

Policies and Procedures for HIPAA Compliance
Public Education Employees' Health Insurance Plan

Effective Date: Restated as of January 1, 2012

Updated December 5, 2013

Table of Contents

1.	Purpose.....	1
2.	Policy	2
3.	Definitions	3
3.1	Benefit Staff.....	3
3.2	Breach	3
3.3	Business Associate	3
3.4	CFR.....	3
3.4	Designated Record Set	3
3.6	Disclosure	3
3.7	Electronic Protected Health Information	3
3.8	Protected Health Information	4
3.9	Privacy Official	4
3.10	Security Official	4
3.11	Unsecured PHI.....	4
3.12	Use.....	4
4.	Procedures – Uses and Disclosures	5
4.1	Uses and Disclosures for Payment and Health Care Operations.....	5
4.2	Administrative use only	6
4.3	Physical Safeguards	6
4.4	Disclosures of PHI to Service Providers or Insurers.....	7
4.5	Disclosures of PHI to Business Associates	7
4.6	Disclosure to a Designated Personal Representative	7
4.7	Disclosure to People Involved in an Individual’s Care or Responsible for Payment	8
4.8	Mandatory Disclosures to Individuals or to the Department of Health and Human Services (DHHS).....	10
4.9	Disclosures for Legal and Public Policy Purposes.....	10
4.10	Disclosures of PHI Pursuant to an Authorization	12
4.11	Disclosure to Spouses, Family Members and Friends	12
4.12	Role of Business Associates with Respect to Requests for Disclosure	13
4.13	Disclosures of De-Identified Information	13
4.14	Minimum Necessary Standard.....	14
4.15	Requests for Disclosure	16
4.16	Disclosures Log.....	16
4.17	Notification in the Event of a Breach of PHI.....	16
5.	Procedures – Security.....	18
5.1	Risk Assessment and Management of EPHI.....	18
5.2	General Work Rules.....	18
5.3	Business Associate Agreements	18
6.	Procedures – Individual Rights.....	19
6.1	Right to Accounting of PHI Disclosures	19

6.2	Right to Review and Copy PHI in Designated Record Set	20
6.3	Right to Amend PHI in a Designated Record Set	21
6.4	Right to Request Restrictions on Use and Disclosure of PHI	23
6.5	Right to Request Confidential Communications	24
6.6	Role of Business Associates	24
7.	Verification of Identity	25
7.1	General Requirements	25
7.2	Verification of Identity and Authority	25
7.3	Document Retention	26
8.	Document Retention	27
8.1	Retention Period	27
8.2	Electronic Records Retention	27
8.3	Business Associate Agreements	28
8.4	Employment File	28
8.5	Storage	28
9.	Distribution of Privacy Notice	30
9.1	Timing	30
9.2	Distribution by Mail	30
9.3	"Around the Board" Intranet Site	30
10.	Privacy Official	31
10.1	Role	31
10.2	Duties	31
11.	Security Official	33
11.1	Role	33
11.2	Duties	33
12.	General Provisions	35
12.1	Complaints	35
12.2	Sanctions	35
12.3	Mitigation	36
13.	Forms and Templates	37
	Certification of Receipt of HIPAA Policies and Procedures	38
	Uses and Disclosures Tracking Form	43
14.	Privacy Notices	44
15.	Business Associate Data Security Policy	49

1. Purpose

Pursuant to Sections 16-25A-1, et seq. of the Code of Alabama 1975 as amended, the Public Education Employees' Health Insurance Board, together with certain of its agents and employees (collectively referred to herein as "PEEHIP") administers the Public Education Employees' Health Insurance Plan (the "Plan"). The Plan constitutes an "organized health care arrangement" as that term is defined under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). PEEHIP and the Plan intend to comply with the administrative simplification requirements of HIPAA (including the amendments included in the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009 (collectively referred to in this document as HIPAA).

To ensure HIPAA compliance, PEEHIP has established policies and procedures for the use and disclosure of protected health information (PHI) and the security of electronic protected health information (EPHI). As part of its compliance effort, PEEHIP has reviewed and updated those policies and procedures, and has set them forth in this document, which replaces all other similar documents in their entirety.

2. Policy

PEEHIP administers medical, prescription drug and health care spending account benefits for eligible employees, retirees and their dependents (the "Individuals") through the Plan. Staff members of PEEHIP, as members of PEEHIP's workforce, may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the PEEHIP Board as the Plan Sponsor; or (3) on behalf of PEEHIP in connection with the administration of the Plan.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations restrict the ability of PEEHIP and the Plan to use and disclose Protected Health Information ("PHI"). In addition, HIPAA imposes requirements to maintain the confidentiality, integrity and availability of PHI retained or transmitted in electronic format.

It is PEEHIP's policy to comply fully with HIPAA's requirements. To that end, all employees of PEEHIP, as well as all employees of the Retirement Systems of Alabama ("RSA"), which by state law assists PEEHIP in some of its administrative functions (e.g., legal, accounting, IT), who have access to PHI must comply with these Policies and Procedures for HIPAA Compliance. Failure to act in accordance with these policies and procedures may result in disciplinary action. To ensure compliance, PEEHIP shall train all Benefit Staff (see Section 3.1) in the requirements of HIPAA and in the application of these Policies and Procedures for HIPAA Compliance.

3. Definitions

3.1 Benefit Staff

Benefit Staff means individuals employed by PEEHIP and/or RSA who have any involvement in the administration or operation of the Plan, or who have access to PHI in connection with services performed for the Plan. Benefit Staff include the Privacy Official, Benefits Administration & Operations staff, Enrollment & Eligibility staff, and in more limited instances, General Counsel and Finance Staff.

3.2 Breach

Breach shall be defined as set out in 45 CFR §164.402 and shall mean the unauthorized acquisition, access, use or disclosure of Unsecured PHI that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

3.3 Business Associate

A business associate is an entity or person who:

- a. Performs or assists in performing a Plan function or activity involving the use, and disclosure of PHI (such as claims processing or administration; data analysis, underwriting, etc.); or
- b. Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves furnishing the service provider access to PHI.

3.4 CFR

CFR means the Code of Federal Regulations.

3.4 Designated Record Set

Designated Record Set means the enrollment, payment, claims adjudication, and case or medical management records maintained by the Plan, or any other group of records that is used by the Plan to make decisions about individuals as it relates to their benefits.

3.6 Disclosure

Disclosure means any release, transfer, provision of access to, or divulging in any other manner, of PHI to persons other than Benefit Staff, or for purposes other than the administration of the Plan.

3.7 Electronic Protected Health Information

Electronic Protected Health Information ("E PHI") is PHI that is retained or transmitted in electronic media.

3.8 Protected Health Information

Protected Health Information (“PHI”) is information that is created or received by the Plan, and that relates to:

- a. the past, present, or future physical or mental health or condition of a covered Individual
- b. the provision of the health care to a covered Individual, or
- c. the past, present, or future payment for the health care of a covered Individual.

In addition, the information must identify the participant; or there must be a reasonable basis to believe the information could be used (alone or in combination with other information) to identify the Individual. PHI includes information about persons living or deceased whether in electronic, printed or spoken form.

3.9 Privacy Official

Privacy Official means the Director of PEEHIP.

3.10 Security Official

Security Official means the PEEHIP IT Security Officer.

3.11 Unsecured PHI

Unsecured PHI shall mean PHI that is not secured through the use of a technology or methodology that renders such PHI unusable, unreadable or indecipherable to unauthorized individuals pursuant to 45 CFR §164.402.

3.12 Use

Use means the sharing, application, utilization, examination, or analysis of PHI by Benefit Staff acting as administrators of the Plan.

4. Procedures – Uses and Disclosures

4.1 Uses and Disclosures for Payment and Health Care Operations

Benefit Staff, acting in their capacity as administrators of the Plan, may use or disclose PHI:

- a. For payment or health care operations of the Plan
- b. For payment activities of another group health plan (e.g., coordination of benefit activities), health care provider, or insured HMO
- c. For the quality assessment and improvement, case management, or health care fraud and abuse detection programs of another group health plan, health care provider, or insured HMO.

Uses and disclosures under this section are subject to the minimum necessary standard, described in Section 4.14.

All uses and disclosures of PHI by Benefit Staff shall be in accordance with the privacy provisions of the plan documents, as adopted and certified by PEEHIP.

Any member of the Benefit Staff who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official.

4.1.1. Payment includes activities undertaken to:

- a). obtain Plan contributions
- b). determine or fulfill the Plan's responsibility for the provision of benefits under the Plan or
- c). obtain or provide reimbursement for health care.

Payment activities include many activities that will be undertaken by Benefit Staff or other administrators, such as the administrator(s) of the hospital medical plan and the pharmacy plan.

Such payment activities include:

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

- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities (including pre-certification and preauthorization of services), concurrent and retrospective review of services;
- Disclosure to consumer reporting agencies of any of the following PHI relating to the collection of premiums or reimbursement (a) name and address, (b) date of birth, (c) Social Security number, (d) payment history, (e) account number, and (f) name and address of the health care provider and/or health plan.

4.1.2 Health care operations means any of the following activities to the extent that they are related to Plan administration:

- a). Conducting quality assessment and improvement activities;
- b). Reviewing health plan performance;
- c). Underwriting and premium rating;
- d). Conducting or arranging for medical review, legal services and auditing functions;
- e). Business planning and development; and
- f). Business management and general administrative activities.

4.2 Administrative use only

Benefit Staff may use PHI only for administrative functions of the Plan. However, in no event will Benefit Staff use PHI that is genetic information for underwriting purposes. Benefit Staff may not disclose PHI to other PEEHIP or RSA employees unless the disclosure is necessary to perform Plan administrative functions. Any disclosure shall be limited to the minimum amount of information necessary to perform the administrative function in accordance with Section 4.14.

In no event shall Benefit Staff, or any employee to whom Benefit Staff have disclosed PHI, use or disclose the information for employment-related decisions unless the affected individual has signed a specific authorization for such disclosure. See Section 4.10.

4.3 Physical Safeguards

Benefit Staff shall establish reasonable physical safeguards to protect PHI from inappropriate use or disclosure. To protect PHI, Benefit Staff will:

- a. take reasonable precautions to ensure that PHI is not visible to passers-by (e.g., computer screens will be reasonably shielded from public view);
- b. maintain paper files in locked cabinets or drawers;

- c. use passwords to prevent access to computers and computer files (i.e., files should be password protected or encrypted as well);
- d. use “locking” screen savers;
- e. limit the use of PHI in email and fax transmissions;
- f. eliminate the use of speakerphones in open areas;
- g. destroy CDs or diskettes containing unneeded PHI in accordance with procedures established by the PEEHIP/RSA Information Technology (IT) staff;
- h. shred (on-site or through the use of contracted service) unnecessary or obsolete papers; and
- i. take other actions as may be appropriate under the circumstances.

4.4 Disclosures of PHI to Service Providers or Insurers

Benefit Staff may disclose PHI to service providers or insurers only under the following circumstances:

- a. To an insured HMO or health insurance issuer to that plan for payment or health care operations of an individual covered under that plan. The Plan documents must include privacy provisions that permit the sharing of the information.
- b. To other service providers (e.g., Blue Cross Blue Shield of Alabama): only if there is a signed business associate agreement with the service provider. See Section 4.5.
- c. To non-health benefit programs (such as disability or life insurance): only if the employee has provided a signed authorization. See Section 4.10 for additional requirements for obtaining an authorization.

4.5 Disclosures of PHI to Business Associates

- a. Benefit Staff may disclose PHI to a business associate only if a business associate contract is in effect and if the disclosure is permitted under the terms of that contract. All uses and disclosures of Plan PHI by a business associate must be in accordance with the terms of a valid business associate agreement.
- b. Before providing PHI to a business associate, Benefit Staff must verify that a business associate contract is in place. The following additional conditions must be satisfied:
 - i. Disclosures must be consistent with the terms of the business associate contract.
 - ii. Disclosures must comply with the minimum necessary standard. See Section 4.14

4.6 Disclosure to a Designated Personal Representative

An individual may designate a personal representative to whom disclosures of Protected Health Information may be made. Before making a disclosure to a personal representative, Benefit Staff shall:

- a. Verify the identity of the representative. See Section 7.
- b. Verify that the designation form is valid. Valid designation forms are those that:
 - i. Are properly signed and dated by the individual and individual's representative;
 - ii. Are not expired or revoked; the expiration date of the designation must be a specific date or specific time period, or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage);
 - iii. Contain a description of the information to which the designation applies;
 - iv. Contain a statement regarding the individual's right to revoke the designation and the procedures for revoking designation; and
 - v. Contain a statement indicating that the personal representative has accepted the designation and has agreed to act on behalf of the individual in accordance with the conditions set forth.

All disclosures made to an individual's representative must be consistent with the terms and conditions of the designation.

4.7 Disclosure to People Involved in an Individual's Care or Responsible for Payment

Benefits Staff may disclose an individual's protected health information to people who are involved in the individual's care or responsible for the payment of care for services provided to the individual in the following circumstances:

a. Disclosure to Facilitate Individual's Care or Payment

An individual's protected health information may be disclosed to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, if such protected health information is:

- i. Directly relevant to the recipient's involvement with the individual's care; or
- ii. Relevant to make payment related to the individual's health care.

b. Disclosure to Locate and Notify Individual's Care Giver

An individual's protected health information may be disclosed if doing so is necessary to identify, locate and notify a family member, personal representative, or other person responsible for the care of the individual of the individual's location, general condition or death.

c. Decision to Disclose

The final decision to disclose the individual's protected health information will be made by the Privacy Official on behalf of the Plan if the individual is not present, or is incapacitated or otherwise unable to make decisions regarding the disclosure of his or her own information. The Plan will use its best judgment in determining if

the disclosure is in the individual's best interest and limiting the disclosure to only the information that is directly relevant to the provision of care.

4.8 Mandatory Disclosures to Individuals or to the Department of Health and Human Services (DHHS)

- a. To an individual: Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the Benefit Staff must follow the procedures in Section 6.2.
- b. To DHHS: Upon receiving a request from a DHHS official for disclosure of PHI, the Benefit Staff must take the following steps:
 - i. Verify the identity of the public official. See Section 7.
 - ii. Maintain a record of these disclosures.

4.9 Disclosures for Legal and Public Policy Purposes

Benefit Staff who receive a request for disclosure of an individual's PHI that appears to fall within one of the following legal or public policy categories described below must contact the Privacy Official. Any such disclosures must comply with the minimum necessary standard in Section 4.14. A record of these disclosures must be maintained in accordance with Section 8.1.

a. *Disclosures about victims of abuse, neglect or domestic violence, if:*

- i. The disclosure is required by law;
- ii. The individual agrees to the disclosure; or
- iii. The disclosure is expressly authorized by law and (a) the Privacy Official believes that the disclosure is necessary to prevent harm to the individual (or other victim) or (b) the individual is incapacitated and unable to agree (but only if the information will not be used against the individual and is needed for an imminent enforcement activity).

The individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

b. *For Judicial and Administrative Proceedings, in response to:*

- i. An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or
- ii. A subpoena, discovery request or other lawful process, not accompanied by an order of a court or administrative tribunal, if the requirements of 45 CFR §164.512 (Uses and disclosures for which an authorization or opportunity to agree or object is not required) of the HIPAA regulations are satisfied.

c. *To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:*

- i. Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information;
 - ii. Information to identify or locate a suspect, fugitive, material witness or missing person, limited in accordance with 45 CFR §164.512(f) of the HIPAA regulations;
 - iii. Information about a suspected victim of a crime (a) if the individual agrees to disclosure; or (b) if the Plan cannot obtain the individual's agreement due to incapacity or other emergency circumstances, and the information is not to be used against the victim, the need for information is urgent, and the disclosure is in the best interest of the individual;
 - iv. Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct; or
 - v. Information that constitutes evidence of criminal conduct that occurred on PEEHIP's premises.
- d. *To Appropriate Public Health Authorities for Public Health Activities, as authorized by law, e.g., to the appropriate agency for reporting and prevention of the spread of communicable diseases, or in connection with activities of the Food and Drug Administration.*
 - e. *To a Health Oversight Agency for Health Oversight Activities, as authorized by law, for activities necessary for appropriate oversight of the health care system, government benefit and regulatory programs or entities subject to civil right laws for which health information is necessary to determine compliance;*
 - f. *To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law;*
 - g. *For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation;*
 - h. *For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board;*
 - i. *To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public;*
 - j. *For Specialized Government Functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities; or*

- k. *For Workers' Compensation Programs*, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

4.10 Disclosures of PHI Pursuant to an Authorization

Any requested disclosure to a third party that does not fall within one of the preceding categories may be made pursuant to an individual authorization.

Benefit staff should advise individuals that an authorization may be required in order to assist the individual in resolving claim questions with the benefit administrator (Blue Cross Blue Shield of Alabama). The individual should also be advised that an authorization will be required if the information requested does not pertain to that individual and the subject of the request is not the individual's minor child. For example, if an employee requests information about his or her spouse's claim, an authorization from the spouse is required.

If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- a. Verify the identity of the individual (or individual's representative). See Section 7.
- b. Verify that the authorization form is valid. Valid authorization forms are those that:
 - i. Are properly signed and dated by the individual or individual's representative;
 - ii. Are not expired or revoked (the expiration date of the authorization form must be a specific date or specific time period, or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage);
 - iii. Contain a description of the information to be used or disclosed;
 - iv. Contain the name of the entity or person authorized to use or disclose the PHI;
 - v. Contain the name of the recipient of the use or disclosure;
 - vi. Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
 - vii. Contain a statement regarding the possibility for a subsequent re-disclosure of the information.
- c. All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
- d. A record of authorized disclosures must be maintained. See Section 8.

All authorizations for use or disclosure for non-Plan purposes must be on a form provided by or approved by the Privacy Official. Benefit Staff shall not attempt to draft authorization forms.

4.11 Disclosure to Spouses, Family Members and Friends

Neither the Plan nor PEEHIP will disclose PHI to an individual's family or friends except as required or permitted by HIPAA (e.g., in the case of an emergency or natural disaster). Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI.

- a. If Benefit Staff receive a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is an unemancipated minor child and the disclosure is not prohibited by state law; or (2) the personal representative of the individual; then the procedures for verifying the identity or authority of the individual in Section 7 should be followed.
- b. Once the identity and authority of a parent or personal representative is verified, the disclosure procedure in Section 4.6 should be followed.
- c. All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See Section 4.10.
- d. A record of authorized disclosures must be maintained. See Section 8.

4.12 Role of Business Associates with Respect to Requests for Disclosure

Where PHI is held by the Plan's third party administrators who are Business Associates, the Plan has delegated the authority to respond to requests for PHI to these Business Associates. The Privacy Official is responsible for monitoring compliance with these Policies and for working with the Business Associates regarding any suspected violations of the Policies.

4.13 Disclosures of De-Identified Information

De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways that the Plan can determine that information is de-identified: either by professional statistical analysis, or by removing all of the following 18 specific identifiers:

- a. Name;
- b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code (three digit zip code may be used only if, according to the current publicly available data from the Bureau of the Census the geographic unit defined by the three-digit zip code contains more than 20,000 people);
- 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 ages and elements may be aggregated into a single category of age 90 or older;
- d. Telephone numbers;
- e. Fax numbers;
- f. Electronic mail addresses;

- g. Social Security numbers;
- h. Medical record numbers;
- i. Health plan beneficiary numbers;
- j. Account numbers;
- k. Certificate/license numbers;
- l. Vehicle identifiers and serial numbers, including license plate numbers;
- m. Device identifiers and serial numbers;
- n. Web Universal Resource Locators (URLs);
- o. Internet Protocol (IP) address numbers;
- p. Biometric identifiers, including finger and voice prints;
- q. Full face photographic images and any comparable images; and
- r. Any other unique identifying number characteristic or code.

Benefit Staff should submit any information it believes to be de-identified to the Privacy Official prior to making the disclosure. The Privacy Official will verify that the information has been de-identified.

The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

4.14 Minimum Necessary Standard

Benefit Staff shall make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose, in accordance with 45 CFR §164.502 (b)(1). If using de-identified information could satisfy the purpose of the use or disclosure, then de-identified information shall be used. For example, a report that is used to confirm an employee's eligibility for coverage does not have to contain information about specific claims. Similarly, a report that is sent to a broker for contract renewal need not include names and social security numbers of participants.

a. Routine Uses and Disclosures:

- i. When soliciting bids from insurance companies for fully insured health plans or stop-loss coverage, Benefit Staff shall provide bidders with necessary underwriting information, including aggregate claims information for one or more prior years, as well as information regarding specific claims as is necessary to determine the cause of unexpected claims that may affect the premiums.
- ii. Benefit Staff who are Plan fiduciaries shall have access to and shall be permitted to disclose such PHI as they deem necessary for the determination of Plan benefits and the full and fair review of appeals from denied claims for benefits.

- iii. Benefit Staff shall have access to claims information for the current and prior years for purposes of reviewing Plan operations and the costs of Plan sponsorship, and may audit individual claims, as it deems necessary, in order to assess the performance of service providers for the Plans.
 - iv. A personal representative who has been appointed by (or for) a Plan participant, shall have access to PHI only as necessary to carry out the purposes of his or her appointment.
 - v. Any attorney for the Plan or for PEEHIP shall have access to any PHI necessary in order for the attorney to carry out his or her representation of the Plan or PEEHIP.
 - vi. Benefit Staff shall have complete access to all enrollment information relating to individuals who are covered, or who are seeking coverage, under the Plans, in order to determine eligibility for participation and benefits.
 - vii. Benefit Staff shall have access to individual claim files as necessary to determine the coverage provided under the Plans with respect to a given claim.
 - viii. Benefit Staff and other health plans or insurers shall have access to any claims or coverage information necessary to the application of coordination of benefits provisions of the Plans or other group health plans.
 - ix. Benefit Staff and any utilization review PEEHIP retained in connection with the Plans shall have access to any PHI necessary to carry out the terms of the Plans' utilization review provisions.
- b. *Non-Routine Uses and Disclosures.* For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure. The Privacy Official shall use the following criteria when making case-by-case determinations for non-routine uses and disclosures of PHI:
- i. Is there a legitimate and reasonable need for any or all of the PHI proposed to be collected?
 - ii. Can the request be satisfied using De-identified Information?
- c. *Exceptions.* The minimum-necessary standard does not apply to any of the following:
- i. Uses or disclosures made to the individual to whom the information relates;
 - ii. Uses or disclosures made pursuant to an individual authorization;
 - iii. Disclosures made to DHHS;
 - iv. Uses or disclosures required by law and in compliance with 45 CFR §164.512; and
 - v. Disclosures to a health care provider for treatment.

4.15 Requests for Disclosure

Benefit Staff, at the express direction of the Privacy Official, may rely upon a requested disclosure as the minimum necessary, when reasonable under the circumstances, in the following instances:

- a. When making disclosures to public officials as permitted under HIPAA, if the public official represents that the information requested is the minimum necessary for the stated purpose of the request;
- b. When the information is requested by another covered entity under HIPAA; or
- c. When the information is requested by Benefit Staff or a Business Associate of the Plan for the purpose of providing professional services to the Plan, if the information requested is the minimum necessary for the stated purposes.

4.16 Disclosures Log

Benefit staff will maintain a record of all disclosures of PHI made in connection with the following activities:

- a. Disclosures that exceed the Minimum Necessary standards outlined in Section 4.14 above;
- b. Mandatory disclosures to the Department of Health and Human Services; and
- c. For the Legal and Public Policies purposes described in Section 4.9 above.

4.17 Notification in the Event of a Breach of PHI

Benefit staff will comply with the breach notification requirements of the HITECH Act, and any regulations promulgated thereunder. If Benefit Staff believe a Breach has occurred, they will present all relevant information to the Privacy Official for review.

- a. If the Privacy Official determines that a Breach of unsecured PHI has occurred, he or she will notify the individual(s) whose information has been breached as soon as practicable, but in no event more than 60 days after the breach is discovered. The notice shall be sent via first class mail to the individual's last known address, unless the individual agrees to receive it via electronic mail. If the last known address is insufficient or out-of-date, the notice will be provided by the alternate means specified in the HITECH regulations. The notice shall contain:
 - i. A description of the event, including date and date of discovery;
 - ii. A description of the *type* of information disclosed;
 - iii. Steps the individual should take to protect himself or herself;
 - iv. Steps the Plan is taking to investigate breach, mitigate harm and protect against additional breaches; and
 - v. Contact information
- b. If the Breach involves more than 500 individuals in a single jurisdiction, the Plan will notify the media in accordance with the HITECH rules.

- c. The Plan will maintain a log of all such Breaches and provide the required notice to the Secretary of Health and Human Services annually.

5. Procedures – Security

5.1 Risk Assessment and Management of EPHI

The Security Official will periodically identify (or re-identify) EPHI that it creates or receives from insurers, third party administrators and other Business Associates of the Plan. The Plan will confirm the storage media and location of such EPHI, assess potential risks and vulnerabilities to the integrity, confidentiality and availability of the EPHI and identify the safeguards in place to protect it. If there is a change in procedures or risk levels, Plan will adopt the necessary policies and procedures to reduce the risk to acceptable levels.

Notwithstanding the above, the Plan will conduct a risk assessment as soon as possible following the occurrence of:

- a. Changes to the HIPAA Security or Privacy Regulations
- b. New federal, state or local laws or regulations affecting the privacy or security of PHI
- c. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures
- d. A serious security violation, breach or incident.

5.2 General Work Rules

Benefits Staff work processes are intended to minimize the amount of EPHI maintained on PEEHIP systems and to protect any EPHI received, stored or transmitted in accordance with these Policies and Procedures. The following minimum practices shall be followed:

- a. Computers shall not be left unattended without locking them;
- b. Access to shared drives containing EPHI shall be limited to Benefits Staff;
- c. EPHI shall be downloaded and stored only if necessary for Plan administration purposes;
- d. Benefit Staff shall comply with the Information Security Policies adopted by the PEEHIP IT department.

5.3 Business Associate Agreements

Benefits Staff may disclose EPHI to a Business Associate and/or permit a Business Associate to create, receive, manage or use EPHI on behalf of the Plan only if a Business Associate Agreement that reflects the requirements of the Privacy Rule and the Security Rule has been fully executed by the Plan and the Business Associate.

6. Procedures – Individual Rights

6.1 Right to Accounting of PHI Disclosures

- a. An individual (or his or her properly designated representative) may request an accounting of disclosures of such individual's PHI made by the Plan. If so requested, Benefit Staff shall provide such individual or such designated representative with an accounting of disclosures of the individual's PHI made by the Plan during the six years prior to the date on which the accounting is requested, or for such lesser time specified by the individual. Notwithstanding the foregoing, such accounting need not include any disclosures of PHI made:
 - i To carry out treatment, payment or health plan operations;
 - ii To the individual regarding his or her own PHI;
 - iii To persons involved in the care of the individual or the payment for such care;
 - iv Pursuant to an authorization;
 - v For national security or intelligence purposes;
 - vi Pursuant to an authorization;
 - vii As part of a mandatory disclosure to DHHS;
 - viii To notify appropriate persons of the individual's location, general condition or death; or
 - ix Prior to the compliance date of May 16, 2003
- b. An accounting made pursuant to this paragraph shall include:
 - i The date of the disclosure;
 - ii The name (and if known, the address) of the entity or person to whom the disclosure was made;
 - iii A brief description of the PHI disclosed; and
 - iv A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
- c. The accounting will be provided no later than 60 days from the receipt of the request.
- d. If an individual requests more than one accounting within a 12-month period, the Plan shall impose a reasonable charge for each subsequent accounting, which charge shall be based on the cost of providing the accounting.

- e. The individual (or his or her authorized representative) shall make any request for an accounting of disclosures of PHI in writing to the contact person specified in the Plan's Notice of Privacy Practices.
- f. A record of all requests shall be maintained, and shall include the date of the request, and its disposition. See Section 8.

6.2 Right to Review and Copy PHI in Designated Record Set

- a. An individual (or his or her properly designated representative) may review and copy any PHI contained in a Designated Record Set, other than the following:
 - i Information compiled in anticipation of or for use in a legal action such as a civil or criminal law suit or an administrative action or proceeding;
 - ii Psychotherapy notes; and
 - iii Any other health information that is not subject to the individual's access rights under HIPAA.
- b. The Plan shall respond to the request for review within 30 days after receiving the request; provided, however, that if the relevant information is not readily available (e.g., because it is stored off-site or has been archived), the Plan shall respond within 60 days from receipt of the request. The Plan may extend either such deadline for another 30 days, by informing the individual of the need and reason for the extension of the initial period, and the date by which a response will be provided. If the request is denied, the Plan shall inform the individual, in writing, of the reason for the denial.
- c. To the extent that the Plan is required to provide access by an individual to his or her PHI, the documents shall be made available in the format requested by the individual, if it may be produced readily in such format. If it is not readily available in that format, it will be provided in a legible hard copy form or such other form or format as agreed to between the Plan and individual. The Plan may provide a summary of the requested PHI, in lieu of providing access to the PHI, or may provide an explanation of the PHI, if the individual agrees in advance to receive the summary or explanation. The individual must also agree in advance to any fees imposed for the preparation of the summary or explanation and/or for postage and copying charges.
- d. If an individual is denied partial access to PHI in a Designated Record Set, the Plan shall, to the extent possible, give him or her access to any other PHI that has been requested and for which there are no grounds for denial of access. To the extent access is denied, the Plan shall provide the individual (or his or her personal representative) with a written denial setting forth the basis for the denial, a statement of any review rights (including an explanation of how to exercise those rights), and an explanation of how the individual may complain to the Plan or to the Secretary of Health & Human Services regarding the denial. Such explanation shall include the name or title, and telephone number of the contact person specified in the Plan's Notice of Privacy Practices.

- e. Grounds for Denial of Access to PHI.
 - i. Unreviewable grounds. The Plan may deny an individual's request for access to PHI in the following circumstances:
 - The PHI is excepted from the individual's access rights, pursuant to the HIPAA regulations;
 - The PHI is contained in records that are subject to the Privacy Act of 1974 (5 U.S.C. §552a), if denial would meet the requirements of that law; or
 - The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
 - ii. Reviewable Grounds. The Plan may deny an individual access, provided the individual is given the right to have such denial reviewed, if a licensed health care professional has determined that such access is reasonably likely to endanger the life or physical safety of, or to cause substantial harm to, the individual or another person. If an individual requests a review of a decision to deny access, the Plan shall refer the request to a designated licensed health care professional who was not directly involved in the denial. The Plan shall promptly provide the individual with written notice of the determination and shall take any other action required by HIPAA to carry out the determination.

An individual (or personal representative) seeking access to PHI must file a written request with the contact person identified in the Plan's Notice of Privacy Practices. If the Plan does not maintain the PHI that is the subject of the request, but the Plan knows where the requested information is maintained, it will inform the individual where to direct the request for access.

- f. Benefit Staff shall take the following additional administrative steps in connection with this procedure:
 - i. Identify the information that is in a Designated Record Set that includes PHI (see Section 3 for a definition of Designated Record Set);
 - ii. Identify the persons or offices responsible for receiving and processing requests for access by individuals;
 - iii. Determine what information in the Designated Record Set a business associate holds, and how that information can be requested from the business associate;
 - iv. Keep all Designated Record Sets separate from employment-related documents and personnel files; and
 - v. Maintain a record of all requests, including the date the request was received and its disposition.

6.3 Right to Amend PHI in a Designated Record Set

- a. An individual has the right to request that the Plan amend his or her PHI that is held in a Designated Record Set for as long as the PHI is maintained in the Designated

Record Set; provided, however, that the Plan may deny the individual's request for amendment if the relevant PHI:

- i was not created by the Plan (except as otherwise provided by the regulations),
 - ii is not part of the Designated Record Set relating to the individual,
 - iii is not available for inspection by the individual under Section 6.2 above, or
 - iv is already accurate and complete.
- b. The Plan shall have 60 days after receiving the request during which to respond. A 30-day extension shall be permitted if the Plan is unable to comply with the request within the initial deadline, provided that notice of the need for the extension is provided to the individual within the initial deadline. Such notice must set forth the reason for the extension and the date by which a response will be provided.
- c. If the Plan accepts the requested amendments to PHI, it shall amend the individual's records accordingly. The Plan shall also inform the individual of the amendment and shall request his or her agreement to notify other relevant parties to whom the amendment must be communicated.
- d. If the Plan rejects the requested amendment (in whole or in part), it shall provide the individual with written notice of the denial that explains:
- i The basis for denial;
 - ii The individual's right to submit a written statement disagreeing with the denial and how to submit such a statement;
 - iii That, if the individual does not submit a statement of disagreement, he or she may request that the Plan send his or her request for amendment and the related denial along with any future disclosures of the relevant PHI; and
 - iv How the individual may file a complaint with the Plan or the Secretary of the U.S. Department of Health and Human Services (including the name or title and telephone number of the privacy contact specified in the Plan's Notice of Privacy Practices).

The Plan may reasonably limit the length of a statement of disagreement. Furthermore, the Plan may prepare a written rebuttal to a statement of disagreement, in which case, a copy of such rebuttal will be provided to the individual. If the individual does not submit a written statement of disagreement, the Plan need not include his or her request for amendment and its denial with any subsequent disclosure of the PHI only if requested by the individual.

- e. If the Plan has been informed by another entity of an amendment to an individual's PHI, it shall amend the PHI in its own records accordingly.
- f. Any request for amendment of PHI must be submitted by the individual or his or her authorized representative in writing, addressed to the Benefit Staff employee responsible for PHI who will forward it to the Privacy Official.

- g. Benefit Staff shall maintain a record of all requests for amendments, including the date the request was received and its disposition. See Section 8.1.

6.4 Right to Request Restrictions on Use and Disclosure of PHI

- a. An individual may request, in writing to the Privacy Official, that the Plan restrict:
 - i the use or disclosure of his or her PHI by the Plan for treatment, payment or health care operations,
 - ii the disclosure of PHI where otherwise permissible to his or her family members, other relatives, personal representatives or other identified persons who are involved in or responsible for payment for the individual's care, or
 - iii the disclosure of PHI where otherwise permissible for purposes of notifying a family member, personal representative or other designated individual of the individual's location, condition or death.
- b. The Plan will comply with the requested restriction if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes) and (2) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.
- c. If the Plan agrees to the individual's requested restrictions, the Plan may not use or disclose PHI in violation of the restrictions, except as may be necessary in the event that the individual needs emergency medical treatment, in which case the PHI may be disclosed to the health care provider, but the Plan shall request that the provider not further use or disclose the PHI.
- d. A restriction of PHI agreed to by the Plan will not be effective to prevent any use or disclosure that is permitted or required under the HIPAA regulations in the following situations:
 - i required to permit the DHHS to investigate or determine the Plan's compliance with HIPAA;
 - ii permitted to be made to family members, relatives or close personal friends, where the individual had the opportunity to approve or object to the disclosure; or
 - iii required by law or in connection with public health activities.
- e. The Plan may terminate any agreement to restrict the use or disclosure of PHI if:
 - i the individual requests or agrees to such termination, in writing;
 - ii the individual orally agrees to the termination, and such oral request is documented in the Plan records; or
 - iii the Plan informs the individual that it is terminating its agreement to the restriction. The termination of the agreement shall apply only to PHI created or received after the individual is notified of the termination.

- f. Benefit Staff shall maintain a record of all requests for amendments, including the date the request was received and its disposition. See Section 8.1.

6.5 Right to Request Confidential Communications

- a. An individual may request, in writing to the Privacy Official, that the individual receive communications of PHI from the Plans by alternative means or at alternative locations. The Plan will accommodate reasonable requests to receive confidential communications.
- b. The request must specify information as to how payment, if any will be handled and specification of the alternate address or means of communication.

6.6 Role of Business Associates

To the extent PHI is held by the Plan's third party administrators who are Business Associates, the Plan has delegated the authority to respond to requests in connection with individual rights to these Business Associates. The Privacy Official is responsible for monitoring compliance with these Policies and for working with the Business Associates regarding any suspected violations of the Policies.

7. Verification of Identity

7.1 General Requirements

Benefit Staff must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. In all cases, copy the documentation provided. Retain it with a record of the request, the date the request was received, and its disposition.

7.2 Verification of Identity and Authority

The identity of any person or entity requesting PHI and the authority of such person or entity to have access to such information must be verified prior to disclosure of the PHI.

- a. Documentation, statements and/or representation (oral or written) should be collected when such documentation, statements and/or representations are a condition of the disclosure.
- b. If the identity of the requestor is not personally known to Benefit Staff:
 - i. Request a form of identification from the individual. Benefit Staff may rely on a valid driver's license, passport or other photo identification issued by a government agency.
 - ii. Verify that the identification matches the identity of the individual requesting access to the PHI. If there is any doubt as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
 - iii. The requestor must:
 - a) Provide his or her relationship to the Individual who is the subject of the PHI;
 - b) Have a general knowledge of the information they are requesting; and know at least two of the following pieces of information about the Individual who is the subject of the PHI:
 1. Social Security number or Employee ID number;
 2. Birth date;
 3. Home address;
 4. Place of employment
- c. If the requestor requests PHI over the telephone, the requestor must: satisfy the requirements outlined in section b.iii, above.
- d. *Request Made by Personal Representative.* When a personal representative requests access to an individual's PHI, request a copy of a valid authorization form or power of attorney (the power must include the power to make medical decisions).

If there are any questions about the validity of this document, seek review by the Privacy Official.

- e. *Request Made by Public Official.* If a public official requests access to PHI, and if the request is for one of the purposes listed in Section 4.8 or 4.9, the following steps should be followed to verify the official's identity and authority:
 - i. If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status.
 - ii. If the request is in writing, verify that the request is on the appropriate government letterhead.
 - iii. If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
 - iv. Request a written statement of legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Official.
 - v. Obtain approval for the disclosure from the Privacy Official.
- f. Benefit Staff must exercise professional judgment in making disclosures of PHI. In the event Benefit Staff is uncertain whether the requestor is acting in good faith, the member should consult with the Privacy Official prior to determining whether disclosure of PHI is appropriate.

7.3 Document Retention

In all cases, Benefit Staff shall copy all documentation provided. Copies of such documentation shall be retained with a record of the request, the date the request was received, and its disposition.

8. Document Retention

8.1 Retention Period

The Plan shall retain the documents listed below either electronically or on paper for six years from the later of the date of creation or the date last in effect:

- a. The HIPAA policies, procedures and privacy notices used in connection with the operation and administration of the Plans;
- b. Individual authorizations and designations of personal representatives;
- c. Documentation relating to individual rights under HIPAA;
- d. When a disclosure of PHI as outlined in Section 4.11 is made:
 - i. The date of disclosure
 - ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - iii. A brief description of the PHI disclosed;
 - iv. A brief statement of the purpose of the disclosure; and
 - v. Any other documentation required under these Procedures.
- f. Any individual complaints regarding HIPAA compliance and their outcomes, as well as any sanctions for violation of HIPAA's requirements;
- g. The disclosure log described in Section 4.16;
- h. Business associate agreements;
- i. HIPAA Training materials and attendance logs; and
- j. PEEHIP's certifications to the Plans regarding Plan amendments, compliance and security procedures

All other Plan records not listed above shall be maintained in accordance with applicable Plan policies consistent with any state or federal laws.

8.2 Electronic Records Retention

Electronic retention of such documents shall be further subject to the following:

- a. The documents shall be maintained in reasonable order, in a safe and accessible location where they are capable of being readily examined;
- b. The document retention system shall have reasonable procedures that are aimed at ensuring the accuracy, integrity and reliability of the records;
- c. The electronically maintained records shall be readily transferable to paper and must be readily accessible, in order to enable PEEHIP to satisfy the applicable reporting and disclosure requirements of ERISA, HIPAA and the Internal Revenue Code.

- d. Records management procedures shall be implemented that adequately ensures the easy identification of Plan documents, and that ensure that secure storage and electronic and/or paper backup copies will be maintained.

8.3 Business Associate Agreements

All business associates shall execute business associate agreements with the Plan in which they agree to comply with these Policies and Procedures in their work with the Plans. Upon the termination of a business associate agreement, PHI will be returned to PEEHIP, destroyed, or retained by the business associate, as provided in the business associate agreement.

8.4 Employment File

No forms or PHI shall be stored in the individual's employment file.

8.5 Storage

- a. PEEHIP on behalf of the Plan may contract with commercial off-site storage facilities to store, control and protect inactive PHI and other records outlined in this Section 8 ("Protected Records"). To the extent that they have access to the Protected Records, the commercial off-site storage facilities must agree to maintain the confidentiality of the Protected Records and, if applicable, will be required to execute a Business Associate Agreement.
- b. Off-site storage facilities are to be in secure locations that safeguard the records from the following:
 - i. Ordinary hazards, such as fire, water, mildew, rodents and insects;
 - ii. Man-made hazards, such as theft, accidental loss and sabotage;
 - iii. Disasters, such as fire, flood earthquakes, hurricanes, wind and explosions; and
 - iv. Unauthorized use, disclosure and destruction.
- c. Off-site storage facilities are to provide proper vault storage with temperature and humidity controls for electronic, audio/video and microfilm storage (as applicable).
- d. Protected records stored in boxes must be adequately labeled and include the following information to facilitate their reference, review and destruction:
 - i. Dates included;
 - ii. Originating Plan department;
 - iii. Type of media;
 - iv. Description of documents contained in the box; and
 - v. Contact name and telephone number.

- e. The Plan will select appropriate media and systems for storing Protected Records in order to:
 - i. Permit easy retrieval in a timely fashion;
 - ii. Facilitate distinction between Protected Records and other Plan records; and
 - iii. Retain records in a usable format.

8.6 Records Destruction

- a. Protected Records that have satisfied their legal, fiscal, administrative and archival requirements may be destroyed if the retention period set forth in Section 8.1 has been satisfied.
- b. Protected Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the records may be destroyed as described in paragraph a, above.
- c. Protected Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information no longer recognizable as Protected Records. Approved methods to destroy Protected Records include, but are not limited to, recycling, burning, pulping, pulverizing and magnetizing. The destruction of records must be approved in writing by the Privacy Official or designee or prior to the destruction of the records. Protected Records cannot be placed in trash receptacles unless the records are rendered no longer recognizable as Protected Records.

9. Distribution of Privacy Notice

9.1 Timing

- a. The Plan distributed the initial Notice of Privacy Practices to covered individuals effective April 14, 2003.
- b. Benefit Staff shall provide a copy of the Notice of Privacy Practices to individuals covered under the Plan at the following times:
 - i. When the individual first enrolls in the Plan; and
 - ii. Within 60 days of a material revision to the Notice.
- c. At least once every three years, Benefit Staff shall notify covered individuals of the availability of the Notice, and how to obtain a copy.

9.2 Distribution by Mail

The Notice must be provided to the covered individual in person, by mail or by e-mail. It cannot simply be posted on a bulletin board or on a web site, or made available only upon request.

- a. Regular mail is acceptable if the Notice is mailed.
- b. If e-mail is used, the individual must agree to electronic delivery, and not have withdrawn the agreement. If the e-mail transmission fails, a paper copy of the notice must be provided to the individual. An individual who has agreed to electronic delivery of the Notice has the right to request a paper copy of it.
- c. The Notice may be provided only to the covered individual; a separate notice does not have to be provided to the covered individual's dependents.
- d. The Notice may be included with other materials, such as the Plan's enrollment materials. However, the Notice shall *not* be combined in a single document with an authorization form.

9.3 PEEHIP Website

In addition to the delivery of the Notice described above, the Plan maintains a web site that provides information about benefits or services available under the Plan; the Notice is posted on and electronically available through that [web site](#).

10. Privacy Official

10.1 Role

The Privacy Official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to PEEHIP's policies and procedures covering the privacy of, and access to, health information in compliance with federal and state laws and the PEEHIP's information privacy policies relating to group health plans covering the PEEHIP's employees and their dependents.

10.2 Duties

The Privacy Official shall

- a. Provide development guidance and assist in the identification, implementation, and maintenance of Plan information on privacy policies and procedures in coordination with Benefit Staff and legal counsel.
- b. Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities.
- c. Ensure that the Plan has and maintains appropriate privacy authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.
- d. Oversee, direct, deliver, or ensure delivery of initial and ongoing privacy training and orientation to relevant employees, business associates and other appropriate third parties.
- e. Participate in the development, implementation, and ongoing compliance monitoring of all business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- f. Establish a mechanism to track access to protected health information, within the purview of the Plan and as required by law and to allow qualified individuals to review or receive a report on such activity.
- g. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Plan's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- h. Ensure compliance with privacy policies and consistent application of sanctions for failure to comply with privacy policies.
- i. Initiate, facilitate and promote activities to foster information privacy awareness within the PEEHIP.
- j. Review all system-related information security plans to ensure alignment between security and privacy practices.

- k. Work with all Benefit Staff to ensure full coordination and cooperation under the Plan's policies and procedures and legal requirements.
- l. Maintain current knowledge of applicable federal and state privacy laws, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- m. Cooperate in any compliance reviews or investigations.

11. Security Official

11.1 Role

The Security Official oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to PEEHIP's policies and procedures covering the security of, and access to, health information maintained or transmitted in electronic form in compliance with federal and state laws and the PEEHIP's information privacy policies relating to group health plans covering the PEEHIP's employees and their dependents.

11.2 Duties

The duties of the HIPAA Security Officer shall include, but not be limited to:

- a. Coordinating with the appropriate IT staff the development and implementation of the Plan's policies and procedures for assuring the confidentiality, integrity, and availability of electronic protected health information to meet the information security requirements of HIPAA. This also includes developing other administrative, technical and physical safeguards to ensure the security of electronic protected health information.
- b. Confirming adoption of necessary amendments to plan documents and business associate agreements as required by HIPAA.
- c. Monitoring the PEEHIP's compliance with applicable HIPAA information security laws and regulations, monitoring compliance with the PEEHIP's HIPAA information security policies and procedures among applicable employees and other third parties, and reporting security issues to appropriate managers or administrators; perform security audits and risk assessments of ongoing system activities.
- d. Receiving reports from all sources regarding Business Associates' compliance with applicable security policies and terminating contracts with Business Associates when necessary to ensure the PEEHIP's compliance with the HIPAA security requirements;
- e. Leading information security awareness and training initiatives to educate appropriate employees and other third parties who are likely to have access to electronic protected health information about information security risks and provide periodic updates;
- f. Suggesting amendments to the PEEHIP's security policies and any forms, contracts or other documents affecting the privacy of electronic PHI;
- g. Performing any other functions assigned to the HIPAAA Security Officer pursuant to the PEEHIP's written privacy and security policies and procedures; and

- h. Documenting in writing the actions taken in compliance with this designation, including reviewing and updating documentation as needed in response to changes affecting the security of electronic protected health information.
- i. Coordinating ongoing review of existing information security programs to ensure continuing integration of information security requirements with business strategies and requirements and regulatory changes, and initiating the development of new programs as the need arises or suggesting amendments to the PEEHIP's security policies and any forms, contracts or other documents, as appropriate, in response to environmental or operational changes affecting the security of electronic protected health information.

12. General Provisions

12.1 Complaints

- a. Any individual who is covered by the Plan may file a complaint with the Privacy Official (or his or her delegate specified in the Notice of Privacy Practices) regarding alleged noncompliance with the requirements of HIPAA and the HIPAA Policies and Procedures maintained by the Plan. The Plan shall keep written records of all complaints (whether oral or written), as well as records of their disposition.
- b. The Privacy Official (or his or her designee) shall investigate any such complaint in accordance with reasonable procedures, and shall mitigate, to the extent practicable, any harmful effect that is known to have resulted from a HIPAA violation. A written explanation of the disposition of any complaint shall be provided to the complainant within 30 days following receipt of the complaint. Neither the Plan nor PEEHIP shall retaliate in any manner against any complainant for filing a complaint.
- c. In order not to compromise the integrity of an investigation, Benefit Staff shall not conduct independent investigations as such investigations may involve complex legal issues.

12.2 Sanctions

- a. Benefits Staff who violate the policies and procedures regarding the use and disclosure of protected health information shall be subject to sanctions and penalties, up to and including, termination of employment.
- b. The Privacy Official is responsible for determining if an employee failed to comply with the Plan's Privacy Policies and Procedures for HIPAA Compliance. If the Privacy Official determines that an employee has failed to comply with these stated policies and procedures, the Privacy Official, in conjunction with appropriate management and PEEHIP Human Resources representatives, will determine the appropriate sanction.
- c. The severity of sanction applied will vary depending on the seriousness of the violation, whether the action was intentional and whether action indicates a pattern of practice of improper use or disclosure of PHI, and other similar factors.
- d. All sanctions imposed will be documented and retained by the Privacy Official and Human Resources for a period of six years from the date of its creation or the date when it was last in effect, whichever is later.
- e. If the Privacy Official determines that the employee disclosed PHI or failed to follow these procedures in pursuit of one of the following actions, then no sanction will be imposed:
 - i. The employee filed a complaint with DHHS pursuant to 45 CFR §16.306.
 - ii. The employee testified, assisted, or participated in an investigation, compliance review, proceeding, or hearing under the HIPAA administrative simplification requirements.

- iii. The employee opposed any act made unlawful by the HIPAA administrative simplification requirements; provided the employee had a good faith belief that the act opposed was unlawful, and the manner of the opposition was reasonable and did not involve a disclosure of PHI in violation of the requirements.

12.3 Mitigation

HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. If Benefit Staff becomes aware of a disclosure of PHI that is not in compliance with these policies and procedures, he or she will immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

13. Forms and Templates

DESIGNATION OF HIPAA PRIVACY OFFICER

Designation:

The following individual shall be designated as the PEEHIP's Privacy Officer:

Name: Donna Joyner, CPA

Title: PEEHIP Director

Address: 201 South Union Street, Montgomery, AL 36104-0001

Telephone: 334-517-7151

Fax: 877-517-0021

E-mail: Donna.Joyner@rsa-al.gov

Duties:

The duties of the HIPAA Privacy Officer shall include, but not be limited to:

1. Developing and implementing programs designed to train employees who are involved in the PEEHIP's privacy policies with respect to group health plans;
2. Receiving reports from employees, volunteers, and other individuals concerning violations of the PEEHIP's privacy policies with respect to group health plans;
3. Investigating and remedying any violations of the PEEHIP's privacy policies, including administering sanctions against employees, where appropriate, for violations of the PEEHIP's privacy policies with respect to group health plans;
4. Suggesting amendments to the PEEHIP's privacy policies and any forms, contracts or other documents affecting the privacy of PHI;
5. Receiving reports from all sources regarding Business Associates' compliance with applicable privacy policies and terminating contracts with Business Associates when necessary to ensure the PEEHIP's compliance with the HIPAA privacy requirements;
6. Cooperating with any audits of the Secretary of the Department of Health and Human Services or any other governmental organization concerning the PEEHIP's compliance with state or federal privacy laws or regulations;
7. Notifying individuals when their health information has been used or disclosed in violation of the PEEHIP's privacy policies with respect to group health plans;

8. Accepting and forwarding to appropriate individuals any legal complaints served upon the HIPAA Privacy Officer;
9. Performing any other functions assigned to the HIPAA Privacy Officer pursuant to the PEEHIP's written privacy policies and procedures; and
10. Documenting in writing the actions taken in compliance with this designation.

The Privacy Officer may delegate tasks to Business Associates, where appropriate

Term:

The HIPAA Privacy Officer shall serve until removed by the PEEHIP or until he or she resigns from the position.

Effective as of May 10, 2012

Signature: Donna M. Gymer

DESIGNATION OF HIPAA SECURITY OFFICER

Designation:

The following individual shall be designated as the PEEHIP's Security Officer:

Name: Jessica Jones

Title: RSA Security Officer

Address: 201 South Union Street

Telephone: 1-334-517-7605

Fax: 1-334-517-7001

E-mail: Jessica.jones@rsa-al.gov

Duties:

The duties of the HIPAA Security Officer shall include, but not be limited to:

1. Developing, implementing, managing and enforcing policies and procedures to meet the information security requirements of HIPAA;
2. Ensuring ongoing integration of information security requirements with business strategies and requirements;
3. Ensuring that the access control, disaster recovery, business continuity, incident response and risk management needs of the covered health plans are addressed;
4. Confirming adoption of necessary amendments to plan documents and business associate agreements as required by HIPAA.
5. Receiving reports from all sources regarding Business Associates' compliance with applicable security policies and terminating contracts with Business Associates when necessary to ensure the PEEHIP's compliance with the HIPAA security requirements;
6. Leading information security awareness and training initiatives to educate workforce about information risks;
7. Suggesting amendments to the PEEHIP's security policies and any forms, contracts or other documents affecting the privacy of electronic PHI;
8. Working with vendors and other third parties to improve information security within the organization;
9. Performing any other functions assigned to the HIPAAA Security Officer pursuant to the PEEHIP's written privacy policies and procedures; and

10. Documenting in writing the actions taken in compliance with this designation.

The Security Officer may delegate tasks to Business Associates, where appropriate.

Term:

The Security Officer shall serve until removed by PEEHIP or until he or she resigns from the position.

Effective as of 5/10/12

Signature: Jessica Jones

CERTIFICATION OF RECEIPT OF HIPAA POLICIES AND PROCEDURES

PEEHIP provides medical, prescription drug and health care spending account benefits to eligible employees through the Plan. Staff members of PEEHIP and/or RSA may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of PEEHIP as Plan Sponsor, in connection with the administration of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations restrict the ability of PEEHIP and the Plan to use and disclose protected health information (“PHI”).

It is PEEHIP’s policy to comply fully with HIPAA’s requirements. To ensure compliance with this policy, PEEHIP has set forth policies and procedures in connection with the administration of the Plan and has distributed them to members of the PEEHIP staff and RSA staff who have access to PHI and must follow them.

Certification and Signature
I am an employee of PEEHIP or RSA who has access to Protected Health Information. I have received a copy of the PEEHIP Policies And Procedures Regarding the Use And Disclosure Of Protected Health Information. I have read and understand its provisions, and agree to abide by them. I understand that my failure to comply with these policies and procedures may result in the imposition of fines and penalties on PEEHIP and that I may be subject to sanctions and penalties, up to and including, termination of employment.
Employee’s Signature: _____ Date: ____ / ____ / ____

**USES AND DISCLOSURES TRACKING FORM
PUBLIC EDUCATION EMPLOYEES HEALTH INSURANCE PLAN**

Date of Disclosure (mm/dd/yy)	Individual who is the Subject of PHI		Recipient of PHI		Description of PHI	Purpose of Disclosure*
	Name	ID # or SSN	Name	Address		

* If the disclosure is pursuant to (1) an authorization by the employee, (2) a court order, or (3) in connection with law enforcement activities, indicate that here.

Note: This log should be maintained electronically so that it may be searched in order to respond to a request for an accounting of disclosures.

14. Privacy Notices

Health Insurance Portability and Accountability Act (HIPAA) Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Public Education Employees' Health Insurance Plan (the "Plan") considers personal information to be confidential. The Plan protects the privacy of that information in accordance with applicable privacy laws, as well as its own privacy policies.

The Plan is required by law to take reasonable steps to ensure the privacy of your health information and to inform you about:

- the Plan's uses and disclosures of your health information
- your privacy rights with respect to your health information
- the Plan's obligations with respect to your health information
- a breach of your PHI
- your right to file a complaint with the Plan and to the Secretary of the U.S. Department of Health and Human Services
- the person or office to contact for further information about the Plan's privacy practices

Effective Date of Notice: This notice was effective as of September 23, 2013.

HOW THE PLAN USES AND DISCLOSES HEALTH INFORMATION

This section of the notice describes uses and disclosures that the Plan may make of your health information for certain purposes without first obtaining your permission as well as instances in which we may request your written permission to use or disclose your health information. The Plan also requires their business associates to protect the privacy of your health information through written agreements.

Uses and disclosures related to payment, health care operations and treatment. The Plan and its business associates may use your health information without your permission to carry out payment or health care operations. The Plan may also disclose health information to the Plan Sponsor, PEEHIP, for purposes related to payment or health care operations.

Payment includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, review for medical necessity and appropriateness of care and utilization review and preauthorizations). For example, the Plan may tell an insurer what percentage of a bill will be paid by the Plan.

Health care operations include but are not limited to underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts, disease management, case management, conducting or arrangement for medical review, legal services and auditing

functions, including fraud and abuse programs, business planning and development, business management and general administrative activities. It also includes quality assessment and improvement and reviewing competence or qualifications of health care professionals. For example, the Plan may use medical benefit claims information to conduct a review of the accuracy of how benefit claims are being paid. However, in no event will Benefit Staff use PHI that is genetic information for underwriting purposes.

The Plan will only disclose the minimum information necessary with respect to the amount of health information used or disclosed for these purposes. In other words, only information relating to the task being performed will be used or disclosed. Information not required for the task will not be used or disclosed.

The Plan may also contact you to provide information about treatment alternatives or other health-related benefits and services that may be of interest to you

Other uses and disclosures that do not require your written authorization. The Plan may disclose your health information to persons and entities that provide services to the Plan and assure the Plan they will protect the information or if it:

- Constitutes summary health information and is used only for modifying, amending or terminating a group health plan or obtaining premium bids from health plans providing coverage under the group health plan
- Constitutes de-identified information
- Relates to workers' compensation programs
- Is for judicial and administrative proceedings
- Is about decedents
- Is for law enforcement purposes
- Is for public health activities
- Is for health oversight activities
- Is about victims of abuse, neglect or domestic violence
- Is for cadaveric organ, eye or tissue donation purposes
- Is for certain limited research purposes
- Is to avert a serious threat to health or safety
- Is for specialized government functions
- Is for limited marketing activities

Additional disclosures to others without your written authorization. The Plan may disclose your health information to a relative, a friend or any other person you identify, provided the information is directly relevant to that person's involvement with your health care or payment for that care. For example, the Plan may confirm whether or not a claim has been received and paid. You have the right to request that this kind of disclosure be limited or stopped by contacting the Plan's Privacy Official.

Uses and Disclosures Requiring Your Written Authorization. In all situations other than those described above, the Plan will ask for your written authorization before using or disclosing your health information. If you have given the Plan an authorization, you may revoke it at any

time, if the Plan has not already acted on it. If you have questions regarding authorizations, contact the Plan's Privacy Official.

YOUR PRIVACY RIGHTS

This section of the notice describes your rights with respect to your health information and a brief description of how you may exercise these rights. To exercise your rights, you must contact the Plan's Privacy Official at 877-517-0020.

Restrict Uses and Disclosures

You have the right to request that the Plan restricts uses and disclosure of your health information for activities related to payment, health care operations and treatment. The Plan will consider, but may not agree to, such requests.

Alternative Communication

The Plan will accommodate reasonable requests to communicate with you at a certain location or in a certain way. For example, if you are covered as an adult dependent, you may want the Plan to send health information to a different address than that of the Employee. The Plan must accommodate your reasonable request to receive communication of PHI by alternative means or at alternative locations, if you clearly state that the disclosure of all or part of the information through normal processes could endanger you in some way

Copy of Health Information

You have a right to obtain a copy of health information that is contained in a "designated record set" – records used in making enrollment, payment, claims adjudication, and other decisions. The Plan may provide you with a summary of the health information if you agree in advance to the summary. You may also be asked to pay a fee of \$1.00 per page based on the Plan's copying, mailing, and other preparation costs.

Amend Health Information

You have the right to request an amendment to health information that is in a "designated record set." The Plan may deny your request to amend your health information if the Plan did not create the health information, if the information is not part of the Plan's records, if the information was not available for inspection, or the information is not accurate and complete.

Right to access electronic records

You may request access to electronic copies of your PHI, or you may request in writing or electronically that another person receive an electronic copy of these records. The electronic PHI will be provided in a mutually agreed-upon format, and you may be charged for the cost of any electronic media (such as a USB flash drive) used to provide a copy of the electronic PHI.

List of Certain Disclosures

You have the right to receive a list of certain disclosures of your health information. The Plan or its business associates will provide you with one free accounting each year. For subsequent requests, you may be charged a reasonable fee.

Right to A Copy of Privacy Notice

You have the right to receive a paper copy of this notice upon request, even if you agreed to receive the notice electronically.

Complaints

You may complain to the Plan or the Secretary of HHS if you believe your privacy rights have been violated. You will not be penalized for filing a complaint.

THE PLAN'S RESPONSIBILITIES

The Plan is required by a federal law to keep your health information private, to give you notice of the Plan's legal duties and privacy practices, and to follow the terms of the notice currently in effect.

THIS NOTICE IS SUBJECT TO CHANGE

The terms of this notice and the Plan's privacy policies may be changed at any time. If changes are made, the new terms and policies will then apply to all health information maintained by the Plan. If any material changes are made, the Plan will distribute a new notice to participants and beneficiaries.

YOUR QUESTIONS AND COMMENTS

If you have questions regarding this notice, please contact PEEHIP's Privacy Official at 877-517-0020.

15. BUSINESS ASSOCIATE DATA SECURITY POLICY

The Public Education Employees' Health Insurance Plan (the "Plan") considers personal information to be confidential. The Plan protects the privacy of personal information in accordance with applicable privacy laws. The Plan is required by law to take reasonable steps to ensure the privacy of our members' healthcare information in accordance with the Health Information Portability and Accountability Act (HIPAA). With the recent addition of the Health Information Technology for Economic and Clinical Health (**HITECH**) Act, (enacted as part of the American Recovery and Reinvestment Act of 2009) it is imperative that PEEHIP maintain reasonable oversight over protected health information that it shares with its business associates. As defined by HIPAA, a business associate is any organization or person working in association with, or providing services to, a covered entity (PEEHIP) who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).

Policy:

PEEHIP shall ensure that all of its business associate agreements (BAA's) meet current regulation requirements and are reviewed annually. Any addendum(s) to a BAA that are required by any current or proposed HIPAA or HITECH statutes or regulations shall be entered into within the time frame mandated pursuant to such statutes or regulations.

As a continued or future business associate of PEEHIP, business associates must provide adequate documentation stating they are in compliance with current HIPAA Security and Privacy rules. Documentation must consist of, at a minimum, one of the following:

- **External HIPAA Audit Certification** – Audit must have been conducted by a credible third party audit firm specializing in HIPAA audits within the last two years or within the last 12 months of a significant change or enacted legislation. Summary must state if business associate meets HIPAA compliance.
- **Detailed Internal Controls Documentation** – Policy and audit documentation demonstrating full compliance with each of the standards outlined in the HIPAA Security and Privacy regulations to be reviewed and approved by RSA's security and privacy officials. The HIPAA Privacy and Security Rules are defined in 45 CFR 164 Subparts A and C for Security and Privacy. The HIPAA Security Rule Implementation Standards are outlined in 45 CFR 164.308 - 164.316.
- **Statement of Controls Audit** - At minimum a SOC 1 report is required but an SOC 2 Type 2 certification is preferred as it evolves to become the standard certification for validating confidentiality, availability, and processing integrity within an organization.

The SOC 2 audit is a replacement for SAS70 Type II. A SSAE 16 SOC 1 generally covers the financial side of the controls audit; therefore, PEEHIP prefers a SOC 2. Audit documentation must depict controls over systems, operations, and facilities where "PEEHIP" data will be processed and stored for the duration of the contract. A SOC 3 Report is considered acceptable documentation as it can be freely distributed (general

*use) and only reported on if the entity has achieved the Trust Services criteria **based upon the SOC 2 audit.***

If a current business associate fails to comply with this Policy, PEEHIP shall have the right, at PEEHIP's sole discretion, to request one of the above defined audits to be completed and results obtained within 90 days from the date such business associate receives written notice of noncompliance from PEEHIP. In such event, the audited party will be solely responsible for all expenses incurred by the parties during the audit, including without limitation, all payment due to the audit firm. Should such business associate not obtain the audit within the 90 days allowed, PEEHIP shall have the right, in its sole discretion, to terminate its relationship with the business associate. In no event shall a new business associate relationship be created with a party not in compliance with this policy.