PAISBOA
Health Benefit Trust

THE TRUSTEES OF THE PHILADELPHIA AREA INDEPENDENT SCHOOL BUSINESS OFFICERS ASSOCIATION HEALTH BENEFIT TRUST

THE PHILADELPHIA AREA INDEPENDENT SCHOOL BUSINESS OFFICERS ASSOCIATION HEALTH BENEFIT PLAN

HIPAA Privacy Policies and Procedures

Effective July 1, 2023

TABLE OF CONTENTS

PAGE

PAISBOA
HEALTH BENEFIT TRUST

INTRODUCTION

The Trustees ("Plan Sponsor") of the Philadelphia Area Independent School Business Officers Association Health Benefit Trust (the "Trust") sponsor the Philadelphia Area Independent School Business Officers Association Health Benefit Plan (the "Plan"). The Plan is a Covered Entity for purposes of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule").[1] and is administered in accordance with the Privacy Rule and these Policies and Procedures.[2]

The Plan Sponsor is the Plan Administrator, responsible for administering the Plan. The Plan Administrator has delegated day-to-day Plan administration authority to certain employees of the Plan Sponsor, referred to as "Privacy Employees" and to certain third parties referred to "Business Associates."

The Plan Administrator, the Privacy Employees and the Business Associates request, receive, use, store and disclose individually identifiable health information about participants and their dependents for the purpose of administering the Plan. This information is protected health information ("PHI") that is protected by the Privacy Rule and covered by these Policies and Procedures.

In addition, the Plan Sponsor, Business Associates, and their authorized agents may perform various non-administration functions related to the Plan, such as collecting enrollment information, deciding plan eligibility, remitting payment for premiums and claims advocacy. The information collected by the Plan Sponsor or its agents when it is performing these functions is not PHI and is not protected by the Privacy Rule or these Policies and Procedures.

The Plan Sponsor, in its capacity as employer, may also request, receive and store health information about its employees for employment-related purposes, or to determine whether an employee is eligible for leave benefits under the Family and Medical Leave Act or an accommodation under the Americans with Disabilities Act. This health information, which is received and stored by the Plan Sponsor in its capacity as employer, is not PHI and is not protected by the Privacy Rule or these Policies and Procedures.

I. PRIVACY POLICY STATEMENT

POLICY: The Plan is committed to complying with the Privacy Rule.

These Privacy Policies and Procedures ("Policies and Procedures") are designed and intended to ensure[3] the Plan's compliance with the Privacy Rule. The Plan adopts these Policies and Procedures to protect the PHI that it creates and maintains from unauthorized use, disclosure, or access, and to maintain the confidentiality and integrity of that PHI. These Policies and Procedures also ensure that individuals have rights related to their PHI. Through the Plan's Notice of Privacy Practices ("Privacy Notice") individuals are informed of the Plan's legal duties and these Policies and Procedures, as well as their individual rights with respect to their PHI.

These Policies and Procedures will be amended and/or supplemented as necessary and appropriate to comply

---

1 This refers to the Privacy Rule, 45 C.F.R. Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health Act, which is at Section 13400, *et. seq.* of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 17921, *et. seq.*, and any regulations promulgated thereunder ("HITECH").

2 The Plan Sponsor sponsors benefits which are not covered by HIPAA and/or these Policies and Procedures.

3 The term "ensure" as used throughout these Policies and Procedures is not meant to guarantee compliance with the Privacy Rule. Rather, "ensure" shall mean the Privacy Officer, Privacy Employees, Business Associates and others, as applicable, will use their best efforts to comply with the Privacy Rule.

with changes in the law or regulations or other interpretation of the Plan's privacy-related obligations, or to reflect changes related to the Plan or the internal structure of the Plan Sponsor. The Plan will document and implement changes to these Policies and Procedures whenever there is a change in the law, regulations or interpretation of the Plan's privacy obligations and/or a material change to the uses or disclosures of PHI or other privacy practices that necessitate a change in these Policies and Procedures. If a change requires revisions to the Privacy Notice, the Plan will not implement the change before the effective date of the revised Privacy Notice unless the Privacy Officer deems it necessary to apply the change to PHI that the Plan created or received before this effective date.

II. PERSONNEL DESIGNATIONS

POLICY: The Plan Administrator has designated a Privacy Officer and HIPAA Contact Person or Office.

A. **PRIVACY OFFICER DESIGNATION.** The Plan Administrator has designated a Privacy Officer who is responsible for overseeing and directing the development and implementation of the Plan's Privacy Policies and Procedures in compliance with the Privacy Rule.

1. **Designated Privacy Officer.** The Plan Administrator has designated the following Privacy Officer:

Executive Director
PAISBOA Health Benefit Trust
301 Iven Avenue, Suite 315
Wayne, Pennsylvania 19087
(484) 580-8844
executive.director@phbtrust.org

2. **Duties and Responsibilities.** The Privacy Officer is responsible, either directly or by delegated authority, for monitoring and ensuring the Plan's compliance with the Privacy Rule requirements and these Policies and Procedures. The Privacy Officer:

a. Oversees the development and implementation of HIPAA compliance processes, and supervises the day-to-day aspects of compliance with the Privacy Rule;

b. Coordinates with Business Associates to identify HIPAA non-compliant processes and systems, and develops and implement those changes necessary to ensure all processes and systems involving the Plan are HIPAA compliant;

c. Serves as central liaison for Business Associates involved in HIPAA systems and processes, and for external business partners and vendors involved in HIPAA systems and processes;

d. Communicates HIPAA compliance assessment findings, including cost and risk exposure, to the Plan Administrator and impacted department personnel;

e. Tracks action items;

f. Prepares budgets for HIPAA compliance as necessary and appropriate;

g. Responds to inquiries from individuals, government officials and other third parties regarding uses and disclosures of PHI, and promptly renders determinations in response to such inquiries and requests;

h. Oversees workforce training on HIPAA compliance;

i. Ensures that the Plan's Privacy Notice is timely disseminated to individual participants; and reviews and revises the Privacy Notice to reflect any changes to the law or these Policies and Procedures or practices;

j. Responds to inquiries from individuals about the Plan's privacy procedures;

k. Investigates any complaints that allege that the Plan, the Plan Administrator, a Privacy Employee, any other Plan Sponsor employee, or a Business Associate has not complied with or has violated these Policies and Procedures;

l. Investigates and conducts risk assessments related to any breach of the Privacy Rule to determine whether Notification of Breach (as provided in Policy VII) is required, and, as appropriate and necessary, provides such Notification in accordance with Policy VII.

m. Oversees document maintenance and retention policies; and

n. Reviews and revises these Policies and Procedures as required or needed to ensure continued compliance with the Privacy Rule and any other applicable law.

B. **HIPAA CONTACT PERSON OR OFFICE DESIGNATION.** The Plan Administrator has designated the Privacy Officer as the HIPAA Contact Person responsible for receiving complaints and providing information about the Privacy Rule and these Policies and Procedures.

1. **Designated HIPAA Contact Person or Office Designation.** The Plan Administrator has designated the following as the HIPAA Contact Person:

Executive Director
PAISBOA Health Benefit Trust
301 Iven Avenue, Suite 315
Wayne, Pennsylvania 19087
(484) 580-8844
executive.director@phbtrust.org

2. **Duties and Responsibilities.** The HIPAA Contact Person is responsible for:

a. Performing functions delegated by the Privacy Officer.

b. Receiving and processing complaints, as well as reports of non-compliance and breaches of privacy;

c. Maintaining the original versions of these Policies and Procedures and the Privacy Notice, and, as these documents are updated, maintaining files of the various versions of those documents;

d. Maintaining copies of the Privacy Notice and promptly providing the Privacy Notice to any individual that requests it;

e. Maintaining documentation related to the disposition of complaints;

f. Maintaining risk assessments conducted for Notification of Breach purposes, copies of any Notices of Breach that are sent or published, and records of the individuals or entities that received such Notices; and

g. Responding promptly to any queries about these Policies and Procedures.

C. **DOCUMENTATION.** Documentation related to these personnel designations will be retained for 6 years in accordance with the Trust's document retention policy.

III. RESTRICTED INTERNAL ACCESS TO PROTECTED HEALTH INFORMATION

POLICY: The Plan Administrator has implemented reasonable safeguards, including appropriate administrative, technical and physical measures, to protect the privacy of PHI, and to prevent impermissible uses and disclosures of PHI. The Plan Administrator and Plan Sponsor have limited access to PHI to only those Plan Sponsor employees who need to use or disclose PHI to carry out their duties.

A. **LIMITED EMPLOYEE ACCESS.** Access to PHI is limited to the following Plan Sponsor employees for the purpose(s) described herein. The Plan Sponsor employees identified in this Section, who are known as the "Privacy Employees" perform the day-to-day services on behalf of the Plan in compliance with the Privacy Rule. These individuals have access to the below-described PHI in order to perform day-to-day, administrative services and other job functions on behalf of the Plan. These employees are listed by title with the understanding that any individual who has the title performs job responsibilities that require access to or the use and disclosure:

1. **Executive Director** - The Executive Director may need access to PHI from time to time in order to perform certain job functions. The Executive Director will only access (or request a Business Associate to access) relevant PHI that is necessary under the circumstances.

2. **Chief Financial Officer** - The Chief Financial Officer may need access to PHI from time to time in order to perform certain job functions. The Chief Financial Officer will only access (or request a Business Associate to access) relevant PHI that is necessary under the circumstances.

3. **Director of Marketing and Communications** - The Director of Marketing and Communications may need access to PHI from time to time in order to perform certain job functions. The Director of Marketing and Communications will only access (or request a Business Associate to access) relevant PHI that is necessary under the circumstances.

4. **Trustees -** The Trustees review and issue appeal determination letters and do not use PHI for any other aspect of their job responsibilities. These individuals are included as Privacy Employees for this limited purpose and will be trained on HIPAA prior to the commencement of any such services.

B. ACCESS CONTROLS AND PHYSICAL PROTECTIONS

1. **External Physical Protections.**

   a. Privacy Employees work from an office space in Wayne, Pennsylvania. All Privacy Employees work within secured workspaces (i.e., locked and/or badged access). Under no circumstances may an individual enter the Privacy Employees' workspace unescorted.

2. **Physical Layout and How Hardcopy PHI Is Handled in Each Location**.

   a. No hard copy PHI is maintained in the office space, and each Privacy Employee is provided with a secure laptop. From time-to-time Privacy Employees will work from their residences. No hard copy PHI is maintained at personal residences.

Privacy Employees do not leave laptops unattended while in use and keep laptops in a locked drawer when not in use.

3. **Secure Equipment**.

   a. **Computer Security.** Privacy Employees do not leave PHI on unattended computer screens. All computer systems are password protected with automatic log-off after a certain amount of inactivity.

      (i) **Email Security.** Privacy Employees do not generally email ePHI. If there is a need to email ePHI, such ePHI is password protected and/or encrypted with Sharefile by Citrix**.**

      (ii) **Network Security**. No ePHI is saved on the Plan Sponsor's network. ePHI is accessed through vendor websites and not saved locally.

   b. **Fax Machines.** PHI is not faxed.

   c. **Printers**. PHI is not printed.

   d. **Copiers**. PHI is not copied.

4. **Secure Conversations.**

   a. **With Others Who Have Access To PHI.** The Privacy Employees only discuss PHI with one another and with Business Associates in private settings and only as required to perform their job responsibilities. Conversations that involve PHI are conducted using moderate voice tones. In most instances the names and any other identifiable information are removed from conversations to protect the identity of covered individuals.

   b. **With Those Who Do Not Have Access to PHI.** The Privacy Employees do not discuss PHI with anyone who does not have access to PHI, except as provided for in these Policies and Procedures and with approval from the Privacy Officer.

5. **Secure Mail Delivery**. PHI is generally not received or delivered by mail, but to the extent it is, that mail is delivered directly to Privacy Employees in a sealed envelope.

6. **Overlapping Duties**.

   a. The Privacy Employees' responsibilities include duties unrelated to the Plan. The Privacy Employees do not use PHI to make decisions related to those duties, and the Privacy Employees do not disclose PHI to the Plan Sponsor, in its role as employer, unless permitted or required by these Policies and Procedures and/or the Privacy Rule and approved by the Privacy Officer.

IMPORTANT: UNLESS SPECIFICALLY AUTHORIZED AS ABOVE OR IN WRITING BY THE PRIVACY OFFICER, ALL OTHER EMPLOYEE ACCESS TO PROTECTED HEALTH INFORMATION IS UNAUTHORIZED, STRICTLY PROHIBITED AND MAY RESULT IN SANCTIONS.

IV. USES AND DISCLOSURES THAT ARE REQUIRED OR PERMITTED BY PRIVACY RULE, OR PERMITTED BY AUTHORIZATION

POLICY: The Plan—acting through the Plan Administrator, the Privacy Employees or Business Associates—uses or discloses PHI only as required or permitted by the Privacy Rule, including those disclosures permitted by an authorization. However, the Plan permits an individual's PHI to be used or disclosed without authorization as provided for in this Policy and Policy V, and in accordance with the minimum necessary standard established in Policy VI.

A. **REQUIRED USES AND DISCLOSURES.** The Plan is required to use or disclose PHI in the following circumstances:

1. **Individual Access.** To the individual who is the subject of the PHI contained in the designated record set as long as individual complies with the following verification procedure:

   a. If the individual sends his/her request in writing (including requests by e-mail), it must state his/her name, address, and, either the last four digits of his social security number or his employee number. If the individual is requesting to inspect and/or copy his/her PHI, he/she must follow the procedures set out in this policy.

   b. If the individual orally contacts the Plan to inquire about matters related to the individual's PHI, the Plan verifies the individual's identity by requesting the last four digits of that individual's social security number and birthdate, or his/her employee number.

2. **Access by Secretary of HHS.** To the Secretary of the Department of Health and Human Services ("HHS") when the Secretary is investigating a complaint or monitoring compliance. The Plan will verify the identity of the HHS requester as set forth in Policy V.B.2.

B. DISCLOSURES TO FAMILY MEMBERS

1. **Spousal Access**. In the normal course, before an individual may have access to PHI related to his/her spouse, the spouse must sign a HIPAA-compliant authorization releasing such PHI to the individual. Before responding to a spousal request, the Plan verifies the identity of the requester and the spouse by requesting the last 4 digits of each person's social security number and birthdate, and/or the employee's employee number.

2. **Parental Access**. In the normal course, parents or guardians ("parents") are considered the personal representatives of unemancipated minors. As such, the Plan generally responds to parental inquiries about their children's treatment and health care claims and provides parents with access to the minors' PHI.

3. **Emergency Access**. If a family member or close friend inquires on behalf of an individual who is in the hospital or from whom it would be difficult to obtain an authorization, the Plan may respond to that family member or close friend's inquiries. (This type of access does not require that the individual be incapacitated or unconscious.) However, before responding:

    a. The Privacy Officer or HIPAA Contact Person must act in accordance with Policy V. A. and approve the disclosure.

    b. The identity of the family member or close friend and the individual must be verified.

    c. The PHI provided must be the minimum necessary for the family member or close friend to ensure the individual receives the medical care he/she needs.

    d. If the Privacy Officer or HIPAA Contact Person is uncomfortable with the request, the Privacy Officer or HIPAA Contact Person may require an authorization.

    e. An example of this type of disclosure would be if an adult child called from the hospital to inquire about his parent's unpaid claims or eligibility for certain benefits.

4. **Communications with Individuals Regarding Payment.** Notwithstanding paragraphs (1), (2) and (3) above, the Plan may communicate directly with participants concerning payment (as defined below) issues related to claims of dependents, including spouses and adult children. For example, explanations of benefits ("EOBs") and other documents related to payment may be addressed to the participant or the dependent who received the health benefit. All non-payment correspondence related to health benefits, however, should be addressed to the individual who received the health benefit regardless of that individual's age or dependent status.

C. **USES AND DISCLOSURES PERMITTED FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS.** The Plan uses or discloses PHI for purposes of treatment, payment or health care operations. No individual authorization is required for these uses or disclosures.

1. **Treatment**. The Plan may use or disclose PHI for treatment purposes to assist any health care provider in that provider's treatment activities or to coordinate or manage with a health care provider to provide treatment for an individual.

2. **Payment**. For payment purposes, the Plan may use or disclose PHI to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or to obtain or provide reimbursement for the provision of health care. These payment activities must relate to an individual, and include, but are not limited to:

   a. determinations of eligibility or coverage, including the coordination of benefits and determination of cost sharing amounts, adjudication or subrogation of health benefit claims;

   b. risk adjustment based on enrollee health status and demographic characteristics;

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

   d. review of health care services with respect to medical necessity, coverage under the Plan, appropriateness of care, or justification of charges;

   e. utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

   f. disclosure to consumer reporting agencies of any of the following PHI relating to the collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the Plan.

3. **Health Care Operations**. The Plan uses or discloses PHI for the following activities, which relate to the Plan's business operations and generally involve the PHI of more than one individual:

   a. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health insurance, including stop-loss insurance and excess of loss insurance. However, if such health insurance or health benefits coverage is not placed with the Plan, then the Plan will not use or disclose that PHI for any other purpose unless required by law.

   b. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

c. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

d. Business management and general administrative activities of the Plan, including, but not limited to:

(i) management activities related to implementing and complying with the Privacy Rule;

(ii) customer service, including the provision of data analyses for policy holders or other customers, provided that PHI is not disclosed to the policy holder or other customers;

(iii) resolution of internal grievances; and

(iv) due diligence in connection with the sale or transfer of assets to a potential successor.

D. **USE AND DISCLOSURE OF PHI PERMITTED PURSUANT TO A VALID AUTHORIZATION.** The Plan will use or disclose PHI consistent with the terms of any valid authorization executed by the individual.

1. **Requirement.** The Plan will only use or disclose PHI to third parties for purposes other than treatment, payment, or health care operations, or reasons other than those specified in the Privacy Rule as not requiring authorization or otherwise required by law, upon receipt of a valid, written authorization. Once a valid authorization is received, the Plan will only use and disclose information consistent with the terms of the authorization. However, the standard authorization received by the Plan will state that once disclosed, the PHI may no longer be protected, and that the information may be further disclosed by the recipient without any additional authorization from the individual.

2. **Authorization Forms.** Authorization Forms, which are available from the Privacy Officer or HIPAA Contact Person, must contain the following information:

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

b. The name or other specific identification of the person(s) or class of person(s) authorized to use or disclose the information from the Plan.

c. The name or other specific identification of the person(s) or class of person(s) to whom the Plan may use or disclose the information.

d. A description of each purpose of the requested use or disclosure. If the individual initiates the authorization, the purpose may be described as "At the request of the individual."

e. A statement that the individual may revoke the authorization in writing, and how to do so.

f. A statement that the Plan shall not condition treatment, payment, enrollment or eligibility for benefits on the authorization (unless one of the conditional exceptions applies, in which case that exception must be explained).

g. The potential for information disclosed under the authorization to be subject to redisclosure by the recipient, and the fact that once the information is disclosed (to a non-covered entity) it is no longer protected by HIPAA.

h. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

i. Signature of the individual who is the subject of the health information and the date. If the authorization is executed by a personal representative, it must include a description of the representative's authority to act for the individual.

3. **Procedure To Obtain or Revoke Authorizations.**

a. **For an Individual to Obtain Authorization**. For certain PHI to be used or disclosed at an individual's request, the individual must contact the Privacy Officer and/or the HIPAA Contact Person, orally or in writing, to request an Authorization Form. In response, the Privacy Officer or HIPAA Contact Person will forward an Authorization Form to be filled out and signed by the individual. Thereafter, the Privacy Officer or HIPAA Contact Person will ensure that the correct PHI is used or disclosed in accordance with the authorization.

b. **For the Plan to Obtain Individual's Authorization.** If the Plan seeks to have an individual sign an authorization, the Plan will send the individual a written request stating the proposed reason for the use or disclosure of the information and enclose an appropriate authorization form to be completed and signed by the individual. The Plan will provide the individual with a copy of his/her executed authorization. Thereafter, the Privacy Officer and/or the HIPAA Contact Person will ensure that the correct PHI is used or disclosed in accordance with the authorization.

c. **Authorization Revocation**. An individual may revoke, in writing, his/her signed authorization at any time, except to the extent that the Plan has taken action in reliance on the authorization prior to revocation. If there is a question as to whether the Plan has relied on the authorization so that revocation may not be possible, the Privacy Officer must decide whether revocation is proper.

d. **Conditions**. The Plan does not condition the provision of an individual's treatment, payment, or enrollment in the health plan, or eligibility of benefits on obtaining an authorization to disclose PHI.

e. **Documentation.** All signed authorizations and related documentation will be retained for six (6) years in accordance with the Trust's document retention policy.

V. USES AND DISCLOSURES PERMITTED FOR REASONS OTHER THAN TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS AND WITHOUT INDIVIDUAL AUTHORIZATION

POLICY: In the following limited instances, which are in addition to Treatment, Payment and Health Care Operations, the Plan is permitted to use or disclose PHI without an individual's authorization.

A. USES AND DISCLOSURES THAT REQUIRE AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT

1. **Disclosures to Designated Individuals.** The Privacy Officer, without written authorization from the individual, may authorize the use or disclosure of PHI to any person identified by the individual, such as a family member or close friend, of any PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's care as long as the following conditions are met:

    a. If the individual is present for, or otherwise available prior to, this type of use or disclosure and has the capacity to make health care decisions, the Privacy Officer will authorize the use or disclosure of the PHI if the Plan: (1) obtains the individual's agreement; (2) provides the individual with the opportunity to object and the individual does not do so; or (3) the Privacy Officer reasonably infers from the circumstances and based on professional judgment, that the individual does not object.

    b. If the individual is not present for, or it is not possible to give the individual the opportunity to agree to the use or disclosure because of incapacity or an emergency, the Privacy Officer will determine, based on professional judgment, whether the use or disclosure is in the best interest of the individual. If use or disclosure is made, only the PHI that is directly relevant to the third person's involvement with individual's health care will be used or disclosed.

2. **Disclosures for Notification Purposes**. The Privacy Officer, without written authorization from the individual, may authorize the use or disclosure of PHI to notify, or assist in notifying (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the individual's care, of the individual's location, general condition or death. The Privacy Officer also may authorize the use or disclosure of PHI to a public or private entity that is authorized by law or by its charter to assist in disaster relief, for the purpose of coordinating with such entities to notify (including identifying or locating) relatives or those close to the individual, of the individual's location, general condition or death. The requirements specified above in V.A.1 are applicable unless the Privacy Officer determines those requirements interfere with an efficient emergency response.

B. USES AND DISCLOSURES FOR WHICH AN INDIVIDUAL'S AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT ARE NOT REQUIRED.

1. **Uses and Disclosures**. In the following circumstances, the Privacy Officer may authorize the use or disclosure of PHI without the individual's written authorization, and without giving the individual the right to agree or object.

   a. To the appropriate governmental or judicial authority as required by law in situations of abuse, neglect or domestic violence (§164.512(c)); in the course of any judicial or administrative proceeding (§164.512(e)); for law enforcement purposes to a law enforcement official as required by law (§164.512(f)). The Plan will only make such disclosures to the extent they are required by law and the use or disclosure complies with and is limited to the relevant requirements of the law. Further, in making such disclosures, the Plan will comply with the additional requirements in §§164.512(c), (e), or (f), as applicable.

   b. To the appropriate public health authority that is authorized by law to collect or receive PHI for the purpose of preventing or controlling disease (including notifying infected individuals when authorized by law), injury or disability; or to receive reports of child abuse or neglect (§164.512(b)(i)-(ii), (iv)). The Plan will comply with the additional requirements in §164.512(b)(i)-(ii), (iv).

   c. To persons or entities subject to the jurisdiction of the Food and Drug Administration ("FDA") to meet the reporting requirements of the FDA, such as submitting adverse event reports, tracking products for recalls, and conducting post-marketing surveillance to track compliance (§164.512(b)(iii)). The Plan will comply with the additional requirements in §164.512(b)(iii).

   d. To an employer to comply with OSHA requirements related to medical surveillance and work-related injuries, and to persons as authorized by workers' compensation laws (§164.512(b)(v), §164.512(l)). The Plan will comply with the additional requirements in §164.512(b)(v), §164.512(l).

   e. To health oversight agencies for oversight activities authorized by law, e.g., fraud and abuse audits, investigations, and inspections; licensure or disciplinary actions; and civil, administrative or criminal proceedings (§164.512(d)). The Plan will comply with the additional requirements in §164.512(d).

   f. To coroners and medical examiners, and funeral directors, the PHI which is necessary to permit those persons to carry out their duties consistent with applicable law (§164.512(g)). The Plan will comply with the additional requirements in §164.512(g).

   g. To organ procurement organizations for donation purposes (§164.512(h)). The Plan will comply with the additional requirements in §164.512(h).

   h. For research purposes, provided that an Institutional Review Board or privacy board (as described in the Privacy Rule) approves the waiver of individual authorization and the additional conditions in (§164.512(i)) are met. The Plan will comply with the additional requirements in §164.512(i)).

   i. To appropriate persons and consistent with applicable laws and standards of ethical conduct, when the Privacy Officer believes, in good faith, that it is

necessary to use or disclose the PHI to prevent or lessen a serious and imminent threat to the health and safety of a person or the public, or to assist law enforcement in identifying or apprehending an individual (§164.512(j)). The Plan will comply with the additional requirements in §164.512(j)).

j. To military and veterans' authorities, national security and intelligence sources, protective services for the President, correctional institutions and other custodial law enforcement, and Department of State for the purposes detailed in §164.512(k)(1)-(5). The Plan will comply with the additional requirements in §164.512(k)(1)-(5)).

2. **Verification Procedures**. Before making any such disclosures, the Privacy Officer will verify the identity of the person requesting the PHI and the authority that person has to have access to the requested PHI.

a. In the normal course, the Privacy Officer will obtain the requisite verification by requiring the requester to send their request in writing on official stationery. The Privacy Officer may also require the requester to provide any other documentation that he/she deems necessary, using professional judgment, to verify the authenticity of the requester.

b. If the request is made to the Privacy Officer in person, the Privacy Officer will require the requester to present sufficient official identification, such as a badge or official credential, to verify the requester's identity and authority.

c. If the request is made pursuant to legal process, such as a subpoena, warrant or court order, the Privacy Officer may rely on the veracity of that request.

d. If the Privacy Officer determines, using professional judgment, that there is an emergency situation that does not allow for a written exchange, the Privacy Officer may verify the requester's identity by calling the requester back. If this occurs, the Privacy Officer must document the exchange and the nature of the emergency and maintain the documentation in accordance with Policy XXII.

C. **DISCLOSURES TO BUSINESS ASSOCIATES.** The Plan may disclose PHI to Business Associates consistent with this policy.

D. **DISCLOSURES TO GROUP HEALTH PLAN SPONSOR OF PHI HELD BY GROUP HEALTH PLAN**

1. The Plan discloses PHI held by it as Plan Sponsor for plan administration functions, such as claims processing, performing quality assurance functions, and auditing and monitoring the Plan.

a. These disclosures are made in accordance with the amended Plan documents, which incorporate specific protective provisions required by the Privacy Rule.

b. These disclosures are only made to the Privacy Employees identified in Policy III.A (Limited Employee Access) and in the amended Plan documents.

c. PHI disclosed for these purposes may include, but is not limited to, vendor reports, information regarding individuals' claims questions, outside consultant reports regarding data analyses and claims adjudication, and extraordinary claims information.

2. The Plan may disclose "summary health information" to the Plan Sponsor for the purpose of (a) obtaining premium bids from health insurers to provide coverage under the Plan, or (b) to modify, amend or terminate the Plan. Summary health information is health information that summarizes claims history, claims expenses and the type of claims experienced by Plan participants and their dependents and is de-identified except that it may be aggregated to include 5-digit zip codes.

3. The Plan may disclose to the Plan Sponsor who is enrolled and disenrolled in the Plan.

E. **DISCLOSURES BY WHISTLEBLOWERS AND WORKFORCE MEMBER CRIME VICTIMS.** A Privacy Employee with access to PHI will not be disciplined if he/she discloses PHI to a health oversight agency or to an attorney only if he/she believes, in good faith, that the Plan has engaged in unlawful conduct. If that Employee believes that he/she should disclose PHI about a suspected perpetrator of a criminal act to a law enforcement official, if feasible, that Employee should first discuss that disclosure with the Privacy Officer.

VI. THE MINIMUM NECESSARY REQUIREMENT

POLICY: The Plan applies the minimum necessary standard whenever it uses or discloses PHI to a third party, or requests PHI from another covered entity. This means that the Plan makes reasonable efforts to limit the use or disclosure, or request of PHI to the minimum necessary to accomplish its intended purposes, which generally means the Plan will limit its uses and disclosures of, and requests for, PHI to Limited Data Set information or any other, applicable standard set by the Secretary.

A. **APPLICABILITY OF THE MINIMUM NECESSARY REQUIREMENT.** The Plan will apply the minimum necessary standard to all uses and disclosures of PHI, except as follows:

1. Disclosures to or requests by a health care provider for treatment purposes;

2. Permitted and required disclosures to the individual who is the subject of the information;

3. Uses or disclosures pursuant to a valid authorization executed by the individual;

4. Disclosures made to the Secretary of HHS in accordance with the Privacy Rule; or

5. Uses and disclosures required by law as described above in Policy V.B.1.a and uses and disclosures that are required for compliance with the HIPAA privacy regulations.

B. **IDENTIFICATION OF EMPLOYEES.**

1. **Identified Employees.** The Privacy Employees who need access to PHI are identified above in Policy II (Personnel Designations) and Policy III.A (Limited Employee Access). No other Plan Sponsor employees may have access to PHI unless specifically authorized by the Privacy Officer.

2. **Restrictions on Employee Access**. The Privacy Employees who need access to PHI only have access to the PHI necessary for their job duties, as expressly limited in Policy III. Privacy Employees may not have access to PHI beyond that specified in Policy III unless specifically authorized by the Privacy Officer.

C. **MINIMUM NECESSARY REQUIREMENT APPLIED TO USES AND DISCLOSURES OF PHI.**

1. **Limited Data Set**. For the Routine and Non-Routine Uses and Disclosures described herein, the Plan will limit its uses and disclosures of and requests for PHI to Limited Data Set information, unless the Privacy Officer makes a determination that additional identifiable PHI is necessary to achieve the purpose of the use, disclosure or request in accordance with the minimum necessary standard.

   a. Limited Data Set information is information that excludes the following direct identifiers of the individual or the relatives, employers or household members of the individual:

      (i) Names;

      (ii) Postal address information (except town, city, state and zip code may be used or disclosed);

      (iii) Telephone and Fax Numbers;

      (iv) Social Security Numbers, Medical Record Numbers, Health Plan Beneficiary Numbers, Account Numbers or Certificate/License Numbers;

      (v) Vehicle Identifiers and Serial Numbers, including license plate numbers;

      (vi) Device Identifiers and Serial Numbers;

      (vii) Email Addresses, Web Universal Resource Locators ("URLs") and Internet Protocol ("IP") Address Numbers;

      (viii) Biometric Identifiers (including finger and voice prints), and Full-Face Photographic Images and any Comparable Images.

   b. Limited Data Set information may include an Individual's town, city, state and zip code, and all elements of dates related to the Individual (including birth date, admission date, discharge date and death date).

   c. If and to the extent that the Secretary issues guidance that no longer defines the Limited Data Set as the default minimum necessary information, the Plan will follow the applicable guidelines issued by the Secretary.

2. **Routine Uses or Disclosures; Protocol.** The Plan makes the following routine uses or disclosures of PHI, and the accompanying protocols ensure that the minimum necessary requirement is met. The Privacy Employees who have access to the requested PHI will use and disclose this PHI in accordance with the below defined protocols.

   a. Use/Disclosure: When an individual requests assistance with a claims issue, the Privacy Employees assisting with such request may disclose necessary PHI to the

claims offices of the relevant third-party administrator(s) ("TPAs") or health care providers.

Protocol:

(i) As described in Policy III.A, the Privacy Employees may provide individuals with assistance related to claims.

(ii) This type of use or disclosure only occurs when an individual expressly requests, orally or in writing, that the Privacy Employees, acting for the Plan, intervene to assist with a claims issue. The Privacy Employee documents the permission granted by an individual, but an authorization is not required.

(iii) The PHI that is used or disclosed is limited to the PHI that is relevant to the claims issue, and the PHI is only disclosed to the third-party administrator(s) relevant to processing the claim and/or the health care providers relevant to the claim.

(iv) Because of the individual nature of these inquiries, the Privacy Officer has determined that identifiable information in addition to the Limited Data Set information is necessary to assist individuals with a claims issue. But any use or disclosure of PHI is limited as described in (iii) above.

(v) If an inquiry is made by an individual on behalf of another adult individual, the individual who is the subject of the PHI generally is required to sign an authorization permitting the Plan to disclose PHI to the individual making the inquiry. But, in emergency circumstances, an authorization may not be needed. *See* Policy IV.B.

(vi) The Privacy Employee who assists the individual documents the assistance and maintains any authorizations or other documentation reflecting permission to act on the individual's behalf for six years in accordance with Policy XXII. However, once the issue is resolved the Privacy Employee either destroys the underlying claims information through shredding, or if requested by the individual, the Privacy Employee may return to the individual the original PHI that the individual provided to the Privacy Employee

(vii) The Privacy Employee who assists the individual does not disclose the individual's PHI to any other Privacy Employee except to the extent necessary to perform his/her job responsibilities. This Privacy Employee does not disclose the individual's PHI to any other Plan Sponsor employee or third party except as directed or approved by the Privacy Officer.

b. Use/Disclosure: If a claims issue presented by an individual presents unique circumstances, the Privacy Employees, for the Plan, may seek a Business Associate's assistance.

Protocol:

(i) Before sharing PHI with an outside consultant, the Plan enters into a Business Associate Agreement with the outside consultant, and only discloses PHI with the outside consultant in accordance with that Agreement.

(ii) Generally, the individual does not need to sign an authorization because this type of disclosure is for payment or health care operations purposes. If appropriate, the Plan informs the individual that it is seeking assistance from an outside consultant.

(iii) The PHI that is disclosed to the outside consultant is limited to the PHI that is relevant to the claims issue and necessary for the disposition of the issue.

(iv) Because of the individual nature of these inquiries, the Privacy Officer has determined that identifiable information in addition to the Limited Data Set information is necessary to assist individuals with a claims issue. But the use or disclosure is limited as described in (iii) above.

(v) The Privacy Employee who seeks the outside consultant's assistance maintains any authorizations or other documentation related to permission to act on the individual's behalf for six years in accordance with Policy XXII. However, once the issue is resolved, the Privacy Employee either destroys the underlying claims information through shredding or, if requested by the individual, the Privacy Employee may return to the individual the original the PHI that the individual provided to him/her.

(vi) The Privacy Employee who seeks an outside consultant's assistance does not disclose the PHI at issue with any other Privacy Employee except to the extent necessary to perform his/her job responsibilities. This Privacy Employee does not disclose that PHI to any other Plan Sponsor employee or third party, except as directed or approved by the Privacy Officer.

c. Use/Disclosure: The Privacy Employees acting for the Plan use or disclose PHI for invoicing, reconciliation and monitoring purposes.

Protocol:

(i) The Privacy Employees may use PHI for invoicing, reconciliation and monitoring purposes.

(ii) If the invoices contain PHI, the Privacy Employee paying the vendor or reconciling/monitoring the accounts reviews the PHI only to the extent necessary to confirm the vendor payment and/or reconcile/monitor the Plan's accounts.

(iii) Because processing invoices and/or reconciliation or monitoring of accounts requires the use and disclosure of identifiable information, the Privacy Officer has determined that identifiable information in addition to the Limited Data Set information is necessary. But the use or disclosure is limited as described in (ii) above.

(iv) The Privacy Employees who pay the vendor invoices or reconcile/monitor the Plan's accounts disclose PHI learned from the vendor invoices to other Privacy Employees and vendors only to the extent necessary to perform their job functions. The Privacy Employee does not share this PHI with any other Plan Sponsor employee or third party except as directed or approved by the Privacy Officer.

d. Use/Disclosure: The Plan discloses PHI, such as name, social security number, amount of claims paid and diagnosis code, to outside consultants for health care operations purposes, such as data analysis, actuarial studies, track trends, auditing and monitoring.

Protocol:

(i) Before disclosing PHI to an outside consultant, the Plan enters a Business Associate Agreement with that outside consultant, and only discloses PHI to that consultant in accordance with that Agreement.

(ii) The Privacy Officer manages the disclosure of PHI to outside consultants for health care operations purposes. Therefore, the Privacy Employees may only disclose PHI to outside consultants at the direction of the Privacy Officer.

(iii) To the extent possible, the Plan only discloses the Limited Data Set Information to the consultants. As there may be instances in which identifiable PHI beyond Limited Data Set information will need to be disclosed to the consultants for health care operations purposes, the Privacy Officer will determine, on a case-by-case basis, whether and the extent to which information beyond the Limited Data Set information is required. In any case, the Privacy Officer ensures that the outside consultants are only provided with the minimum amount of PHI necessary for them to perform their functions.

e. Use/Disclosure. The Plan provides computerized eligibility feeds to certain TPAs. Those feeds contain enrollment information maintained by the Plan Sponsor, and therefore, do not contain PHI to which the minimum necessary standard applies.

3. **Non-Routine Uses/Disclosures.** For each use or disclosure not specified above, the following criteria must be applied to ensure that the minimum necessary requirement has been met.

a. Criteria:

(i) The Privacy Employee who has access to the requested PHI in the normal course handles the request for the non-routine disclosure of that PHI. Before disclosing that PHI, the Privacy Employee: verifies the identity of the requesting party; determines whether an individual authorization is required to release the PHI and provides the necessary form to the individual; determines whether information beyond Limited Data Set information may be required; and verifies that the disclosure is limited in scope and permissible under these Policies and Procedures.

(ii) The Privacy Employee submits the request, his/her recommended response to the request, any required authorization, and verification information to the Privacy Officer for his/her review. If the Privacy Employee determines that more than Limited Data Set information is necessary, he/she identifies what additional information is necessary and why. The Privacy Officer determines whether the use, disclosure or request for information is warranted, approves the type and amount of PHI to be disclosed, and documents his/her determination.

(iii) The Privacy Employee documents such disclosures of PHI, and maintains the documentation required by the Privacy Rule for a period of six years from the date of the disclosure in accordance with Policy XXII.

(iv) The Legal Department Employees, when acting on behalf of the Plan, may use their discretion to make non-routine uses or disclosures. However, to the extent possible, they inform the Privacy Officer of any such uses or disclosures. And, if the Legal Department Employees determine that PHI beyond Limited Data Set information is necessary, they document that determination.

b. Review: The Privacy Officer reviews all requests for non-routine disclosures prepared by Privacy Employees on an individual basis to make sure that the response discloses only the minimum necessary information.

4. **Reliance.** The compiling Privacy Employees, as well as the Privacy Officer, may rely on the judgment of the requesting party in determining the minimum amount of information to be disclosed if:

a. the request for PHI is made by another covered entity; or

b. the request for PHI is made by a public official, and the official represents that the information requested is the minimum necessary for the stated purpose.

5. **Resolving Disputes.** While using or disclosing PHI, the Privacy Officer is responsible for negotiating with the requesting party about the amount of PHI that needs to be disclosed to comply with the minimum necessary requirement. The Privacy Officer always seeks to limit the disclosure to the extent possible without impeding on the health care delivery process. If the parties cannot agree on the amount of information that is the minimum necessary, the Privacy Officer makes the final determination. In resolving such

disputes, the Privacy Officer limits the disclosure to the Limited Data Set information unless the requesting party provides a written explanation as to why additional identifiable information is necessary, and the Privacy Officer agrees with that explanation.

D. **REQUESTS FOR PHI AND THE MINIMUM NECESSARY REQUIREMENT.** Because a covered entity to whom a request is made may rely on another covered entity's minimum necessary determination, all requests for PHI initiated by the Plan seek only the minimum necessary to accomplish the purpose for which the request is made.

1. **Routine Requests; Protocol.** The following are the routine requests that the Plan makes, and the accompanying protocol ensures that the minimum necessary requirement is met. The Privacy Employees who have access to the requested information in the normal course will be responsible for making these routine requests.

a. Request: The Plan requests information from its vendors, health care providers and other third parties when assisting individuals with claims inquiries.

Protocol:

(i) The Privacy Employees only make such requests if the individual provides permission to pursue the claims inquiry.

(ii) The Privacy Employees request only the minimum amount of PHI required to accomplish the purpose of the request.

(iii) Because of the individual nature of these inquiries, the Privacy Officer has determined it is necessary to request identifiable information in addition to the Limited Data Set information to assist individuals with a claims issue. But the use or disclosure is limited as described in (ii) above.

(iv) The Privacy Employees do not share that PHI with other Plan Sponsor employees or third parties, except as directed or approved by the Privacy Officer, or as required by law and approved by the Privacy Officer.

b. Request: From time to time, the Plan requests that its TPAs or outside consultants provide information for payment and health care operations purposes.

(i) The Privacy Employees ensure that they request only the minimum amount of information necessary to accomplish the purpose of the request.

(ii) To the extent these inquiries involve the payment of specific claims, the Privacy Officer has determined it is necessary to request identifiable information in addition to the Limited Data Set information to assist individuals with a claims issue. But the use or disclosure is limited as described in (i) above.

(iii) The Privacy Officer acknowledges that, in some instances, health care operations purposes (such as audits or claims analysis) require the use or

disclosure of identifiable PHI in addition to the Limited Data Set information. The Privacy Officer will determine, on a case-by-case basis, when identifiable PHI beyond the Limited Data Set information is necessary for such purposes.

(iv) The Privacy Employees with access to this PHI do not share that PHI with other Plan Sponsor employees or third parties, except as directed or approved by the Privacy Officer.

2. **All other requests.** All other requests for PHI are formulated by Privacy Employees who need the requested information to perform their job responsibilities. Each request is reviewed and approved by the Privacy Officer to ensure that the request seeks the minimum amount of PHI reasonably necessary to accomplish the purpose of the request.

E. **LIMITATION REGARDING USING, DISCLOSING OR REQUESTING ENTIRE MEDICAL RECORD.** For all uses, disclosures, or requests to which the minimum necessary requirements apply, the Plan will not use, disclose or request an entire medical record, except when the entire medical record is specifically justified, and Plan has documented the specific justification.

VII. NOTIFICATION OF BREACH

POLICY: To notify individuals, the Secretary of Health and Human Services (the "Secretary") and the media of breaches of Unsecured PHI in accordance with the Notification of Breach Rule, 45 C.F.R Part 164, subpart D.

A. **MAINTENANCE OF UNSECURED PHI**. The Plan uses reasonable efforts to "secure PHI" to maintain as little Unsecured PHI as possible.

1. "Unsecured PHI" is PHI that is not secured through the use of a technology or methodology specified by the Secretary. The core technologies and methodologies identified thus far by the Secretary are:

a. Encryption for electronic PHI "in motion," "at rest" and "in use." The Plan's encryption technologies, if any, are described in its Security Policies and Procedures.

b. Destruction of PHI:

(i) Hardcopy PHI, whether documents, discs, tapes or any other version of hardcopy PHI, is destroyed by shredding the information when it is no longer needed for the purpose for which it was created, maintained, used or disclosed, or at the end of the requisite document retention period, in accordance with the Trust's document retention policy.

(ii) Electronic PHI should be destroyed in accordance with applicable guidance issued by the Secretary. Whether and to the extent that the Plan Sponsor is complying with the Secretary's applicable guidance is described in the Plan's Security Policies and

Procedures.

c. The Plan recognizes that the Secretary will be issuing guidance related to the acceptable technologies and methodologies on a periodic basis. These Policies and Procedures and the Security Policies and Procedures will be updated to reflect that guidance as is necessary and appropriate.

B. **BREACH OF UNSECURED PHI**. A Breach that requires notification occurs when there is an unauthorized acquisition, access, use or disclosure of Unsecured PHI that compromises the privacy or security of that information.

1. **Three-Step Analysis**. To determine if a Breach that requires notification has occurred, the Privacy Officer conducts the following Three-Step Analysis:

- **Step 1**: Has there been an impermissible use or disclosure of Unsecured PHI that violates these Policies and Procedures and/or the Privacy Rule? If not, there is no Breach. If so, the analysis continues to Step 2.

- **Step 2**: An impermissible use or disclosure of Unsecured PHI is presumed to be a Breach, unless there is a low probability that the Unsecured PHI was compromised. To determine whether there is a low probability that the Unsecured PHI was compromised, the Privacy Officer conducts a fact-specific risk assessment, which must consider the following factors:

  a. What is the nature and extent of the Unsecured PHI that was used or disclosed? Consider the type of PHI involved, including the types of identifiers disclosed and the likelihood of re-identification

  b. Who used or received the Unsecured PHI? Another covered entity or business associate? The Plan Sponsor in its capacity as employer? Another employee who is not authorized to access PHI? A member of the public?

  c. Was the Unsecured PHI actually acquired or viewed? Is it possible to verify that the Unsecured PHI was not actually accessed, opened, copied or compromised?

  d. To what extent has the risk to the Unsecured PHI been mitigated? Was the Unsecured PHI returned? Has the unauthorized recipient provided satisfactory assurances that the information has been destroyed?

  If it is determined that there is a low probability that the Unsecured PHI was compromised, notification is not required. Otherwise, the Privacy Officer continues the analysis with Step 3.

- **Step 3**: Does the Breach fall within one of the following three exceptions to the definition of a Breach? If so, there is no Breach.

  a. Was the Breach an unintentional access, use or disclosure of Unsecured PHI by a Privacy Employee or a Business Associate's workforce member that was an action taken in good faith and within that person's scope of authority, and which did not result in any further, impermissible use or disclosure of the Unsecured PHI?

  b. Was the Breach an inadvertent disclosure by and between Privacy Employees and/or a Business Associate's workforce members authorized to access PHI, and was the Unsecured PHI not further used or disclosed in an impermissible manner?

c. Is there a good-faith belief by the Plan and/or its Business Associate that the unauthorized person to whom the Unsecured PHI was disclosed would not reasonably be able to retain the Unsecured PHI?

1. If the Breach does not fall within an exception, notification is required.

2. The Privacy Officer shall prepare and maintain documentation regarding the Three-Step Analysis described herein.

C. **DISCOVERY OF BREACH**. The Breach is "Discovered" on the first day the Plan knows of it or, by exercising reasonable diligence, should have known of it. A Plan Sponsor employee's or agent's knowledge of the Breach is imputed to the Plan, except that such knowledge held by the individual who committed the Breach is not attributable to the Plan.

D. **NOTIFICATION OF BREACH**. When a Breach of Unsecured PHI is Discovered, the Plan provides notice as described herein.

1. **To the Impacted Individuals**. Upon the Discovery of a Breach, the Plan or its Business Associate provides notice to each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the Breach.

a. **Timing**. This notice is provided without unreasonable delay, and in no case later than 60 days after the Discovery of the Breach.

b. **Content**. The notice to the impacted individuals will be in plain language and contain the following information:

(i) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach (if such dates are known);

(ii) A description of the types of Unsecured PHI involved in the Breach (such as name, social security number, date of birth, home address, account number, diagnosis, or other identifiable information);

(iii) Any steps the impacted individuals should take to protect themselves from potential harm resulting from the Breach;

(iv) A brief description of what the Plan (or its Business Associates) is doing to investigate the Breach, to mitigate any harm to impacted individuals and to protect against further breaches; and

(v) Contact information that impacted individuals can use to ask questions or learn additional information. The contact information will include a toll-free number, email address, website or postal address, or any combination thereof.

c. **Methods of Notice**.

(i) Written notice will be provided to impacted individuals via first-class mail to their last known address, except that electronic notice may be provided if an impacted individual agrees to such notice and such agreement has not been withdrawn.

(ii) If the Plan knows that the impacted individual is deceased and has the address of that individual's next of kin or personal representative, written notice will be sent to that person via first-class mail.

(iii) If the Plan has insufficient or out-of-date contact information, it will provide substitute notice as follows:

(a) If fewer than 10 individuals are involved, notice may be provided by an alternative form of written notice, telephone or any other effective means;

(b) If 10 or more individuals are involved, the substitute notice will be (1) in the form of a conspicuous posting for a period of 90 days or longer on the Plan's website, or (2) conspicuous notice in major print or broadcast media in the geographic areas where the impacted individuals likely reside. In either case, the substitute notice will include a toll-free number that remains active for at least 90 days through which an Individual can learn if his/her Unsecured PHI may have been included in the Breach.

(c) If the Plan determines that there is an urgency associated with the notice because of possible, imminent misuse of the Unsecured PHI, the Plan may provide additional information to individuals by telephone or alternative written communications. However, these notified individuals will still receive the written notice described in c(i) above.

(d) With regard to this notice, notification may be provided in one or more mailings as information becomes available.

2. **To the Media**. If there is a Breach of Unsecured PHI that involves more than 500 residents of a state or jurisdiction, the Plan or its Business Associate will notify the prominent media outlets serving the state or jurisdiction.

a. **Timing**. Notice to the media generally will be provided at the same time it is sent to the impacted individuals. In sum, it will be provided to the media without unreasonable delay and in no case later than 60 calendar days after the Discovery of the Breach.

b. **Content**. The notice shall contain the same information as the notice to impacted individuals, which such information is detailed above in subsection D.1.b.

c. Notice also may be provided to the media if there is insufficient address information as described in subsection D.1.c(iii)(b).

3. **To the Secretary**. If there is a Breach of Unsecured PHI, the Plan will provide notice to the Secretary as follows:

a. **Breach Involving 500 or More Individuals**: In such case, the Plan will provide notice to the Secretary at the same time as it provides notice to the impacted individuals. The Plan will provide electronic notice to the Secretary in the manner specified on the HHS website. The Secretary may thereafter post the Plan's name on its website.

b. **Breach Involving Less Than 500 Individuals**. In such a case, the Plan will report the Breach to the Secretary at the same time as it notifies impacted individuals, or the Plan will provide an annual log to the Secretary, which will be provided in the manner specified on the HHS website and within 60 days after the end of each calendar year. To meet this requirement, the Plan will maintain an annual log that has the information necessary to meet the Secretary's reporting requirements, as specified on the HHS website.

c. The website address that contains the Secretary's notice specifications is: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

4. **Notification by Business Associate**.

a. **Delegation**. Through its Business Associate Agreements or other written agreements, the Plan may contract with its Business Associates to have the Business Associates provide notice to the impacted individuals, media and/or the Secretary as described above in 1–3. If the Business Associate accepts this delegation, it also may be responsible for conducting the Three-Step Analysis set forth in subsection B above to determine if there has been a Breach.

b. **Notification to the Plan**. To the extent that the Plan and a Business Associate do not agree to an alternative notification process through written agreement, the Business Associate will provide the Plan with notice of a Breach of Unsecured PHI as follows:

(i) **Timing**. Notice to the Covered Entity should be provided without unreasonable delay and in no case later than 30 calendar days after Discovery of the Breach. Business Associate "discovers" the Breach on the first day it knows of the Breach or, by exercising reasonable diligence, should have known of it. Knowledge of the Breach by Business Associate's employees or

agents (except for the breaching person) is imputed to the Business Associate.

(ii) **Content**. The Business Associate will notify the Plan of:

(a) The identity of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during the Breach; and

(b) Any other available information that the Plan needs to provide impacted individuals with the content described above in D.1.b to the extent available. If the Business Associate is not able to provide all necessary information within the time period to provide notice to impacted individuals, it will promptly supplement with relevant information as it becomes available.

5. **Law Enforcement Delay**. If and to the extent that a law enforcement official informs the Plan or its Business Associate that a notification, notice or posting required above would impede a criminal investigation or cause damage to national security, the Plan or its Business Associate will:

a. If the notice from Law Enforcement is in writing and specifies the time for which a delay is required, delay the notification, notice or posting for the time period specified by Law Enforcement's written communication; or

b. If the notice from Law Enforcement is oral, document the statement, including the identity of the official making the request, and delay the notification, notice or posting temporarily, but not longer than 30 days from the date of the oral statement. If the oral statement is followed up with a written statement, then (a) above will govern.

6. **Training**. In accordance with Policy XVIII, the Privacy Employees and other appropriate Plan Sponsor employees will be trained on discovering Breaches, mitigating any related harm and the necessary notice requirements for impacted individuals, the media and the Secretary.

VIII. DE-IDENTIFICATION POLICY

POLICY: The Plan may use or disclose de-identified information, which is health information that does not identify an individual and is not PHI, without obtaining the individual's authorization. If the Plan re-identifies information, it becomes PHI that is treated in accordance with the Privacy Rule and these Policies and Procedures.

A. **CREATION OF DE-IDENTIFIED INFORMATION.** The Plan may create, or direct a Business Associate to create, de-identified information pursuant to the following guidelines.

1. **Expert Method.** The Plan de-identifies information by designating an expert, who has the appropriate knowledge of and experience with statistical and scientific principles and methods for rendering information not individually identifiable and applies such principles and methods to:

   a. Determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information; and

   b. Document the methods and results of the analysis that justify such determination; or

2. **Removal of Identifiers Methods.** The Plan de-identifies PHI by removing the following individual identifiers related to individuals, their relatives, household members and employers, and ensure, to the extent practicable, that the de-identified information cannot be used alone or in combination with other information to identify the individual who is a subject of the information.

   a. Names;

   b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, that complies with the specifics in §164.514(b)(2)(i)(B);

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

   d. Telephone numbers, fax numbers, and e-mail addresses;

   e. Social security numbers, medical record numbers, health plan beneficiary numbers, and account numbers;

   f. Certificate/license numbers, vehicle identifiers and serial numbers; including license plate numbers, and device identifiers and serial numbers;

   g. Web Universal Resource Locators (URLs), and Internet Protocol (IP) address numbers;

h. Biometric identifiers, including finger and voice prints, full face photographic images and any comparable images; and

i. Any other unique identifying number, characteristic, or code.

3. **Business Associates.** The Plan may disclose PHI to a Business Associate for de-identification, whether or not the de-identified information is to be used by the Plan.

B. **RE-IDENTIFICATION.** The Plan may assign a code to de-identified information in order to later re-identify the information. Re-identified information and the re-identification code is PHI that may be disclosed and used only as permitted by the Privacy Rule and these Policies and Procedures. In addition, the Plan will make a reasonable effort to limit the use, disclosure or request of re-identified PHI to the minimum necessary to accomplish the intended purpose in accordance with Policy VI.

IX. BUSINESS ASSOCIATE RELATIONSHIPS

POLICY: The Plan ensures that its Business Associates, the entities that perform services for the Plan and receive, use or disclose PHI that belongs to the Plan in the course of providing such services, protect the privacy of the PHI and provide individuals with certain rights related to the PHI. After the Plan obtains satisfactory, contractual assurances that the Business Associates will protect the PHI and limit their use and disclosure of PHI, the Plan discloses PHI to its Business Associates only the extent necessary for the Business Associates to carry out their contractual duties. In addition, after providing the required assurances, the Business Associates may create or receive PHI on behalf of the Plan. Under HITECH, and effective on or after February 17, 2010, certain provisions of the Privacy Rule and Security Rule also apply directly to the Business Associates.

A. APPLICABILITY.

1. **The Plan Enters Business Associate Agreements for the Following Types of Services**:

   a. Third party administration, claims processing and billing services; and

   b. Legal, accounting, consulting, broker, actuarial and audit services.

2. **The Plan Does Not Enter a Business Associate Agreement in the Following Instances:**

   a. For disclosures of PHI to health care providers concerning individuals' treatment;

   b. For disclosures to the Plan Sponsor, but the plan documents have been amended and the Plan Sponsor, has provided the requisite certification in accordance with Policy V.D;

   c. For disclosures to financial institutions processing consumer-conducted financial transactions by debit, credit or other payment card, clearing checks, funds transfers or any other activity that directly facilitates the transfer of funds for compensation for health care. However, the Plan will enter into a Business Associate Agreement with financial institutions to the extent such institutions perform any other service, such as billing or remittance processing;

   d. For disclosures to conduits such as the U.S. Postal Service, Internet Service Providers, and telephone companies; and

   e. For incidental disclosures inadvertently made to maintenance providers, such as electricians, janitors, and plumbers, and deliverymen.

B. PROCEDURE.

1. **Obtain Assurances.** Before the Plan discloses PHI to a Business Associate or permits a Business Associate to create or obtain PHI on behalf of it, the Plan obtains satisfactory assurances from the Business Associate, in the form of a **binding contract** that meets the requirements of 45 CFR §164.314, 504(e) and HITECH (42 U.S.C. §§ 17931, 17934).

2. **Monitoring and Non-Compliance.** The Privacy Officer monitors Business Associates' compliance with their obligations only if he/she has a reasonable belief that a Business Associate has violated its agreement. Any Plan Sponsor employee, including Privacy Employees, or Business Associate or agent who becomes aware that a Business Associate may be violating its obligations to the Plan must immediately report such to the Privacy Officer, who must investigate the matter and, if warranted, take reasonable steps to cure the violation.

   a. **Investigation.** The Privacy Officer may take the following steps as appropriate if he/she becomes aware of a possible violation of a Business Associate Agreement: interview Plan Sponsor employees (including Privacy Employees) who may have knowledge of the alleged violation; interview the Business Associate's employees who may have knowledge of the alleged violation; collect any documentation from the Plan or the Business Associate that relates to the alleged violation; contact the Business Associate to obtain information related to the alleged violation; review the documents that pertain to the alleged violation; and take any other actions that the Privacy Officer deems appropriate.

   b. **Response If Violation Has Occurred**. If the Privacy Officer determines that the Business Associate has violated the agreement, the Privacy Officer may:

      (i) sanction any Plan Sponsor employee (including but not limited to Privacy Employees) involved with the violation;

      (ii) request that the Business Associate sanction any of its employees who were involved with the violation;

      (iii) coordinate with the Business Associate to perform a risk assessment for Notification of Breach purposes and to send out or publish any necessary Notifications of Breach in accordance with Policy VII and any relevant written agreements with the Business Associate;

      (iv) mitigate any harmful effect that the Plan knows of resulting from the improper use or disclosure of the PHI as provided for in Policy XVI;

      (v) take any remedial steps provided for by the Business Associate Agreement; and/or

      (vi) work with the Business Associate to cure the violation and ensure such violation will not occur again. But, if the reasonable steps taken to cure the violation are unsuccessful, the Plan may terminate the contract with the Business Associate, if feasible.

      (vii) If termination is not feasible because there are no other viable business alternatives for the Plan, the Plan will promptly report the violation to the Secretary of Health and Human Services.

3. **Disclosures by Whistleblowers and Workforce Member Crime Victims.** The Plan will not terminate a Business Associate Agreement if the Business Associate discloses

PHI to a health oversight agency or to an attorney because it believes, in good faith, that the Plan has engaged in unlawful conduct.

X. REQUESTS TO RESTRICT USES AND DISCLOSURES

POLICY: Individuals may request that restrictions or limitations be placed on the use or disclosure of their PHI by the Plan as described below.

A. PARAMETERS OF REQUESTED RESTRICTIONS.

1. Individuals may request that restrictions be placed on the PHI that the Plan may use or disclose for treatment, payment or health care operations.

2. Individuals also have the right to request a limit on the PHI that the Plan discloses to a third party involved with the individual's care or payment for care rendered.

3. An agreed upon restriction may not prevent uses or disclosures of PHI that are permitted or required by the Privacy Rule.

4. Except as otherwise required by law, the Plan will not object to any request to a health care provider whereby an individual requests that the provider not disclose to the Plan PHI related to payment or health care operations that involve a service or treatment for which the individual has fully paid the health care provider out of pocket (and not submitted any claims to the Plan).

B. PROCEDURE.

1. To request a restriction of PHI that is maintained by the Plan Sponsor in its capacity as Plan Administrator, an individual must make a request in writing to:

   Executive Director
   PAISBOA Health Benefit Trust
   301 Iven Avenue, Suite 315
   Wayne, Pennsylvania 19087
   (484) 580-8844
   executive.director@phbtrust.org

   that(a) states the individual's name, address and the last four digits of his/her social security number, or his/her employee number; and describes the requested restriction.

2. To request a restriction of PHI that is maintained by a TPA, an individual should submit the request to the appropriate entity identified on Appendix A hereto.

C. **THE PLAN IS NOT REQUIRED TO AGREE TO REQUEST.**

1. The Plan is not required to agree to a request, except as described above in A.4.

2. If the Plan agrees to a documented restriction, the Plan will abide by that agreement, except in cases of an emergency. If the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment, the Plan may use the restricted PHI or may disclose such information to a health care provider to provide such treatment to the individual. If the Plan discloses restricted PHI to a health care provider for emergency treatment, the Plan shall request that such health care provider not further use or disclose the information.

D. **REVIEW BY PRIVACY OFFICER**. Unless there is an emergency, all questions related to the application of these provisions must be referred to the Privacy Officer before any disclosure is made.

E. **TERMINATING RESTRICTIONS.** A restriction may be terminated if:

1. The individual agrees to or requests the termination in writing;

2. The individual agrees orally to the termination and the oral agreement is documented by the Plan; or

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

F. **DOCUMENTATION**. All information related to an individual's request for a restriction as described herein must be retained for six (6) years in accordance with Policy XXIII.

XI. REQUESTS BY INDIVIDUALS TO INSPECT AND COPY PHI

POLICY: Individuals have a right to inspect and copy their PHI contained in their designated record sets.

A. PROCEDURE.

1. **Written Request.**

   a. To inspect and copy PHI maintained by Plan Sponsor in its capacity as Plan Administrator, an individual must submit a request in writing to:

      Executive Director
      PAISBOA Health Benefit Trust
      301 Iven Avenue, Suite 315
      Wayne, Pennsylvania 19087
      (484) 580-8844
      executive.director@phbtrust.org

      that states the individual's name, address and the last four digits of his/her social security number, or his/her employee number and describes the PHI the individual is seeking.

   b. To inspect and copy PHI maintained by a TPA or benefit manager, an individual must submit a request in writing to the appropriate entity identified in Appendix A hereto.

2. **Required Information.** The designated record set to which the individual will be entitled includes,

   a. All application, enrollment, and benefit information, all claims information, and any and all information used by the Plan in making decisions about individuals' claims.

   b. Information in the individual's Electronic Health Record created and/or maintained by the Plan, to the extent such Record exists. Electronic Health Records are electronic records of individualized health-related information that is created, gathered, managed and consulted by authorized health care clinicians and staff. As such, in the ordinary course, the Plan is not expected to maintain Electronic Health Record information.

   c. The Plan may deny individual access to PHI described in section C.1 of this Policy.

3. **Time for Response/Access**. Except as provided below, any request for access is responded to no later than 30 days after it was received by the Plan.

   a. 60 days are permitted for a request to access PHI that is not maintained or accessible on-site.

   b. A one-time extension of 30 days is available to the Plan if it is unable to take action within the first 30 or 60 days. Within the first 30 or 60 days after the individual's request is made, the individual will be furnished with a written statement that states:

(i) the reasons for the delay and;

(ii) the date by which a response will be provided.

B. **GRANTING OF REQUEST.**

1. **Procedure.** If a request for access to PHI is granted by the Plan, the Privacy Officer will notify the requesting party in writing of the acceptance of the request and the requested access will be provided. The Privacy Officer or Contact Person will be available to discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. To the extent the information is maintained in an Electronic Health Record, the Plan shall make available to the requesting party a copy of such information in an electronic format.

2. **Access**. The access includes inspection, copying or both and the Privacy Officer or HIPAA Contact Person will:

   a. arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI; or

   b. mail the PHI to the individual at his/her request, and

   c. to the extent the information is maintained in an Electronic Health Record, the Plan shall electronically transmit the information to the requesting individual or, as clearly directed by the requesting individual, to an entity or person clearly designated by the requesting individual to receive such information.

3. **PHI Maintained by Business Associates**. If a requesting individual is not directed to contact the TPA or benefit manager to inspect or copy his or her PHI, the Plan may arrange for the PHI related to the requesting individual that is maintained by one of its Business Associates to be made available to the individual as part of his/her designated record set.

4. **Format.** The requested information will be provided in the format requested by the individual, unless it is not readily reducible to such form. If the requested format cannot be provided, a readable hard copy form as agreed to by the Plan and the individual will be provided. If the requested PHI is maintained in more than one record set, that PHI need only be produced once. To the extent the information is maintained in an Electronic Health Record, it will be made available in electronic format.

5. **Fees.** An individual will be charged a reasonable per page fee for the hardcopy copies, or a reasonable cost-based fee for the preparation of an explanation or summary of the requested PHI. The fee includes only the cost of:

   (i) copying (including supplies and labor) the PHI; and

   (ii) postage when the individual requests mailing.

(iii) for electronic versions of Electronic Health Record information, the costs shall not be greater than the Plan's labor costs in responding to the request for the copy or summary or explanation.

C. **DENIAL OF REQUEST FOR ACCESS.** A request to inspect and copy PHI may be denied in certain limited circumstances specified by the Privacy Rule.

1. **Requests That May Be Denied**. Requests for access to the following information may be denied:

a. Psychotherapy notes (they are not part of the medical record); **[Not Reviewable "NR"]**

b. Information compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding; **[NR]**

c. PHI maintained by the Plan that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA); **[NR]**

d. Information that a licensed healthcare provider has determined that access to may endanger the life or physical safety of the individual or other person; **[Reviewable "R"]**

e. PHI that refers to another person, who is not a health care provider, and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to the other person; **[R]**

f. Access requested is made by the individual's personal representative and a licensed health care professional has determined that access to the personal representative is reasonably likely to cause substantial harm to the individual or another person; **[R]**

g. The individual agreed to temporary denial of access when he/she consented to participate in research that includes treatment, and the research is not yet complete. The individual's right of access will be reinstated upon completion of the research; **[NR]**

h. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirements of that law; **[NR]**

i. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and access would likely reveal the source of the information. **[NR]**.

2. **Form of Denial.** A denial of a request for access must:

a. Be written in plain language;

b. State the basis for the denial;

c. If applicable, state the individual's right to an independent review of the denial;

d. If applicable, provide a description of how the individual may exercise such review rights; and

e. Provide a description of how the individual may appeal the denial to the Plan, including the name and address of the Privacy Officer or HIPAA Contact Person, or to the Secretary of HHS.

3. **Making Other Information Accessible.**

a. **Partial Denial.** If access is denied in part, the individual will be given access to any other PHI requested after the Plan excludes the PHI for which access has been denied.

b. **PHI Maintained by Other Entity.** If access is denied, in whole or in part, because the requested information is not maintained by the Plan and the Plan knows where the requested information is maintained, the Privacy Officer or the HIPAA Contact Person will inform the individual where to direct the request for access.

D. REVIEW OF DENIAL OF ACCESS.

1. **Right of Review.** In certain instances, referred to above with the symbol **[R]**, an individual whose request for access is denied has the right to have the denial reviewed by a licensed health care professional designated by the Plan who did not participate in the original decision. In other situations, referred to above with the symbol **[NR]**, the Plan may deny an individual access without providing an opportunity for review.

2. **Written Request for Review.** To secure review of a denial of a request to inspect and copy PHI, an individual must submit a request in writing to:

Executive Director
PAISBOA Health Benefit Trust
301 Iven Avenue, Suite 315
Wayne, Pennsylvania 19087
(484) 580-8844
executive.director@phbtrust.org

3. **Review Procedure.**

a. Upon receipt of a request for review of a denial, the Privacy Officer must promptly refer the matter to a licensed healthcare professional who was not directly involved in the denial.

b. The designated licensed healthcare professional will, within a reasonable time, review the individual's request and the denial of the request based on the following standards:

(i) Whether access may endanger the life or physical safety of the individual or other person;

(ii) Whether the PHI makes reference to another person who is not a health care provider and the access requested is reasonably likely to cause substantial harm to that person; or

(iii) Whether the access requested is made by the individual's personal representative and access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

c. The Plan will provide prompt written notice to the individual of the determination by the designated healthcare professional.

d. The Plan will take prompt action to carry out the healthcare professional's determination.

E. **DOCUMENTATION.** Information related to individual requests for access to their PHI and the titles of the Plan personnel responsible for receiving and processing requests for access by individuals will be retained for six (6) years in accordance with the Trust's document retention policy.

XII. REQUESTS FOR CONFIDENTIAL COMMUNICATIONS OF PHI AND/OR ALTERNATIVE MEANS OF COMMUNICATIONS POLICY: Individuals may request that the Plan provide them with their PHI by confidential communications or at an alternative location as described below.

A. **STANDARD TO RECEIVE CONFIDENTIAL COMMUNICATIONS.** The Plan may accommodate an individual's reasonable request to receive communications of PHI in a confidential manner or at an alternative location. If the individual clearly and reasonably states that the disclosure of all or part of that information could endanger the individual, the Plan will accommodate the individual's request.

B. **PROCEDURE.**

1. **Written Request**.

a. For confidential communications or communications at an alternative location of PHI maintained by Plan Sponsor in its capacity as Plan Administrator, an individual must make a request in writing to:

Executive Director
PAISBOA Health Benefit Trust
301 Iven Avenue, Suite 315
Wayne, Pennsylvania 19087
(484) 580-8844
executive.director@phbtrust.org

b. For confidential communications or communications at an alternative location of PHI maintained by a TPA, requests should be made to the appropriate entity identified in Appendix A herein.

2. **Required Information.** The request should:

a. state the individual's name, address and the last four digits of his/her social security number, or his/her employee number; and

b. specify how or where communications are to be made; and,

c. if appropriate, include a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

3. **Granting Requests.** The Plan will accommodate reasonable requests and may condition its accommodation on:

a. Information as to how payment, if any will be handled and;

b. Specification of an alternative address or other method of contact.

C. **DOCUMENTATION.** The Plan will maintain all information related to requests for confidential communications or communications at an alternative location for six (6) years as required by Policy XXIII.

XIII. ACCOUNTING OF DISCLOSURES OF PHI

POLICY: Individuals have a right to receive an accounting from the Plan that lists certain disclosures of their PHI made by the Plan during the 6-year period prior to the request.

A. PROCEDURES TO REQUEST AN ACCOUNTING.

1. **Request for Accounting**.

   a. All requests for an accounting of disclosures of PHI maintained by the Plan Sponsor in its capacity as Plan Administrator must be submitted in writing to:

      Executive Director
      PAISBOA Health Benefit Trust
      301 Iven Avenue, Suite 315
      Wayne, Pennsylvania 19087
      (484) 580-8844
      executive.director@phbtrust.org

   b. All requests for an accounting of disclosures maintained by a TPA or benefits manager should be made to the appropriate entity identified in Appendix A hereto.

Required Information. The individual's written request must state:

   a. Name, address and telephone number of person who is the subject of the information for which an accounting is requested;

   b. The last four digits of the individual's social security number or his/her employee number;

   c. Time period for which accounting is sought -- not to exceed 6 years from the date of the request; and

   d. Format of the information sought -- paper or electronic (if electronic, requesting party must provide an e-mail address).

2. **Fees.** A single accounting request within a 12-month period will be free of charge. The requesting individual will be responsible for paying a reasonable cost-based fee for any additional accounting requests, provided they are notified of the costs involved before they are assessed and given an opportunity to withdraw or modify the request.

3. **Time for Response/Access**. Except as stated, any request for an accounting will be acted upon no later than 60 days after it was received.

   a. A one-time extension of 30 days is available to the Plan if it is unable to take action within the first 60 days, provided that within the first 60 days the Plan provides the individual with a written statement stating the reasons for the delay and the date by which a response will be provided.

B. **CONTENTS OF THE ACCOUNTING**:

1. **Accounting Requirements**. The accounting will be written and provide the following information to the individual:

   a. A list of the covered disclosures that occurred during the 6 years preceding the request, unless that period is shortened by the compliance date or the individual's request, and the date of each disclosure;

   b. A list of the disclosures to or by Business Associates that occurred during the relevant time frame, and the date of each disclosure;

   c. The name of the person or entity who received the disclosed information and, if known, the address of such person or entity;

   d. A brief description of the PHI disclosed in each disclosure; and

   e. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of the disclosure. In lieu of such statement, the Plan may provide a copy of a written request for a disclosure for the purpose of complying with the Secretary of HHS's compliance activities or for disclosures for which authorization is not required.

2. **Items Excluded.** The accounting for disclosures will <u>not</u> include the following disclosures:

   a. Disclosures for carrying out treatment, payment or health care operations (except as provided for in subsection C below);

   b. Disclosures pursuant to a valid authorization executed by the individual;

   c. Disclosures of PHI to the individuals;

   d. Disclosures for the facilities directory, disclosures to persons involved in the individual's care, or for other notification purposes;

   e. Disclosures for national security or intelligence purposes;

   f. Disclosures to correctional institutions or law enforcement officials; or

   g. Disclosures that occurred before April 14, 2003.

3. **Accounting Requirements; Multiple Disclosures.** If, during the period covered by the accounting request, the Plan has made multiple disclosures of PHI to the same person or entity for the purpose of complying with the Secretary of HHS's compliance activities, for disclosures for which authorization is not required, or pursuant to a single authorization, the accounting may, with respect to such disclosures, provide:

   a. The information required by Section B.1 above for the first disclosure during the accounting period;

b. The frequency, periodicity, or number of disclosures made during the accounting period; and

c. The date of the last such disclosure during the accounting period.

C. **SUSPENSION OF RIGHT.**

1. **Temporary Suspension of Right Through Written Request.** The Plan will temporarily suspend an individual's right to receive an accounting of disclosures pursuant to a health oversight agency or law enforcement official's request if the agency or official provides a written statement to the Plan:

   a. Stating that the accounting to the individual would likely impede the agency's activities and;

   b. Specifying the time period for which the suspension is required.

2. **Temporary Suspension of Right Through an Oral Request.** If the agency or official statement requesting that an accounting not be disclosed is made orally, the Privacy Officer or HIPAA Contact Person will:

   a. Document the statement, including the identity of the agency or official making the statement;

   b. Temporarily suspend the individual's right to an accounting subject to the statement; and

3. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement as required above is submitted during that time.

D. **DOCUMENTATION.** Information related to any accountings of disclosures and the titles of the Plan personnel responsible for receiving and processing requests for accountings will be retained for six (6) years in accordance with Policy XXIII.

XIV. AMENDMENT REQUESTS

POLICY: An individual has the right to request that the Plan amend his/her PHI maintained in the designated record set. However, in certain instances described below, the Plan may deny the request.

A. AMENDMENT REQUEST PROCEDURE.

1. **Amendment Requests.** All requests for amendments must be submitted in writing to:

   Executive Director
   PAISBOA Health Benefit Trust
   301 Iven Avenue, Suite 315
   Wayne, Pennsylvania 19087
   (484) 580-8844
   executive.director@phbtrust.org

   a. All requests for an amendment to PHI maintained by a TPA or benefits manager should be submitted to the appropriate entity identified in Appendix A.

2. **Required Information.** The written request should state:

   a. Name, address and telephone number of person who is the subject of the information for which an amendment is requested;

   b. The last four digits of the individual's social security number or his/ her employee number; and

   c. The reason(s) in support of the request.

3. **Time for Action on Notice of an Amendment.** Amendment requests will be acted upon no later than 60 days after receipt of the request.

   a. A one-time 30-day extension is available to the Plan so long as the individual is provided, within the first 60 days, with a written statement of the reasons for the delay and the date by which the Plan will complete the requested amendment.

B. **GRANTING AN AMENDMENT REQUEST.** If the Plan grants the request, in whole or part, it will:

1. Make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

2. Timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the Plan notify the relevant persons with which the amendment needs to be shared; and

3. Make efforts to inform and provide, within a reasonable time, the amendment to:

   a. Persons identified by the individual as having received PHI about the individual and needing the amendment; and

   b. Persons, including Business Associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information.

C. **DENIAL OF AN AMENDMENT REQUEST.**

1. **Reasons for Denial.** The Plan may deny a request for amendment for the following reasons:

   a. It is not in writing;

   b. It does not include a reason to support the request;

   c. The information was not created by the Plan, unless the individual shows that the originator of the PHI is no longer available to make the amendment;

   d. The information is not PHI kept by or for the Plan;

   e. The information is not part of the information the individual would be permitted to inspect and copy as set forth herein at Policy X; or

   f. The information that the individual seeks to amend is accurate and complete.

2. **Timely, Written Denial.** A denial will be in writing and state in plain language:

(i) The basis for denying the amendment;

(ii) That the individual has the right to submit a written statement disagreeing with the denial, and may do so by submitting a written letter to the Privacy Officer that summarizes the amendment requested, and explains why the individual disagrees with the decision to deny the amendment;

(iii) That if the individual does not submit a statement of disagreement, he/she may request that his/her request for amendment and denial be provided with any future disclosures of the PHI that is the subject of the amendment request;

(iv) That the individual has the right to file a formal complaint with the Plan and may appeal a denial of a requested amendment to PHI to the Secretary of HHS. The denial letter should explain how to file such complaints, which procedure is set forth in Policy XIV.

D. DISAGREEMENT AND REBUTTAL PROCEDURE.

1. **Statement of Disagreement and Rebuttal.** In the event that an individual files with the Plan a statement of disagreement, as he/she is entitled to do, a Privacy Officer may include a written rebuttal to the individual's statement of disagreement. If a rebuttal is prepared, a copy will be provided to the individual.

2. **Appending to the Record.** A Privacy Officer must identify the record of PHI and the record that is the subject of the disputed amendment and append or otherwise link the following to the designated record set.

a. The individual's amendment request;

b. The denial;

c. The individual's statement of disagreement, if any; and

d. The rebuttal, if any.

3. **Future Disclosures.** The following materials will be included with an individual's PHI when disclosed:

a. **Where Statement of Disagreement Filed.** If a statement of disagreement has been submitted by the individual, the Plan will include it with any subsequent disclosure of the PHI to which the disagreement relates. The material will be appended in accordance with Section 2 above or an accurate summary of any such information will be appended.

b. **Where No Statement of Disagreement Filed.** If the individual has not submitted a written statement of disagreement, the Plan will include the

individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

E. **NOTICE OF AMENDMENT BY OTHER ENTITY.** In the event that the Plan is informed by another covered entity of an amendment to an individual's PHI, it will amend the PHI in designated record sets in accordance with Section B above.

F. **DOCUMENTATION**. Information related to any request for an amendment to PHI and the titles of the Plan personnel responsible for receiving and processing requests for amendment will be retained for six (6) years in accordance with Policy XXIII.

XV. COMPLAINTS

POLICY: All individuals or parties, including Plan Sponsor Employees and their dependents, who believe that privacy rights have been violated or who have a complaint arising under the Privacy Rule or these Policies and Procedures have the right to make an inquiry or complaint with the Plan, or with the Secretary of Health and Human Services.

A. PROCEDURE TO FILE A COMPLAINT WITH THE PLAN.

1. **Reporting.** Individuals may report a complaint to the Plan as follows:

   An individual must make a complaint in writing to the Privacy Officer or HIPAA Contact Person. The complaint must include the individual's name, address and the last four digits of his or her social security number or employee number, a description of the individual's complaint, and any documentation that supports his/her complaint. The Privacy Officer or HIPAA Contact Person is available to discuss any questions the individual might have about the compliant procedure. An individual may contact the Privacy Officer or HIPAA Contact Person at the following address and phone number:

   Executive Director
   PAISBOA Health Benefit Trust
   301 Iven Avenue, Suite 315
   Wayne, Pennsylvania 19087
   (484) 580-8844
   executive.director@phbtrust.org

2. **Investigation.** When an individual makes a complaint, the Privacy Officer will promptly investigate the circumstances related to the report.

   a. **Reasonable Steps.** The Privacy Officer may take the following steps, as he/she deems appropriate, to investigate the alleged violation: interview the individual complainant; interview the Privacy Employees or any other Plan Sponsor employees, or Business Associates who may have knowledge of the alleged violation and review any relevant documents that pertain to the alleged violation. These procedures are not exclusive, and the Privacy Officer may take any steps he/she deems necessary to investigate the complaint.

   b. **Confidentiality**. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the need to undertake a full investigation.

   c. **Results of Investigation**. If the Privacy Officer determines that a violation has occurred, he/she may take action as is necessary and supported by the facts, including:

      (i) sanctioning the Privacy Employees or other Plan Sponsor employees who have acted improperly, and requesting that any Business Associate employees who have acted improperly be sanctioned by the Business Associate;

(ii) working with a Business Associate to cure any violation by the Business Associate, or terminating the Business Associate Agreement if no cure is possible;

(iii) mitigating any harmful effect that the Plan knows of resulting from the improper use or disclosure of PHI as per Policy XVI.

3. **Determination.** Upon completion of the investigation, appropriate action will be taken, as necessary and supported by the facts.

B. **PROCEDURE TO FILE A COMPLAINT WITH SECRETARY OF HHS**.

1. **Filing Complaint**. To file a complaint with the Secretary of HHS, the individual should submit a completed HHS complaint form to the Regional Office of the Office of Civil Rights, Department of Health and Human Services, in the region where the individual resides. The complaint form and the address of the appropriate Regional Office can be found at www.hhs.gov/ocr/hipaa, or by calling 1.800.368.1019. The complaint may be filed by mail, fax or email.

2. **Timing**. The complaint must be filed within 180 days of the individual's knowledge of the alleged violation.

C. **DOCUMENTATION.** Information related to each complaint received by the Plan and the disposition of each complaint will be documented by the Plan, and that documentation will be retained for six (6) years in accordance with Policy XXIII.

XVI. MITIGATION

POLICY: The Plan, to the extent practicable, will mitigate any harmful effect that it knows of resulting from the use or disclosure of PHI in violation of the Privacy Rule or these Policies and Procedures by the Plan, any Privacy Employees, other Plan Sponsor employees or Business Associates.

A. REPORTING REQUIREMENTS. Any person, including the Privacy Employees, other Plan Sponsor employees, or Business Associates, who becomes aware that an improper disclosure was made must immediately:

1. Limit any further improper disclosure; and

2. Report the matter to the Privacy Officer.

B. MITIGATION STRATEGY.

1. Process. In order to mitigate any harmful effects of an improper use or disclosure that the Plan knows of, the Privacy Officer may take the following steps:

a. notify the affected individual;

b. immediately request the return or destruction of the PHI by the disclosing party and/or the party who received the PHI;

c. create additional safeguards for protecting PHI;

d. discipline the Privacy Employees or other Plan Sponsor employees who have acted improperly;

e. work with a Business Associate who may be involved to cure a violation, including requesting that the Business Associate discipline any involved employees; and

f. terminate a Business Associate Agreement if the violation does not cease; or in the alternative, if it is not feasible to terminate the Business Associate Agreement, report the violation to the Secretary of the HHS.

The above steps are not mandatory or exclusive and the Privacy Officer may take any steps he/she deems necessary to mitigate the violation.

XVII. NON-RETALIATION AND WAIVER

POLICY: The Plan, the Privacy Employees, other Plan Sponsor employees and Business Associates are prohibited from intimidating, threatening, coercing, discriminating against or taking any retaliatory action against any an individual for exercising his/her rights under the Privacy Rule or these Policies and Procedures. In addition, the Plan is prohibited from requiring any individual to waive his/her rights under HIPAA as a condition of the provision of treatment, payment, enrollment or eligibility.

A. PROHIBITED RETALIATORY ACTIONS. The Plan, Privacy Employees, other Plan Sponsor employees, and the Business Associates will not retaliate against any individual because he/she:

1. Exercised any right under, or participated in any process established by, the Privacy Rule or these Policies and Procedures;

2. Filed a complaint with the Plan or the Secretary of HHS, or acted with regard to Notification of Breach as provided for in Policy VII;

3. Testified, assisted or participated in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of HHS; or

4. Opposed any act or practice made unlawful by the Privacy Rule or improper by these Policies and Procedures, provided that the individual has a good faith belief that the practice opposed is unlawful or contrary to these Policies and Procedures, and the manner of the opposition is reasonable and does not involve an impermissible disclosure of PHI.

B. PROCEDURE. The report and investigation of allegations of retaliation will follow the procedures set forth in Policy XV.

C. WAIVER. Individuals may not be required to waive their rights under the Privacy Rule or these Policies and Procedures, including their rights to file a complaint with the Secretary of Health and Human Services under HIPAA or obtain a Notification of Breach as provided by Policy VII herein, as a condition of treatment, payment, enrollment in the Plan or eligibility for benefits.

D. SANCTIONS. Any Privacy Employees or other Plan Sponsor employees found to have retaliated against an individual for making a complaint under Policy XV, for participating in an investigation, or for seeking or obtaining a waiver from an individual, will be subject to appropriate sanctions as set out in Policy XXII. Any Business Associates' employee found to have retaliated against an individual or sought or obtained a waiver from an individual may be sanctioned in accordance with the Business Associates' sanctions policies.

XVIII. TRAINING

POLICY: The Plan will train the Privacy Employees and other appropriate Plan Sponsor employees on these Policies and Procedures as necessary and appropriate for those employees to carry out their functions.

A. TRAINING REQUIREMENTS.

1. **Responsibility.** The Privacy Officer is responsible for ensuring timely and proper training.

2. **Time for Training.** Training will be provided:

   a. To the appropriate Privacy Employees and other Plan Sponsor employees;

   b. To each new Privacy Employee or other Plan Sponsor employee who needs training within a reasonable time after joining the workforce; and

   c. To each Privacy Employee or other Plan Sponsor employee whose functions are affected by any material changes in these Policies or Procedures within a reasonable time after the effective date of those changes. The HITECH amendments to HIPAA caused material changes in these Policies and Procedures the majority of which became effective on or about February 17, 2010, and with regard to which appropriate Employees will be or were timely trained.

   d. As determined by the Privacy Officer, Privacy Employees will be required to attend periodic "refresher" training on the Privacy Rule and these Policies and Procedures.

B. **DOCUMENTATION.** The Plan will document that all training has been provided as required and retain those records for six (6) years in accordance with Policy XXIII.

XIX. MARKETING, FUNDRAISING AND PROHIBITION ON SALE OF PHI

POLICY: The Plan limits its marketing communications as described in this Policy, prohibits the use of PHI for fundraising purposes and prohibits the sale of PHI except as permitted by this Policy.

A. **LIMITATION ON MARKETING**: "Marketing" includes making a communication that encourages the purchase or use of a product or service where the Plan receives financial remuneration from a third party for making the communication. Except as provided below, the Plan must acquire an individual authorization for all marketing communications, whether for "treatment" or "health care operations" purposes where the Plan receives financial remuneration for making the communications from a third party whose product or service is being marketed. "Financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described.

1. **Communications Permitted Without Authorization.** Under this exception to the above rule, the Plan may make the following marketing communications without an individual's authorization:

a. Communications to describe a health-related product or service (or payment for such product or service) that is part of the Plan's benefits. Such communications may include information about (i) the entities participating in the Plan's network, (ii) replacement of or enhancement to a Plan benefit, or (iii) health-related products that add value to but are not part of the Plan's benefits.

b. Communications for the treatment of an individual.

c. For case management or care coordination for the individual, or to direct or recommend to the individual alternative treatments, therapies, health care providers or health care settings.

d. However, for marketing communications under (a)–(c) to be permitted without authorization, the Plan may not receive direct or indirect remuneration in exchange for the communication, except if:

(i) The communication describes a drug or biologic that the individual is currently being prescribed, and the payment received by the Plan is a reasonable amount; or

(ii) The communication is made by a Business Associate on behalf of the Plan, and pursuant to a Business Associate Agreement.

B. **PROHIBITION ON FUNDRAISING**. Neither the Plan nor its Business Associates may contact participants for fundraising purposes.

C. **PROHIBITION ON SALE OF PHI**. The Plan may not receive direct or indirect remuneration in exchange for PHI, except in the following instances.

1. Pursuant to a valid authorization from an individual, which specifies whether the PHI may be further exchanged by the entity receiving the PHI;

2. If the exchange of PHI is for public health activities described in 45 C.F.R. § 164.512(b);

3. If the exchange of PHI is for research purposes (as described in 45 C.F.R. § § 164.501 and 164.512(i)) and the price charged reflects the costs of preparation and transmittal of the data for that purpose;

4. If the exchange of PHI is for the Treatment of the individual (subject to any limit set by the Secretary);

5. If the exchange is for the following Health Care Operations: the sale, transfer, merger or consolidation of all or part of the Plan with another Covered Entity, or an entity that will become a Covered Entity after the transaction, and due diligence related to such transaction activity.

6. If the remuneration is paid by the Plan to its Business Associates for the Business Associates to provide services to or on behalf of the Plan pursuant to a Business Associate Agreement;

7. If the exchange is to provide an individual with a copy of his/her PHI in accordance with Policy XI; or

8. If the exchange is otherwise permitted by the Secretary in regulations.

XX. PROHIBITION ON USE AND DISCLOSURE OF GENETIC INFORMATION

POLICY: The Plan will not use or disclose an individual's genetic information for underwriting purposes.

A. Definition of Genetic Information: Genetic information means information about an individual's genetic tests, the genetic tests of family member of the individual, the manifestation of a disease or disorder in family members of the individual or any request of or receipt of genetic services, or participation in clinical research that includes genetic services by the individual or a family member of the individual. The term genetic information includes, with respect to a pregnant woman, genetic information about the fetus and with respect to an individual using assisted reproductive technology, genetic information about the embryo. Genetic information does not include information about the sex or age of an individual.

B. Definition of Underwriting Purposes: Underwriting purposes means that the Plan will not use or disclose genetic information to: (a) determine eligibility under the Plan; (b) compute the premium or contribution amounts under the Plan; (c) apply any pre-existing condition exclusions under Plan; and (d) any other activities related to the creation, renewal, replacement of a contract of health insurance or health benefits provided under the Plan.

XXI. NOTICE OF PRIVACY PRACTICES; DISSEMINATION; CHANGES

POLICY: The Plan disseminates and maintains a Notice of Privacy Practices ("Privacy Notice") that clearly states the manner in which it may use and disclose the individuals' PHI and provides adequate notice of the individuals' rights and the covered entities' legal duties with respect to PHI. Individuals have a right to request and receive a paper copy of the Privacy Notice at any time.

A. PRIVACY NOTICE.

1. Responsibility. The Privacy Officer is responsible for developing, reviewing, revising, updating and disseminating the Plan's Privacy Notice to ensure that it conforms to these Policies and Procedures.

2. Notice Requirements. The Privacy Notice will be in plain language and include the content requirements set forth in 45 CFR 164.520.

3. Reservation of Rights to Change Policy/Notice. The Plan herein reserves its right to revise these Policies and Procedures and its Privacy Notice and to make any revisions effective for PHI currently in its possession as well as any information it receives in the future.

    a. Changes to Comply with Law: These Policies and Procedures will be changed to maintain compliance with the Privacy Rule and/or governing law.

    b. Corresponding Changes to Notice: If there is a change in these Policies and Procedures a corresponding change will be made to the Privacy Notice to comply with the notice requirements of the Privacy Rule.

4. Change to Term Covered by Notice. The Plan may change a privacy practice that is stated in the Notice, and the related Policies and Procedures, without having reserved the right to do so, provided that such change:

    a. Is effective only with respect to PHI created or received after the effective date of the Notice;

    b. Complies with the Privacy Rule;

    c. Is documented in accordance with Policy XXIII; and

    d. Is incorporated into a revised Notice that is made available as required by the Privacy Rule and these provisions.

5. Change to Term Not Covered by Notice. The Plan may change, at any time, a policy or procedure that does not materially affect the content of the Notice, provided that:

    a. The Policies and Procedures, as revised, complies with the Privacy Rule and these provisions; and

    b. Prior to the effective date of the change, the revised Policies and Procedures are documented in accordance with Policy XXIII.

B. **DISSEMINATION OF NOTICE.**

1. **Time to Notify Individuals.** The Notice must be available on request to any person and/or individual as follows:

   a. **Notification.** The Plan must distribute the "Notice of Privacy Practices" to individuals covered by the Plan:

      (i) At enrollment for new enrollees; and

      (ii) Within 60 days after a material revision to the Notice; or

      (iii) If the Plan posts the Notice on its website, it shall:

         (a) prominently post the material change or the revised Notice on its website by the effective date of the material change to the notice; and

         (b) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual enrollment (or at the beginning of the plan year if there is no annual enrollment) to individuals then covered under the Plan.

   b. **Three Years.** The Plan must notify individuals covered by the plan, at least once every three years, of the availability of the Notice and how they can obtain a copy of the Notice statement.

2. **Availability of Privacy Notice.**

   a. **Electronic Notice**. The Plan may provide Notice to an individual by e-mail if the individual agrees to such Notice. If the Plan becomes aware that e-mail transmission has failed, a paper copy of the Notice must be provided to the individual. An individual receiving e-mail Notice always maintains the right to obtain a paper copy of Notice from the Plan upon request.

   b. **Paper Copy of Notice**. Individuals have a right to a paper copy of the Privacy Notice, even if they have previously agreed to receive the Privacy Notice electronically. Individuals may receive a copy of the Privacy Notice by:

      (i) In-Person Request. An individual may make a request in person to the Plan's Privacy Officer or HIPAA Contact Person.

      (ii) Written Request. An individual can submit a request for Notice in writing to:

      Executive Director
      PAISBOA Health Benefit Trust
      301 Iven Avenue, Suite 315
      Wayne, Pennsylvania 19087
      (484) 580-8844

executive.director@phbtrust.org

C. **DOCUMENTATION.** The Plan will retain copies of the Notices issued by it for six (6) years in accordance with Policy XXIII.

XXII. SANCTIONS FOR NON-COMPLIANCE

POLICY: The Plan Sponsor will apply appropriate sanctions against any of its employees, including Privacy Employees, who fail to comply with these Policies and Procedures or the requirements of the Privacy Rule.

A. SANCTIONS FOR NON-COMPLIANCE.

1. **Discipline**. The Plan Sponsor has a zero-tolerance policy regarding the improper use or disclosure of PHI by any employee. Any Plan Sponsor employee, including any Privacy Employee, who violates the Privacy Rule and/or these Policies and Procedures will be subject to sanctions, which may include oral counseling, write-ups, suspension and/or termination. All Plan Sponsor employees are employees-at-will whose employment at the Plan Sponsor may be terminated at any time, with or without cause or notice.

2. **Discretion of the Privacy Officer**: The Plan Sponsor does not guarantee that one form of discipline will necessarily precede another. Further, the Plan Sponsor reserves the right, at all times, to take whatever disciplinary action it deems appropriate, up to and including termination. Prior notification and progressive discipline are not prerequisites for termination or other disciplinary action.

B. EXEMPTIONS.

1. **Whistleblower.** No violation may be considered to have been committed if a Plan Sponsor employee:

   a. Discloses PHI with a good faith belief that the Plan has engaged in conduct that is violative of these Policies and Procedures or the Privacy Rule and the disclosure is to:

      (i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan; or,

      (ii) An attorney retained by or on behalf of the employee or Business Associate for the purpose of determining legal options with regard to whether the Plan has engaged in conduct that is unlawful.

2. **Victims of a Crime.** No violation can be considered to have been committed where a Plan Sponsor employee who is the victim of a criminal act, discloses PHI to a law enforcement official, provided that:

   a. The PHI disclosed is about the suspected perpetrator of the criminal act; and

   b. The PHI is limited to the information listed in Section 164.512(f)(2)(i).

C. **DOCUMENTATION.** All sanctions that are applied will be documented and any related records will be retained for six (6) years in accordance with Policy XXIII.

XXIII. DOCUMENTATION, RECORDS RETENTION AND DOCUMENT DESTRUCTION

POLICY: The Plan will maintain a written or electronic record of certain documentation, in accordance with this policy.

A. **DOCUMENTATION.** The following documents must be maintained:

1. The Policies and Procedures for complying with Privacy Rule;

2. Any communication required by the Privacy Rule to be in writing; and

3. Any action, activity, or designation required to be documented by the Privacy Rule.

B. **RECORDS RETENTION**. The Plan will retain the above-described required documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later. If the documentation is plan documentation under ERISA, then the Plan will retain that information for seven (7) years.

C. **DOCUMENT DESTRUCTION.** All hardcopy documents shall be destroyed by shredding, either at the end of the six- year document retention period or**,** for PHI that is not subject to the six-year document retention requirements, when the information is no longer necessary for the purpose for which it was created, obtained, used or disclosed. The Plan Sponsor maintains clearly marked, locked "shredding" bins into which PHI should be deposited to be shredded.