestation for any request of PHI that is potentially related to Reproductive Health Care if the request is made for disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for law enforcement purposes, disclosures required by law, or disclosures about decedents to coroners and medical examiners. If the Plan, upon receipt of the attestation and additional investigation, determines that the request is not for purposes of investigating or imposing liability for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care that was lawful under the circumstances in which it was provided, the Plan may disclose the PHI upon the request.

PROCEDURES:

1. The Plan will presume Reproductive Health Care is lawful under the circumstances in which such health care is provided unless the Plan has:

    a. Actual knowledge that the Reproductive Health Care was not lawful under the circumstances in which it was provided; or

    b. Factual information supplied by the person requesting the use or disclosure of PHI that would demonstrate to a reasonable covered entity a substantial factual basis that the Reproductive Health Care was not lawful under the specific circumstances in which such health care was provided.

2. All requests for PHI related to Reproductive Health Care for purposes as stated above must be accompanied by a valid attestation. A valid attestation for these purposes is a document that must only contain the following elements:

    a. A description of the information requested that identifies the information in a specific fashion, including one of the following:

        i. The name of any individual(s) whose PHI is sought, if practicable; or

        ii. If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose PHI is sought.

b. The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure;

c. The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure;

d. A clear statement that the use or disclosure is not for a purpose prohibited under the Privacy Rule;

e. A statement that a person may be subject to criminal penalties if that person knowingly and in violation of HIPAA obtains Individually Identifiable Health Information relating to an individual or discloses Individually Identifiable Health Information to another person; and

f. Signature of the person requesting the PHI, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.

3. An attestation is not valid and, therefore will not be accepted by the Plan if the document submitted has any of the following defects:

   a. The attestation lacks an element or statement required by the list as stated above;

   b. The attestation contains an element or statement not required by paragraph 2 of this section;

   c. The attestation is combined with any other document except where such other document is needed to satisfy the requirements of this Section of the Policies or other sections of the Privacy Rule as applicable;

   d. The Plan or its business associate has actual knowledge that material information in the attestation is false; or

   e. In light of the facts and circumstances of the request, a reasonable covered entity or Business Associate in the same position as the Plan would not believe that the attestation is true.

4. The Plan will only accept an attestation that has been written in plain language that clearly identifies the purpose of the request.

5. If, during the course of using or disclosing PHI in reasonable reliance on a facially valid attestation, the Plan or its Business Associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or disclosure for a purpose prohibited under the Privacy Rule, the Plan or its Business Associate will cease such use or disclosure.

G. De-Identified Information

POLICY:

The Plan will use or disclose de-identified information instead of PHI to the extent practicable.

PROCEDURES:

1. The following common and recurring uses and disclosure by the Plan of health information will be conducted using de-identified information:

   a. Plan utilization and cost;

   b. Plan design;

   c. Participation in healthcare surveys; and

   d. Reporting required by government agencies.

2. The Privacy Officer will review other uses and disclosures on a case-by-case basis to determine if de-identified information is preferable to PHI.

3. The Privacy Officer will work with the Plan's third-party administrator, insurer, or Business Associate to obtain the relevant PHI for purposes of creating de-identified information.

4. If necessary, the Privacy Officer will engage a service provider to create the de-identified information. Any such service provider will sign a business associate agreement as required under the Plan's Business Associates Policy.

5. The Privacy Officer will ensure that none of the following data elements are included in any de-identified information (or alternatively, will engage a statistical expert to determine that the risk of identifying an individual based on the information included is very small):

   - Names
   - All geographic units smaller than a state (except for the first three zip code digits if the number of persons in that zip code region is greater than 20,000)
   - All ages over 89
   - All dates (except year)
   - Telephone and fax numbers
   - Social security numbers
   - Health plan beneficiary numbers
   - Certificate/license numbers

- Internet Protocol address numbers
- Medical record numbers
- Account numbers
- Vehicle identifiers and serial numbers (including license plate numbers)
- Full face photos (and comparable images)
- Device identifiers and serial numbers
- E-mail addresses
- URLs
- Biometric identifiers (including finger and voice prints)
- Any other unique identifying number, characteristic, or code

H. Requests for Restrictions on Use or Disclosure of PHI

POLICY:

Participants or beneficiaries have the right to request that the Plan (a) restrict using or disclosing PHI for payment and health care operations, and (b) restrict disclosing PHI to family members or friends involved in their care or payment relating to their care. The Plan *will not* agree to restrictions on its use and disclosure of PHI relating to payment and health care operations. The Plan generally *will* accommodate requests to restrict disclosures to family members or friends involved in the care or payment of care of the participant or beneficiary, provided those restrictions are administratively feasible.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions should be addressed, in the first instance, by the Privacy Officer.

2. Participants and beneficiaries must request restrictions on the use and disclosure of their PHI in writing. In general, before responding to such a request, the Privacy Officer should review it for completeness. It should contain the following information:

    a. Name, address, and daytime phone number of the participant or beneficiary making the request; and either:

    b. The manner in which the participant or beneficiary wishes the Plan to restrict its uses and disclosures of PHI for payment and health care operations; or

    c. The persons involved in their care to whom the Plan should not disclose PHI.

3. If a participant or beneficiary requests a restriction on the use or disclosure of PHI for payment and health care operations purposes, in almost all instances the Privacy Officer should send a response stating that the request has been denied.

4. If the participant or beneficiary has requested that the Plan not disclose his or her PHI to certain family members or friends, the Privacy Officer should take the following steps:

    a. Determine whether the requested restriction is feasible. This may include discussing the restriction with Business Associates (such as the Plan's third party administrator).

    b. If the restriction is feasible, send a written response indicating that the Plan agrees to the restriction. Inform relevant Business Associates (such as the Plan's third-party administrator) of the restriction.

c. Consider whether the participant or beneficiary intended to request confidential communications of PHI. These are generally granted if reasonable, and if the participant or beneficiary alleges that they will be subject to harm if the PHI is disclosed. See the Plan's Policy on Requests for Confidential Communications.

d. If the restriction is not feasible, send a response stating that the request has been denied.

5. The Privacy Officer should ensure that agreed-to restrictions are communicated to relevant Business Associates.

6. If the Plan determines it no longer wishes to continue operating in accordance with an agreed-to restriction, it may terminate the restriction by:

   a. Obtaining oral or written assent from the participant or beneficiary.

      i. Assent should be documented.

      ii. If the participant or beneficiary agrees, then the restriction is terminated both prospectively and retrospectively.

   b. Notify the participant or beneficiary that the agreed-to restriction is terminated.

      i. This method of terminating an agreed-to restriction should be used only if the Privacy Officer is unable to obtain oral or written assent from the participant or beneficiary.

      ii. A restriction terminated by notification operates prospectively only.

7. If the participant or beneficiary notifies the Plan that they no longer need the restriction, the restriction will be lifted both prospectively and retrospectively.

8. All written requests for privacy protection must be tracked on a privacy tracking log.

9. All written requests for privacy protection to which the Plan has agreed, and any termination documentation, must be maintained by the Plan for six years from the date the document was created or the date it was last in effect, whichever is later.

I. Requests for Confidential Communications

POLICY:

Participants and beneficiaries have the right to request that communications to them about their PHI be by alternative means or alternative locations. The Plan will agree to requests for confidential communications but only if (1) the requestor states that disclosure of the information at issue could endanger them; (2) the request is in writing; and (3) the alternative means or alternative locations given for the communications are administratively reasonable.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions should be addressed, in the first instance, by the Privacy Officer.

2. Participants and beneficiaries who wish to request confidential communications must do so in writing. In general, before responding to such a request, the Privacy Officer should review it for completeness. It should contain the following information:

    a. Name, address, and daytime telephone number of the participant or beneficiary making the request;

    b. The types or categories of communications to which the request applies;

    c. The alternative means or locations for the Plan to continue the communications with the participant or beneficiary; and

    d. A statement that the participant or beneficiary believes that the disclosure of PHI in the identified communications could endanger them.

3. Grounds for denial.

    a. The Privacy Officer should deny the request in writing if it does not include a statement that the participant or beneficiary fears they will be endangered.

    b. The Privacy Officer should deny the request in writing if the requested alternative means or location is not feasible. Investigate whether the alternative means or location is feasible, including conducting discussions with relevant Business Associates, such as its third-party administrator.

4. Granting a request.

    a. If the request is feasible, or partially feasible, the Privacy Officer should send a written response that includes a statement describing what communications are covered and the manner in which they will be communicated.

b. Consider whether, even if it is feasible, there might be other ways the information will be disclosed to someone who could endanger the participant or beneficiary. Example: Explanations of Benefits (EOBs) relating to a beneficiary dependent's reproductive health medical services can feasibly be sent to a Post Office box separate from their home address. It may be, however, that later EOBs sent to the participant will include an indication that part of the covered charge for the beneficiary's services qualified toward the deductible. If such a situation exists, carefully explain it in the response.

c. Inform relevant Business Associates (such as the Plan's third-party administrator) of any agreed-to confidential communication.

5. All written requests for privacy protection must be tracked on a log of privacy protection requests.

6. All written requests for confidential communication to which the Plan has agreed must be maintained by the Plan for six years from the date the document was created or the date it was last in effect, whichever is later.

J. Right of Access to PHI

POLICY:

Beneficiaries and participants, or their personal representatives, have a right to access PHI contained in the Plan's designated record sets.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions should be addressed, in the first instance, by the Privacy Officer.

2. Participants and beneficiaries, or their personal representatives, must request access to their PHI in writing. In general, before responding to such a request, the Privacy Officer should review it for completeness. It should contain the following information:

    a. Name, address, and daytime telephone number of the participant or beneficiary making the request;

    b. If submitted by personal representative, proof of status;

    c. Time period of the request; and

    d. Form of access requested (on-site, mailed copy, etc.).

3. Requests for access must be granted or denied within 30 days from the date a written request is received. If more time is needed, send a notice indicating that additional time (up to an additional 30 days) is needed to respond to the access request.

4. If the PHI requested is maintained electronically in one or more designated record sets, and the participant or beneficiary requests an electronic copy of such information, the Plan will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format. If the PHI is not readily producible in such form and format, the PHI will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual cannot agree on an acceptable electronic form and format, the Plan will provide a paper copy of the information.

5. Reviewing a Request.

    a. Determine whether any requested PHI is in a designated record set and if the information is maintained electronically (if requested).

    b. Determine if there is any basis on which to deny or partially deny the request. The following are permissible bases for denial:

i. If the request is made by a person asserting that they are the personal representative of a participant or beneficiary, review the documentation provided to verify that status. If the documentation is inadequate, or if the requested information is not within the scope of the personal representation, deny the request. If necessary, check with the Privacy Officer or legal counsel regarding the legal requirements for personal representatives.

ii. The Privacy Officer, after consulting with a licensed health care professional, determines that access will endanger the life or physical safety of the participant or beneficiary or another person.

iii. The requested PHI contains psychotherapy notes.

iv. The requested PHI was compiled by the Plan or one of its Business Associates in anticipation of a legal proceeding.

v. The information was obtained from someone other than a covered health care provider under a promise of confidentiality and access would likely reveal the source of the information.

c. If a denial is appropriate, send a written notice denying the request for access. Provide partial access if possible.

d. Granting a Request.

i. Gather the PHI from designated record sets. If copies are to be provided, keep track of the time spent copying the records and the cost of the copies.

ii. Send the response to the request for access to the requestor.

- Provide the access or information in the manner requested, if possible; or

- If not possible, contact requestor to reach an agreement on an alternative manner of delivery (for example, on-site inspection).

6. If the participant, beneficiary, or personal representative appeals a denial that was based on "safety" concerns, the appeal will be reviewed by legal, after consulting with a different licensed health care professional, who should determine within a reasonable period of time whether the denial was appropriate. No other basis for denial is appealable.

7. All documents received or sent relating to the right of access must be tracked on a log of access requests.

8. All written requests, responses, or other related correspondence must be maintained by the Plan.

K. Right to Request Amendment of PHI

POLICY:

Beneficiaries and participants, or their personal representatives, have a right to request amendment of their PHI contained in the Plan's designated record sets.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions should be addressed, in the first instance, by the Privacy Officer.

2. Participants and beneficiaries, or their personal representatives, must submit amendment requests in writing.

    a. In general, before responding to the request, the Privacy Officer should ensure it has the following information:

        i. Name, address, daytime telephone number of the participant or beneficiary making the request;

        ii. If submitted by personal representative, proof of status;

        iii. The particular PHI requested to be amended; and

        iv. Specific reasons for the requested amendment (i.e., a statement of why the existing PHI is inaccurate or incomplete).

    b. No response is required if an amendment request is not submitted in writing and does not contain the reasons supporting the proposed amendment.

3. Amendment requests must be granted or denied within 60 days from the date the written request is received. If it is not possible to respond to an amendment request within 60 days from the date of the request, the Plan may, upon notice to the requestor, take an additional 30 days. The notice of additional time in which to respond must be sent within 60 days from the date of the original amendment request.

4. Denying an amendment request.

    a. An amendment request may be denied if:

        i. The Privacy Officer determines the existing PHI is accurate and complete.

ii. The PHI was not created by the Plan (unless the requestor establishes that the originator of the PHI no longer is available to act on the request).

iii. The PHI is not in the Plan's designated record sets.

iv. The information would not be subject to the right of access, meaning it falls into one of the following four categories:

- The Privacy Officer, after consulting with a licensed health care professional, determines that access will endanger the life or physical safety of the participant or beneficiary or another person.
- The requested PHI contains psychotherapy notes.
- The requested PHI was compiled by the Plan or one of its Business Associates in anticipation of a legal proceeding.
- The information was obtained from someone other than a covered health care provider under a promise of confidentiality and access would likely reveal the source of the information.

b. If a denial of the amendment request is appropriate, send a written notice denying the request for amendment.

5. Participants and beneficiaries may not appeal a denial of their amendment requests. Instead, they may take, and the Plan Sponsor will respond to, the following actions:

a. Written statement of disagreement. Participants and beneficiaries may submit a written statement of disagreement of no more than one page.

i. If the Privacy Officer determines it is necessary, a rebuttal to the written statement of disagreement may be prepared.

ii. The written statement of disagreement (and rebuttal, if any) will be appended or linked to the PHI that is the subject of the amendment request.

iii. The written statement of disagreement (and rebuttal, if any) will be disclosed with any subsequent disclosure of the PHI that is the subject of the amendment request.

b. Request to include amendment request and denial when disclosing information. A participant or beneficiary may request that their original amendment request and the Plan's denial be disclosed with subsequent

disclosures of the PHI that is the subject of the amendment request. Such a request must be complied with.

6. Granting a request.

   a. Identify the records in the designated record sets that contain the PHI that is the subject of the amendment request. The PHI may be maintained by the Plan's Business Associates.

   b. Append or link the amendment to the relevant PHI records.

   c. Notify the requestor in writing that the Plan is granting the request. If the requestor submits the names of persons or entities who they believe have received the medical or health information that is the subject of the amendment request, share the amendment with those persons or entities.

   d. Inform persons or entities, such as Business Associates, that may have relied on the PHI that is the subject of the request.

7. Upon receipt of a notice from another covered entity that the covered entity has agreed to the amendment request of a participant or beneficiary, append or link the amendment in the relevant records in the Plan's designated record sets.

8. All documents received or sent relating to amendment requests must be tracked on a log of amendment requests.

9. All written requests, responses, or other related correspondence relating to amendment requests must be maintained by the Plan.

L. Right to Request an Accounting of Disclosures

POLICY:

Participants and beneficiaries, or their personal representatives, have a right to request an accounting of certain disclosures of their PHI made by the Plan. They are entitled to one free accounting within a twelve-month period. The Plan charges reasonable actual costs for any additional requests within a twelve-month period.

PROCEDURES:

1. The Privacy Officer has responsibility for the implementation of this Policy. All questions about accountings should be addressed, in the first instance, by the Privacy Officer.

2. Generally, participants have the right to receive an accounting of disclosures of their PHI. However, the Plan does not have to comply with the request for accounting if the disclosure was:

    a. Used to provide treatment, payment or health care operations;

    b. Provided to the participant;

    c. Provided for national security or intelligence purposes; or

    d. Provided to correctional institutions or law enforcement officials.

3. Participants and beneficiaries, or their personal representatives, must request an accounting of disclosures of their PHI in writing. In general, before responding to the request, the Privacy Officer should ensure the request includes the following information:

    a. Name, address, daytime telephone number, group health plan enrollment information (i.e., particular plan(s) in which participant or beneficiary is enrolled);

    b. If submitted by personal representative, proof of status; and

    c. Time period of the request.

4. The Plan responds to accounting requests within 60 days from the date a written request is received. If the Plan needs additional time to respond, it will send a notification of additional time to respond to accounting request, which entitles the Plan to an additional 30 days in which to respond.

5. Responding to the Request.

a. Determine if the requestor has submitted an accounting request in the prior 12 months. If so:

   i. Send a written notification of the charges for second request in a 12-month period.

   ii. Do not respond to the accounting request unless you receive an acknowledgment from the requestor agreeing to pay the costs of the accounting.

b. If the request has been submitted by a personal representative, review and substantiate personal representative status. Ensure participant or beneficiary has not requested (and been granted) a restriction on disclosures of confidential communications (see the Plan's Policy on Requests for Restrictions on Use or Disclosure of PHI and the Plan's Policy on Requests for Confidential Communications).

c. Request from any plan sponsor workforce member responsible for tracking covered disclosures any covered disclosures within the applicable time frame of the request (no more than six years).

d. Request from all relevant Business Associates any covered disclosures within the applicable time frame of the request.

e. Provide an accounting of disclosures.

6. All documents received or sent relating to the right to request an accounting must be tracked on a log of accounting requests.

7. Documentation.

   a. Documentation of all covered disclosures will be maintained by the Plan.

   b. All written requests for accountings, responses to such requests, and other related correspondence will be maintained by the Plan.

M. Sanctions for Violating the Privacy Rule

POLICY:

The Plan Sponsor will sanction any employee that uses or discloses a participant's or beneficiary's PHI in violation of the Plan's Policies related to privacy or in violation of the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this Policy.

2. All uses and disclosures of PHI that potentially violate the Plan's Policies related to privacy should be reported directly to the Privacy Officer.

3. The Privacy Officer should, in the first instance, determine whether the allegedly improper use or disclosure violates the Plan's Policies or the Privacy Rule.

4. If there was a violation, the Privacy Officer should take the following steps:

    a. Determine if the improper use or disclosure was intentional or unintentional;

    b. Determine if the improper use or disclosure was a one-time incident or constitutes a pattern or practice;

    c. Determine if there are any mitigating factors (such as self-reporting or lack of proper training or supervision); and

    d. Based on the results of the Privacy Officer's investigation, the employee or employees who improperly used or disclosed the PHI will be subject to disciplinary action in accordance with Plan Sponsor's policy, which may include, but not be limited to: verbal warnings, probation, demotion, temporary suspension, or discharge.

5. The Privacy Officer should consider, in light of the nature of the improper use or disclosure of PHI, if additional training should occur for one or more employees.

6. The Privacy Officer should consider, in light of the nature of the improper use or disclosure of PHI, whether any of the Plan's Policies need to be amended.

7. The Privacy Officer or the Privacy Officer's designee will maintain records showing the sanctions imposed under this Policy for six years following the date the sanctions are imposed.

N. Privacy Complaints

POLICY:

The Privacy Officer will receive and respond to all complaints about the Plan's Policies related to privacy, its adherence to those Policies, or its compliance with the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this Policy.

2. Upon receiving a complaint regarding the Plan's Policies related to privacy, its adherence to those Policies, or its compliance with the Privacy Rule, the Privacy Officer will investigate and, with the assistance of legal counsel if necessary, determine if there is any validity to the complaint.

    a. If the complaint is not valid, meaning the Plan has not violated its Policies or the Privacy Rule, the Privacy Officer will send an appropriate response to the individual who submitted the complaint.

    b. If the Privacy Officer determines that the complaint is valid, the following steps will be taken:

        i. If the complaint is that the Plan's privacy notice, as written, does not comply with the Privacy Rule, and the complaint does not allege any improper use or disclosure of PHI, then the Privacy Officer will determine whether an amendment of the privacy notice and the Plan's Policies is necessary to correct the alleged violation.

        ii. If the complaint is that the Plan or one of its Business Associates used or disclosed PHI in a way that violates the Plan's Policies related to privacy or the Privacy Rule, then the Privacy Officer will:

            - Send a letter (drafted and/or approved by legal counsel) explaining what steps will be taken to correct any future improper uses or disclosures;

            - Determine whether there is any harm that should be mitigated, if practicable, under the Plan's Policy on Mitigation of Harm Due to Improper Uses and Disclosures;

            - If the use or disclosure was by a member of the Plan's workforce, consider whether sanctions should be imposed under the Plan's Policy on Sanctions for Violating the Privacy Rule;

- If the use or disclosure was by a Business Associate, determine whether further investigation or actions are necessary to ensure future violations do not occur;

- Consider, in light of the nature of the improper use or disclosure of PHI, if additional training should occur for one or more employees; and

- Consider, in light of the nature of the improper use or disclosure of PHI, whether any of the Plan's Policies need to be amended.

3. All complaints and their disposition (i.e., response letters) must be documented and retained for six years. These documents will be maintained by the Plan.

O. Mitigation of Harm Due to Improper Uses or Disclosures

POLICY:

The Plan will mitigate, to the extent practicable, any harm caused by a use or disclosure of a participant's or beneficiary's PHI that is in violation of the Plan's Policies related to privacy or in violation of the Privacy Rule.

PROCEDURES:

1. The Privacy Officer has responsibility for implementation of this Policy.

2. If any plan sponsor workforce member or other employee has been made aware that PHI has been misused by an employee or Business Associate, the employee shall report this information to the Privacy Officer.

3. Upon learning of an improper use or disclosure by a plan sponsor workforce member or Business Associate, the Privacy Officer will take the following steps:

    a. Determine whether a participant or beneficiary could be or has been harmed by the improper use or disclosure;

    b. Determine whether there are any practicable steps that might have a mitigating effect with regard to the potential harm identified. If so, implement the mitigating steps; and

    c. Determine if improper use or disclosure constitutes a Breach. If so, implement the Plan's Breach Policy.

P. No Retaliation or Intimidation

POLICY:

The Plan will not retaliate against any participant or beneficiary who chooses to exercise his or her individual privacy rights, including the right to access PHI, the right to request amendment of PHI, the right to an accounting of disclosures, and the right to request certain privacy restrictions. The Plan also will not intimidate any participant or beneficiary who seeks to exercise those rights. Further, the Plan will not retaliate against or intimidate any person or organization that files a complaint regarding the Plan's privacy practices with HHS, that participates in any investigation of the Plan's privacy practices, or that opposes any act of the Plan that allegedly violates the Privacy Rule.

Q. No Waiver of Rights

POLICY:

The Plan will not require participants or beneficiaries to waive any rights under the Privacy Rule in order to enroll in the Plan or in order to receive the provision or payment of benefits under the Plan.

R. Notice of Privacy Practices

POLICY:

The Privacy Officer is responsible for developing and maintaining a Notice of Privacy Practices that complies with the Privacy Rule.

PROCEDURES:

1. The Notice of Privacy Practices will be placed on the Plan Sponsor's intranet site, if any, or website where the Plan Sponsor posts other benefit plan information.

2. The Notice of Privacy Practices will be provided to each newly eligible employee upon hire, or if later, when the employee first enrolls in the Plan.

3. The Notice of Privacy Practices will be provided to any participant or beneficiary upon request.

4. A new Notice of Privacy Practices will be provided within 60 days of any material revision to these Policies related to privacy.

5. At least once every three years, the Plan will notify individuals then covered by the Plan of the availability of the Notice of Privacy Practices and how to obtain it.

PART III

SECURITY POLICIES

A. Risk Analysis

POLICY:

The Security Officer will periodically conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to the confidentiality, availability and integrity of all Electronic PHI that the Plan or Plan Sponsor creates, receives, maintains, or transmits. The Security Officer will update the risk analysis as required to respond to risks associated with environmental or operational changes.

PROCEDURES:

The risk analysis will include the following:

1. A thorough analysis of information systems, including hardware, software, input and output sources, and identification of all Electronic PHI;

2. Identification of possible threats to the confidentiality, integrity, and availability of Electronic PHI. These threats include:

    a. natural threats such as floods, earthquakes, tornadoes, and landslides;

    b. human threats such as network and computer based attacks, malicious software upload, unauthorized access to Electronic PHI and unintentional actions (e.g., inadvertent data entry or deletion and inaccurate data entry);

    c. environmental threats such as power failures, pollution, chemicals, and liquid leakage;

3. Identification of vulnerabilities, such as failure to disable the passwords of terminated employees, poor or nonexistent firewalls, ineffective barriers to viruses and other malicious software, failure to install operation system patches, fire-control measures that damage hardware and software, etc.;

4. Determination of the likelihood and impact of each identified threat; and

5. Identification of the features that should be implemented to lessen threats to a reasonable and appropriate level.

B. Risk Management

POLICY:

The Plan will manage risks to its Electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level. Security measures put into place will be commensurate with the risks to the information systems that store, process, transmit or receive Electronic PHI, and will be designed to reduce the risks to Electronic PHI to reasonable and manageable levels. The risk management plan and these Policies were developed with the understanding that the Plan Sponsor maintains very little Electronic PHI on its systems.

PROCEDURES:

1. The Plan Sponsor will apply already existing University security policy and procedures to reduce risks and vulnerabilities to a reasonable and appropriate level. To the extent that the standard University security policy and procedures do not adequately reduce risks and vulnerabilities to Electronic PHI, the Plan will implement additional measures to reduce the risks and vulnerabilities.

2. The Plan will prioritize risk mitigation efforts based on the following when managing its risks:

    a. The size, complexity, and capabilities of the Plan;

    b. The Plan's technical infrastructure, hardware, software, and security capabilities;

    c. The costs of security measures; and,

    d. The criticality of the Electronic PHI potentially affected.

3. The Plan will use a risk matrix to assist in determining risk levels and show the likelihood of threat occurrence and resulting impact of threat occurrence.

4. The Plan will prioritize risks using information from the risk analysis. When deciding what resources should be allocated to identified risks, the highest priority will be given to risks with unacceptable risk ratings.

C. Sanctions for Violating the Security Rule

POLICY:

The Plan Sponsor will sanction any employee that has violated any part of these Policies related to security or the Security Rule.

PROCEDURES:

1. The Security Officer has responsibility for implementation of this Policy.

2. Any incidents that potentially violate the Plan's Policies related to security should be reported directly to the Security Officer.

3. The Security Officer should, in the first instance, determine whether the alleged incident violates the Plan's Policies or the Security Rule.

4. If the violation was the result of an act or omission of a workforce member, the Security Officer should take the following steps:

    a. Coordinate with the Privacy Officer to determine if the violation was intentional or unintentional;

    b. Determine if the workforce member's action or omission was a one-time incident or constitutes a pattern or practice;

    c. Coordinate with the Plan Sponsor to determine if there are any mitigating factors (such as self-reporting or lack of proper training or supervision); and

    d. Based on the results of the investigation, the employee or employees involved will be subject to disciplinary action in accordance with Plan Sponsor's discipline policies, up to and including discharge.

5. If the violation was the result of an act or omission of a Business Associate or the agent or subcontractor of a Business Associate, the Security Officer should take the steps outlined in the Business Associate Agreement and determine if the contractual relationship with the Business Associate should be terminated.

6. The Security Officer should coordinate with the Privacy Officer to determine whether the violation resulted in an improper use or disclosure of PHI that could harm the participant or beneficiary or if the violation constituted a breach. If harm may occur, the Privacy Officer should implement the Plan's Policy on Mitigation of Harm Due to Improper Uses and Disclosures. If the violation was a breach, the Security Officer should implement the Plan's Policy on Breach Notifications.

7. The Security Officer should consider, in light of the nature of the violation, if additional training should occur for one or more employees.

8. The Security Officer should consider, in light of the nature of the security violation, whether any of Plan's Policies need to be amended.

9. The Security Officer or the Security Officer's designee will maintain records showing the sanctions imposed under this Policy for six years following the date the sanctions are imposed. These documents will be maintained by the Plan.

D. User Access Management

POLICY:

The Plan Sponsor shall establish rules for authorizing access to the computing network, applications, workstations, and to areas where Electronic PHI is accessible. Workforce members shall have authorization when working with Electronic PHI or when working in locations where it resides. Workforce security includes ensuring that only workforce members who require access to Electronic PHI for work related activities shall be granted access and that when work activities no longer require access, authorization shall be terminated. The policy also permits management to grant emergency access to workforce members who have not completed HIPAA security training if the facility declares an emergency. In addition, this Policy provides guidelines on how user access is routinely reviewed and updated.

PROCEDURES:

1. The Plan Sponsor will have the responsibility for authorizing all individuals access to the electronic communication systems that contain PHI and the Security Officer or the Security Officer's designee will have the responsibility for granting access authority to all individuals authorized by the Plan Sponsor to access the electronic communication systems that contain PHI.

    a. Only individuals who have a "need to know" will be provided access to PHI.

    b. Workforce members will only be granted access to the minimum necessary to electronic PHI that they require to perform their duties.

2. Plan Sponsor began obtaining background checks on all workforce members upon commencement of employment beginning July 1, 2017.

3. All workforce members with access to Electronic PHI will have a unique identification and password for the electronic systems.

4. All workforce members with access to Electronic PHI through outside vendor websites are given unique identification and passwords to those systems.

5. The Security Officer shall maintain a list of authorized individuals and their level of access to both internal systems containing PHI and outside vendor systems containing PHI.

6. The Security Officer shall periodically check with Business Associates to receive an account report from each Business Associate for confirmation of active user accounts and privileges.

7. The Plan Sponsor will determine when a workforce member is hired or promoted what level of access the individual will have to the Plan Sponsor's electronic

communication system and the data that the workforce member can access and use. The supervisor of such individual will communicate this information to the Security Officer or the Security Officer's designee, so that appropriate access is granted.

8. The Plan Sponsor will notify the Security Officer or the Security Officer's designee when a workforce member's access needs to be terminated. The Security Officer or the Security Officer's designee shall terminate access to information systems, including terminating any login capabilities to any systems that contain Electronic PHI, and other sources of PHI including access to rooms or buildings where PHI is located, when a workforce member, agent or Business Associate ends his or her employment or engagement.

9. The Security Officer or the Security Officer's designee will terminate access to specific types of PHI when the status of a workforce member no longer has a "need to know" of those types of information.

10. The Security Officer will disable user access when it finds a breach that endangers the security of electronic PHI.

11. If a workforce member changes role, the Privacy Officer is responsible for evaluating the member's current access and for requesting new access to Electronic PHI commensurate with the workforce member's new role and responsibilities.

12. The Security Officer may make exceptions to these access procedures for the following:

    a. To comply with a legitimate request from public health or law enforcement officials;

    b. To ensure continued operations of the organization in the presence of temporary mechanical or technical interruption;

    c. To ensure continued operations of the organization when temporarily or permanently replacing a workforce member who has access to Electronic PHI; or

    d. To audit the effectiveness of the Policies related to security.

13. The Security Officer has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if the facility declares an emergency or is responding to a natural disaster that makes the management of plan information security secondary to immediate personnel safety activities or management determines that granting immediate access is in the best interest of plan participants.

14. If the Security Officer grants emergency access, the Security Officer shall review the impact of emergency access and document the event within 24 hours of it being granted.

15. After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.

16. It may be necessary for the Security Officer to grant emergency access to a user's account without the user's knowledge or permission. This access may be granted if:

    a. The workforce member terminates or resigns and management requires access to the person's data;

    b. The workforce member is out for a prolonged period; or

    c. The workforce member has not been in attendance and therefore is assumed to have resigned.

E. Authentication & Password Management

POLICY:

The Plan Sponsor shall ensure that all information systems shall uniquely identify and authenticate workforce members. Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of Plan Sponsor's entire network. As such, all worksite employees are responsible for taking the appropriate steps to select and secure their passwords.

PROCEDURES:

1. Passwords to any systems containing PHI must be changed in accordance with the University's password policy.

2. Passwords should be constructed consistent with University policy.

3. Passwords must not be inserted into email messages or other forms of electronic communication unless protected.

4. Passwords should not be shared with others. In cases where password sharing is unavoidable, restricted accounts should be established to protect information resources.

5. If passwords need to be written down or stored on-line, they must be stored in a secure place separate from the application or system that is begin protected by the password.

6. The "Remember Password" feature should not be used by any workforce member, unless the system or application has the means to encrypt the "remembered password."

7. For logging into the Plan Sponsor's system remotely, a multifactor authentication system has been implemented.

8. If an account or password is suspected to have been compromised, the workforce member shall report the incident to the Security Officer in accordance with the Security Incident Response and Reporting Policy and change all passwords to systems containing PHI immediately.

F. Log-In Monitoring

POLICY:

To ensure that computers and workstations containing Electronic PHI are appropriately secured, the Plan Sponsor will configure all critical components that process, store or transmit Electronic PHI to record log-in attempts and lock in accordance with standard security policy and procedures.

PROCEDURES:

1. Plan Sponsor uses extensive endpoint protection to protect against impermissible logins.

2. The Security Officer or the Security Officer's designee will review such log-in activity reports and logs on a periodic basis.

3. All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported immediately to the Security Officer and will be promptly investigated by the Security Officer.

4. The multi-factor authentication system locks a user out after 10 failed attempts and notifies the IT department after the 10th bad attempt. The IT department will promptly investigate and take appropriate action.

G. Facility Access Controls

POLICY:

The Plan Sponsor shall reasonably safeguard Electronic PHI from any intentional or unintentional use or disclosure and shall protect its facilities where Electronic PHI is located. The Plan Sponsor shall safeguard the equipment therein from unauthorized physical access, tampering, and theft. The Security Officer shall periodically audit Plan Sponsor facilities to ensure Electronic PHI safeguards are continuously being maintained.

PROCEDURES:

1. Workforce members should not share access cards, hard key access, or alarm or keypad codes.

2. In facilities where Electronic PHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls that vary depending on facilities structure, type of visitors, and where Electronic PHI is accessible.

3. If facilities use metal/hard keys, the appropriate key locks shall be changed when keys are lost or a workforce member leaves without returning a key.

4. Every network closet shall be locked whenever the room is unoccupied or not in use.

5. The server shall always be in a location that is behind at least one locked door.

6. Repairs or modifications to any physical security (e.g., replacement of locks) for each facility where Electronic PHI can be accessed shall be logged and tracked by the Plan Sponsor.

H. Workstation Use & Security

POLICY:

The Plan Sponsor shall establish procedures for securing workstations that access Electronic PHI. Since Electronic PHI may be portable, this Policy requires workforce members to protect Electronic PHI in all locations.

PROCEDURES:

1. All workstations required their own unique identification and passwords.

2. Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens.

3. Workforce members shall always have the user session-lock implemented when any computer or device they use to access Electronic PHI is left idle.

4. All workstations with Electronic PHI are set to automatically log off and/or screen lock after a period of inactivity. The automatic log off and/or screen locking should block further access until the workforce member reestablishes the connection using the identification and authentication process.

5. The Plan Sponsor will take corrective action against any person who knowingly violates the security of workstation use.

6. Workforce members who work from home or other non-office sites shall take the necessary steps to protect Electronic PHI from other persons who may have access to their home or other non-office sites, including password protection on personal computers, and security for all other forms of Electronic PHI such as locking smart phones, and laptops.

I. Portable Device & Media Controls

POLICY:

The Plan Sponsor shall ensure that Electronic PHI that is created, received, maintained or transmitted on portable devices, storage devices and removable media is appropriately controlled and managed. This Policy covers accountability, media re-use, disposal, and data backup and storage as well as use of portable devices to access PHI. It only applies to the portable devices that may be used to access, receive or transmit Electronic PHI. Portable devices include laptops, tablets, smart phones, and other similar devices. Storage devices and media include, but are not limited to, CD rom disks, USB drives, backup tapes, copiers and printers, and other items that can hold data.

PROCEDURES:

1. Portable devices that are assigned to workforce members for remote use will be accounted for on a computer asset inventory.

2. Unless necessary, no Electronic PHI, including screenshots of Electronic PHI, shall be saved on portable devices.

3. Workforce members shall protect all the hardware and electronic media that contain Electronic PHI.

4. In order to limit the amount of portable Electronic PHI, workforce members shall not save Electronic PHI on CD Rom disks, USB drives, or other portable items. The Electronic PHI must be stored either on the network or an electronic media that can be retrieved in an emergency.

5. All workforce members shall receive permission from the Privacy Officer before removing Electronic PHI from the facility. Approvals shall include the type of permission and the time period for the authorization. The time period shall not exceed one year and should be documented.

6. Laptops, tablets and other portable devices that can access the Plan Sponsor's network must be configured to the Plan Sponsor's standards prior to remote use.

7. All remote access to the Plan Sponsor's networks or cloud-based applications containing Electronic PHI shall be done with the use of a secure access.

8. All portable devices must be configured to automatically log off in accordance with the Workstation Use & Security Policy and to comply with the Protection from Malicious Software Policy. Workforce members are not permitted to change any of the security settings on their University issued portable devices without approval from the Security Officer.

9. When portable device security patches or updates are not able to be automatically downloadable but otherwise can be downloaded from a website, the Security Officer or his designees, will notify, by email, all workforce members who have a University issued portable devise requesting they download and install the update.

10. Portable devices that may contain Electronic PHI will be encrypted at either the entire drive or solid-state memory level, or with a partition encryption where the partition contains Electronic PHI.

11. Mobile telephones that have access to the University's email system will be configured with remote security controls that will remotely wipe the device upon loss or theft.

12. Portable devices, when in transit, must be carried in the workforce member's immediate vicinity with appropriate covers or containers. Portable devices should never be left unattended in a public place.

13. Portable devices that may contain Electronic PHI may not be used by family, friends or other unauthorized individuals.

14. If Electronic PHI is lost, workforce members are responsible to promptly contact the Security Officer within one business day upon awareness that Electronic PHI is lost.

15. Tablets and smartphones that are used to access, receive or transmit Electronic PHI via email shall only do so within a secure domain and the email settings on the device shall be configured to limit the number of recent emails stored on the device.

16. Workforce members shall never text Electronic PHI or request PHI be texted to them. If a text message received by a workforce member contains Electronic PHI, the workforce member should immediately delete the text message.

17. Portable devices that use wireless communications including Bluetooth will be configured to always turn off the discoverable mode to ensure the device is not viewable by unauthorized persons. Alternatively, where discoverable mode is necessary for proper pairing, workforce members hall be trained to disable this mode when in public places.

18. All Electronic PHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the Electronic PHI or when the equipment is transferred to a new worker with different Electronic PHI access needs. Hard drives shall be wiped clean before transfer. In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

19. Electronic media and portable devices that contain Electronic PHI will be wiped of all PHI before disposal. If the media is not technology capable of being cleaned, the media shall be overwritten or destroyed.

20. When the technology is capable and where no other backup copies exist, an exact copy of the Electronic PHI shall be created and the Electronic PHI removed from the server hard drive before sending the device out for repair.

21. Before moving server equipment that contains Electronic PHI, a retrievable copy needs to be created.

22. Data backups should be reviewed periodically to verify the reliability and integrity of the backup.

J. Transmission Security

POLICY:

Electronic PHI that is transmitted over an electronic communications network shall be protected against unauthorized access to, or modification of, Electronic PHI. When Electronic PHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

PROCEDURES:

1. When the Security Officer feels it is necessary to protect the security of Electronic PHI, Electronic PHI will be encrypted while at rest.

2. When possible, Electronic PHI should be uploaded or downloaded using a secure website. When Electronic PHI must be emailed, consideration will be given to encrypting the information before sending it.

3. When communicating internally, no encryption is necessary.

4. Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the Security Officer.

5. When technology is capable, the transmission of Electronic PHI over a wireless network within the Plan Sponsor's domain is permitted if the local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized and the local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

6. Electronic PHI should not be sent over a public wireless network or over a private wireless network that is not utilizing an authentication mechanism, unless the Electronic PHI is encrypted before transmission.

K. Protection From Malicious Software

POLICY:

The Plan Sponsor will take all reasonable measures to ensure that computers that may be used to access, receive, transmit or otherwise use Electronic PHI will be protected from viruses, worms, ransomware, or other malicious codes.

PROCEDURES:

1. Consistent with University procedures, all computers owned, leased or operated by Plan Sponsor have enterprise-level anti-virus software installed and maintained. Such software is automatically and regularly updated.

2. Workforce members will be instructed not to disable the automatic virus scanning feature.

3. All downloadable files shall be virus checked prior to use.

4. Advanced technologies have been installed for detecting and testing email for malicious content or links.

5. Plan Sponsor automatically and regularly provides security patches, including on portable devices that may contain Electronic PHI.

6. The Security Officer or the Security Officer's designee shall provide security reminders to the workforce to inform them of any new virus, worm, ransomware, or other type of malicious code that may be a threat to Electronic PHI.

7. Workforce members should delete spam, chain and other junk email without forwarding and should never download files form unknown or suspicious sources.

8. Workforce members are instructed to immediately contact the IT department if a virus, worm, ransomware, or other malicious code is suspected or detected.

9. In the event that a virus, worm, ransomware, or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately cleaned.

L. System Audits, Audit Controls & Activity Review

POLICY:

The Security Officer or the Security Officer's designee shall implement controls for auditing Plan Sponsor's systems policies and procedures to ensure that implemented security controls are effectively protecting the integrity, availability and confidentiality of Electronic PHI.

PROCEDURES:

1. All processing systems with Electronic PHI will be audited on a regular basis. The information reviewed will include, but not be limited to, audit logs, access reports, and security incident tracking reports.

2. The Plan Sponsor leverages a portfolio of third-party detection capabilities.

3. The level and type of auditing mechanisms implemented will be determined by the most recent risk analysis and reviewed periodically. Auditable events can include but are not limited to:

    a. Access of Electronic PHI files;

    b. Use of workforce member's account;

    c. Information system start-up or stop;

    d. Failed login attempts;

    e. System upgrades; and

    f. Security Incidents.

4. A process will be developed for the review of exception reports and/or logs.

5. The Security Officer or the Security Officer's designee will periodically conduct audits of workforce member's computers to ensure virus protection is being maintained at correct levels.

6. Documentation of any risks or violations should be documented and kept for six years.

M. Response and Reporting

POLICY:

The Plan Sponsor will identify and respond to suspected or known security incidents to protect the integrity, availability, and confidentiality of Electronic PHI. The Plan Sponsor will mitigate the harmful effects of known or suspected security incidents to the extent possible and document the security incidents and their outcomes. It is imperative that this Policy be followed when responding to security incidents.

PROCEDURES:

1. All security incidents, threats, violations, or activities contrary to the Plan Sponsor's Acceptable Use Policy that affect or may affect the confidentiality, integrity or availability of Electronic PHI shall be reported and responded to promptly.

2. Incidents that shall be reported include, but are not limited to:

    a. Virus, worm, trojan, ransomware, or other malicious code attacks;

    b. Network or system intrusions or persistent intrusion attempts from a particular entity;

    c. Compromised passwords or data;

    d. Unauthorized access to Electronic PHI, an Electronic PHI based system, or an Electronic PHI based network, Electronic PHI data loss due to disaster, failure, error, theft;

    e. Loss of any electronic media that contains Electronic PHI;

    f. Loss of the integrity of Electronic PHI; and

    g. Unauthorized person found in Plan Sponsor's facility where PHI is kept or other physical security breaches or attempts.

3. The Security Officer shall be notified immediately of any suspected or actual security incident. If it is unclear as to whether a situation is a security incident, the Security Officer shall be contacted to evaluate the situation.

4. Any incidents that potentially violate the Plan's Policies should be reported directly to the Security Officer.

5. Upon notification of a security incident report, the Security Officer will review (and conduct superficial investigation if necessary) in order to confirm the validity and level of risk associated with the reported incident.

6. The Security Officer, Privacy Officer and any other department manager will convene within a reasonable period of time upon notification of the security incident to:

   a. Investigate and validate the facts included in the incident report, including any damage to the organization;

   b. Determine if the incident needs to be reported to law enforcement;

   c. Determine if the incident is a breach and if it is a Breach the procedures in the Breach policy should be followed;

   d. Determine if any sanctions are necessary in accordance with the Sanctions Policy;

   e. Lessen or mitigate any harmful effects to the extent necessary and applicable;

   f. Determine if issue should result in any changes to Security policies or procedures; and

   g. Address communication and training to all affected workforce members and provide refresher training as needed.

7. The Security Officer shall test the incident response capability periodically using tests and exercises to determine the effectiveness.

8. On a routine basis, the Security Officer should provide to the leadership team aggregate reporting of all received security incident reports, the organization's response, including any sanctions applied, mitigation attempts, and/or resulting changes to procedures as a result of these security incidents.

9. A report of all security incidents shall be maintained for at least six years.

10. If the Plan Sponsor is notified by a Business Associate of a Security incident that occurred with Electronic PHI in its possession or a subcontractor's possession, the Security Officer shall work with the security officer of the Business Associate to investigate the incident in accordance with this Policy.

N. Contingency Plan

POLICY:

The Plan Sponsor needs to have procedures in place to access any necessary Electronic PHI when normal resources are not available. These procedures will be used in the event of an emergency, disaster or other occurrence (e.g., fire, vandalism, system failure, natural disaster or ransomware attack) when any system that contains Electronic PHI is affected, including: applications and data criticality analysis, data backup, disaster recovery plan, and emergency mode operation plan. Since the Plan Sponsor maintains very little Electronic PHI on its systems and what it does maintain is information also maintained by outside service providers, these procedures should rarely, if ever, need to be implemented.

PROCEDURES:

1. The contingency plans must be periodically reviewed and tested by the Security Officer to determine if new procedures need to be implemented.

Applications and Data Criticality Analysis

2. The Security Officer shall assess the relative criticality of specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

3. The Security Officer shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact, if any.

4. The assessment of data and application criticality shall be conducted periodically to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup

5. All Electronic PHI shall be stored on network servers in order for it to be automatically backed up by the system consistent with University information technology policy and procedures.

6. Electronic PHI shall not be saved on the local drives of personal computers.

7. Electronic PHI shall not be stored on portable media and shall be saved to the network to ensure backup of Electronic PHI data.

8. The system shall conduct backups of user-level and system-level information and store the backup information in a secure location consistent with University information technology policy and procedures.

9. If an off-site storage facility or backup service is used, a written contract shall be used to ensure that the contractor shall safeguard the Electronic PHI in an appropriate manner.

Disaster Recovery Plan

10. Plan Sponsor has a University wide disaster recovery plan that ensures that each workforce member can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, natural disaster or ransomware attack. The Disaster Recovery Plan need not be additionally modified for HIPAA if Plan Sponsor does not maintain any Electronic PHI that is not maintained by an outside service provider.

Emergency Mode Operation Plan

11. The Security Officer shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of Electronic PHI while operating in emergency mode. Emergency mode operation involves those critical business processes that shall occur to protect the security of electronic PHI during and immediately after a crisis situation. An Emergency Mode Operation Plan need not be established if the Plan Sponsor does not maintain any Electronic PHI that is not maintained by an outside service provider.

12. Emergency mode operation procedures shall be tested on a periodic basis to ensure that critical plan processes can continue in a satisfactory manner while operating in emergency mode.