**THE EMPLOYEES RETIREMENT SYSTEM OF TEXAS**
**TEXAS EMPLOYEES GROUP BENEFITS PROGRAM**
**PRIVACY POLICIES AND PROCEDURES**

## I. GENERAL PRINCIPLES

The Employees Retirement System of Texas administers the Texas Employees Group Benefits Program ("GBP") on behalf of employees and retirees of the State of Texas and certain Texas higher education institutions. The GBP (also referred to as "the health plan") is committed to protecting the privacy of program participants' protected health information ("PHI") in accordance with federal and state regulations consistent with the delivery of a quality health plan, effective management of health care operations, and payment of covered health care services. These health plan policies and procedures implement privacy protections in accordance with the Health Insurance Portability and Accountability Act of 1996, Privacy Regulations ("Privacy Regulations") promulgated by the Secretary of the U. S. Department of Health and Human Services ("Secretary of HHS") at 45 C.F.R. Subtitle A, Subchapter C and the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A of the American Recovery and Reinvestment Act ("HITECH").

## II. PURPOSE AND SCOPE

The purpose and scope of these policies and procedures is to delineate the privacy policies of the health plan and the procedures for implementing the policies to achieve compliance with the Privacy Regulations.

## III. PROTECTED HEALTH INFORMATION DEFINITION

PHI is any individually identifiable health information that is transmitted or maintained in any form, including genetic and demographic information collected from an individual, and:

A. Is created or received by a health care provider, health plan, or health care clearinghouse; and

B. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   1. That identifies the individual; or

   2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI includes information of persons living or deceased, including genetic information.

## IV. DESIGNATION OF PRIVACY OFFICER

A. The Privacy Officer for the health plan is:
Nancy Lippa

B. The Privacy Officer has overall responsibility for administering the policies and procedures to assure compliance with the Privacy Regulations. Additionally, the Privacy Officer is the designated authority to receive and process: (i) complaints, (ii) requests for copies of PHI, (iii) requests for communications by alternative means or alternative locations (confidential communications), (iv) subpoenas and other requests from judicial authorities, and (v) other correspondence and matters related to the privacy of PHI.

C. Complaint Filing Procedures

The Privacy Officer is designated to receive complaints filed with the health plan regarding the health plan's privacy policies and procedures and its compliance with those privacy policies and procedures. Complaints must be filed in writing and directed to the Privacy Officer. The writing must contain a description of the complaint and an explanation of the circumstances surrounding the complaint. The health plan is not required to respond to complaints, but the Privacy Officer shall be responsible for documenting receipt of a complaint and any resolution thereof.

Complaints may also be filed with the Secretary of HHS. No retribution or negative action will be taken or tolerated because a health plan participant files a complaint with the health plan or the Secretary.

D. Business Associate Agreements

The Privacy Officer is responsible for ensuring that the health plan complies with the provisions of the HIPAA privacy rule regarding business associates, including the requirement that the health plan have a HIPAA-compliant business associate agreement in place with all business associates, and that all business associates have written contractual agreements in place with any subcontractor or vendor with whom it shares PHI in accordance with 45 C.F.R. § 164.314. The Privacy Officer shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and these policies and procedures.

## V. NOTICE OF PRIVACY PRACTICES - SYNOPSIS

A. Each employee will receive a Notice of Privacy Practices (the “Notice”) from the health plan. However, we have provided below a summary of some of the important points contained in the Notice.

B. The health plan generally uses and discloses PHI only in furtherance of providing the medical and/or dental benefits described in one of the health plan's specific benefit document(s), also referred to sometimes as the Master Benefit Plan Documents. The health plan uses and discloses the PHI to process requests for payment, to respond to eligibility and benefit inquiries from providers, and for other reasons related to the operation of the specific benefit plan (these reasons are described in the Notice as "health care operations"). The health plan contracts with business associates to perform various services or to perform certain specified functions, such as administration of claims, customer service support, utilization

management, subrogation, pharmacy benefit management, stop-loss insurance and other similar functions. The health plan utilizes these business associates to receive, create, maintain, use and disclose relevant PHI for the purposes of treatment, payment of health claims and health care operations.

C. The health plan requires each business associate to adopt the health plan's Privacy Policies and Procedures or a similar set of policies and procedures that meet the same objectives required by the Privacy Regulations and HITECH, including, but not limited to, notification of breach of unsecured PHI.

D. The health plan discloses PHI to the plan sponsor for the purpose of plan administration functions, including funding benefits and determining the health and viability of the health plan. The plan sponsor has certified that, among other actions, it has limited the access to PHI to relevant personnel and that PHI will not be used in any employment action or in connection with any other plan sponsor benefit.

E. Periodically the health plan requests proposals from third-party administrators, pharmacy benefit managers, insurance and stop-loss companies to ensure the viability of the health plan. In the course of developing proposals, occasionally specific PHI is required by these companies. The health plan assists in providing the required information in furtherance of its responsibility to maintain plan integrity and fiscal health. These companies are included in the health plan's business associates and, as such, will comply with the rules set forth in these policies and procedures for business associates.

F. The health plan may disclose PHI to various health care providers for the purpose of treatment, payment, for services to plan members, or in furtherance of disease management or other health care operations of the health plan.

G. The Notice will inform participants that the health plan will have access to PHI in connection with its plan administrative functions. The Notice will also provide a description of the health plan’s compliant procedures, the name and telephone number of the contact person for further information, and the date of the Notice. The Notice shall be placed on the health plan’s website. The Notice will also be individually delivered, as required by law. The health plan will also provide notice of availability of the Notice (or a copy of the Notice) at least once every three years in compliance with the HIPAA Privacy Regulations. Additionally, the health plan will prominently post any changes or revisions to the Notice on its website by the effective date of the material change to the privacy notice, or otherwise, provide information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the health plan.

## VI. RETENTION OF DOCUMENTATION

A. Documentation required by the Privacy Regulations shall be maintained for six (6) years from the date a document is created or the date when it was last in effect, whichever is later.

B. A database for retaining required documentation has been created. Required documentation shall be entered in the electronic database and retained for six (6) years from the date a document is created or the date when it was last in effect, whichever is later, beginning with the required compliance date of the Privacy Regulations. The Privacy Officer shall be responsible for assuring that relevant data is entered promptly and destroyed appropriately.

C. Where electronic copies are not available or actual practice requires paper copies of documents, the paper copies shall be securely maintained for the required six (6) years. The Privacy Officer shall maintain a list of documents that must be retained in paper form.

## VII. HEALTH PLAN PARTICIPANT PRIVACY RIGHTS

A. Policy

Health Plan Participants generally have the following rights:

1. The right to request restrictions on certain uses and disclosures of PHI. However, the health plan is not obligated to agree to a requested restriction.

2. The right to receive confidential communications of PHI, provided that the participant: (i) describes in writing the desired alternative location for, or alternative means of communication, and (ii) indicates in the writing that the disclosure of the PHI in a manner inconsistent with the request could endanger the individual.

3. The right to inspect and obtain a paper or electronic copy of most PHI contained in a designated record set. If an electronic copy of the PHI is requested, a copy in the electronic form and format requested will be produced if readily producible in such form and format; otherwise, an agreement with the participant will be made as to an agreed upon readable electronic format.

4. The right to request amendment of PHI; however, the health plan is not obligated to agree to a requested amendment.

5. The right to receive an accounting or audit of electronic disclosures of PHI made within the past three years.

6. The right to obtain a paper copy of the Notice of Privacy Practices even if previously agreeing to receive such notice electronically.

7. The right to receive notification if unsecured PHI has been breached. A breach means the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under HIPAA that compromises the security or privacy of PHI.

8. The right to ask a health care provider to withhold PHI from the health plan if the participant paid in full for the medical care and the disclosure is not otherwise required by law. The request for restriction will only be applicable to that particular service, and each service thereafter will require a separate request to the participant's health care provider for restriction of disclosure.

B. Procedures

1. Participant Requested Restrictions

a. The participant must submit all restriction requests in writing to the Privacy Officer.

b. The health plan shall monitor and maintain a log of requests for restrictions on uses and disclosures of PHI. The Privacy Officer shall be responsible for determining the reasonableness of all requests, and for conveying in writing the health plan's decision on such requests.

c. A log shall be maintained of such requests and the disposition of such requests.

d. The participant shall be notified of the decision concerning the requested restriction.

e. The Privacy Officer is not obligated to agree to such requests but shall include in the consideration of a request the impact and feasibility of such request in view of difficulties or disruptions that may result on plan administration.

f. If the Privacy Officer agrees to a request for restriction, the Privacy Officer will:

(i) Document such restriction and maintain it in accordance with the Retention of Documentation policy and procedures referenced in Article VI above; and

(ii) Take the appropriate and necessary steps to ensure that the health plan complies with the restriction.

g. Even if the health plan has agreed to a restriction, the health plan may disclose the restricted PHI to a health care provider for emergency treatment of the individual.

h. The Privacy Officer may terminate a restriction, if:

(i) The participant requests or agrees in writing to terminate the restriction; or

(ii) The Privacy Officer informs the participant that the restriction is terminated with respect to PHI received or created after the effective date of the

termination.

2. Confidential Communications with Participants

   a. A participant may request in writing confidential communications if the disclosure of PHI could endanger the participant.

   b. The written request shall be sent to the Privacy Officer and must:

      (i) specify in writing the alternative address or alternative means for confidential communications, and

      (ii) state that the disclosure of the PHI in a manner inconsistent with the request could endanger the participant.

   c. The Privacy Officer will accommodate a participant's reasonable request to receive communications regarding his/her PHI in an alternative manner or at an alternative location when disclosure of the PHI in a manner inconsistent with the participant's request could endanger the participant.

   d. The Privacy Officer will take the appropriate and necessary steps to ensure that the health plan complies with any approved request for confidential communications.

3. Right of Access

   a. Participants have the right to request electronically or in writing a paper or electronic copy of their PHI maintained by the health plan in designated record sets. See Article VII "Health Plan Participant Privacy Rights" above regarding the specific form and format of an electronic request for a copy of PHI.

      "Designated record set" is a term that is defined in the Privacy Regulations. The designated record sets shall generally only include claims history, payments, benefits and eligibility. A participant has a right to access, inspect, and obtain a copy of PHI about the participant maintained in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

      (i) Psychotherapy notes;

      (ii) Information compiled in reasonable anticipation of or for use in, a civil, criminal, or administrative action or proceeding; or

      (iii) PHI maintained by a Covered Entity that is:

         (a) Subject to the Clinical Laboratory Improvements

Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the member would be prohibited by law; or

(b) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 C.F.R. § 493.3(a)(2).

b. Participants may request information by submitting a written request to the Privacy Officer.

c. If the requested information is on site at the health plan, the request will be honored or denied within thirty (30) days of receipt.

d. If some or all of the requested information is not on site, or is maintained by a business associate, the request will be honored or denied within sixty (60) days. An approved request shall be forwarded promptly to the relevant business associates.

e. If necessary, the Privacy Officer may take one extension of thirty (30) days in which to make access available. The Privacy Officer shall send a written notice to the participant of the delay with the reasons for the delay and the date by which the participant will be allowed access. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures referenced in Article VI above.

f. If the request is granted in whole or in part, the Privacy Officer will inform the participant that the request has been granted in whole or in part.

g. The Privacy Officer will establish the amount of the charge for copying the requested information, if there is to be a charge. If established, the charge shall be based only on actual costs. The costs to be considered shall be the cost of supplies, labor for copying, preparation of the information, and postage if mailed. The Privacy Officer will communicate to the participant the charge for copying the requested information. The Privacy Officer may from time to time establish the appropriate charge for copying the requested information. Such established charges shall be reviewed at least annually to verify that the charges are reflective of actual costs. The charge for requested information shall be the same as the charge for public information requests established in 34 Tex. Admin. Code § 65.3, “Records of the System.”

h. If the request is denied in whole or in part, the Privacy Officer

shall provide written notice of the denial in plain language and include: (i) the reasons for the denial, (ii) an explanation of the participant's right for a review of the denial, and (iii) a description of how the participant may file a complaint with the health plan or the U. S. Department of Health and Human Services ("HHS"). The denial shall be maintained in accordance with the Retention of Documentation policy and procedures referenced in Article VI above.

i. If the reason for denial is that the information is not maintained by the health plan, the Privacy Officer shall direct the participant to where the information may be obtained, if such location is known by the health plan.

j. If the participant requests in writing a review of the denial, the request will be forwarded for review and resolution to a designated licensed health care professional that has not been directly involved with the review process resulting in the denial.

k. The designated reviewing health care professional shall, within a reasonable time, review the denial in accordance with the standards established in Section 164.524(a)(3) of the Privacy Regulations.

l. The results of the review will be sent to the participant in a written notice and the health plan will take appropriate action to follow the health care professional's determination. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures referenced in Article VI above.

4. Right to Request Amendment

a. Participants have the right to request an amendment to their PHI maintained by the health plan.

b. Participants may request amendment of information by submitting a written request to the Privacy Officer.

c. The health plan will act upon the request within sixty (60) days of receipt.

d. If necessary, the Privacy Officer may take one extension of thirty (30) days in which to determine whether to make an amendment. The Privacy Officer will send a written notice to the member of the delay with an explanation of why the delay is required, and the date by which a decision will be made regarding the requested amendment. The written notice shall be maintained in accordance with the Retention of Documentation policy and procedures referenced in Article VI

above.

e. If the request for amendment is accepted, the health plan shall:

(i) Identify the designated record set(s) in which the PHI that is the subject of the amendment request is contained and make the amendment;

(ii) Inform the participant that the amendment is accepted;

(iii) Obtain from the participant the names and addresses of persons to whom the amended information should be sent;

(iv) Once agreement is obtained from the participant:

(a) Make reasonable efforts to provide the persons identified by the participant with the amended information; and

(b) Make reasonable efforts to provide the amended information to other relevant persons and business associates: (i) that have the PHI that is the subject of the amendment; and (ii) that may have relied or could rely on the PHI to make a decision about the participant.

f. If the request is denied in whole or in part, the Privacy Officer shall provide a written notice of the denial and include:

(i) The reasons for denial;

(ii) The participant's right to submit a statement disagreeing with the denial;

(iii) How the participant may submit the statement of disagreement;

(iv) A statement that the participant may request the health plan to include the participant's request for amendment and its denial with any future disclosures of the disputed PHI, in lieu of submitting a statement of disagreement; and

(v) A clear statement of the participant's right to complain to the health plan and to the Secretary of HHS.

g. The denial shall be maintained in accordance with the Retention of Documentation policy and procedures referenced in Article VI above.

h. The health plan, at its option, may prepare a rebuttal statement.

i. Upon the request of the participant, any future disclosures will include the request for amendment and the denial.

j. Any future disclosures will include any statement of disagreement and rebuttal.

k. The Privacy Officer will maintain a log of all requests for amendment and the applicable resolutions.

l. When another covered entity sends the health plan amended PHI, the Privacy Officer will ensure that the health plan takes all appropriate and necessary steps to amend the PHI that it maintains in designated record set(s).

## VIII. DISCLOSURES AND USES OF PROTECTED HEALTH INFORMATION

A. The health plan will not and is not required to obtain a consent or authorization to use and disclose PHI to carry out treatment or payment or health care operations.

B. When the use and disclosure of PHI is not for treatment, payment, health care operations, or otherwise permitted or required by law without an authorization, the health plan will obtain a valid authorization from the participant prior to using or disclosing PHI. Specifically, an authorization may be obtained for the TexFlex program administration, Long-term Care Insurance, Short-term Disability Insurance, Medical and Family Medical Leave Act requests and other similar operations when offered or the request requires release of health plan PHI.

1. There will not be a health plan authorization for information containing PHI when it comes directly from the employee and not the health plan. For example, a doctor's note describing a condition supporting a disability claim that did not originate from the health plan will not require a health plan authorization.

2. There will not be a health plan release for employer-mandated health activities, such as work place drug testing, workers' compensation, Americans With Disabilities Act or the Occupational Safety and Health Administration.

C. When the health plan receives an authorization for disclosures from another entity or person, the Privacy Officer will review the authorization to determine: (i) that it is a valid authorization pursuant to Section 164.508 of the Privacy Regulations, and (ii) the minimum amount of information that is necessary to disclose to comply with the authorization.

## IX. CLASSES OF USERS OF PROTECTED HEALTH INFORMATION

A. All of the classes of users of PHI within the health plan are also employees of the plan sponsor. For the purposes of these policies and procedures, the classes of users, or workforce, includes individuals who would be considered part of the workforce under HIPAA such as

employees, volunteers, trainees, and other persons whose work performance is under the direct control of ERS, whether or not they are paid by ERS. The term “employee” used herein includes all of these types of workers. Classes of users of PHI are to have access to the minimum amount of PHI reasonably necessary to perform their functions and responsibilities. The classes of persons within the health plan who need access to PHI to carry out their duties, along with the conditions of access and the uses of such information, are as follows:

B. CLASSES

1. HR Agency Analysts

HR Agency Analysts, also referred to as "benefits coordinators," are the individuals assigned in each agency to assist participants in making contact with the call center, the administrator or carrier as may be appropriate. An HR Agency Analyst will not receive or have access to PHI. An HR Agency Analyst shall have access only to enrollment information necessary to facilitate proper enrollment of employees and participants in the health plan including appropriate listing of dependents.

2. ERS HR Analysts

ERS HR Analysts are the subset of HR Agency Analysts that service the ERS employees and have the same access as HR Agency Analysts except they are limited to assisting ERS employees, dependents and retirees in the manner prescribed for the class of HR Agency Analysts.

3. Information Technology

IT personnel shall have access as needed to PHI in the performance of their duties in preparing data, managing data, administering data, maintaining applications, and delivering applications for processing and managing the health plan. IT personnel include personnel responsible for creating and maintaining plan data sets and applications. IT personnel also include system technicians responsible for organization and maintenance of websites, connectivity within the organization's networks, email and for connectivity with external networks.

4. Clerical

Clerical personnel shall have access to PHI only to the extent necessary to perform duties in assisting in the administration of health claims and in communicating information to the relevant supervisors and personnel. Clerical personnel include mail personnel, secretarial support, and others responsible for document handling and preparation. Clerical personnel shall have access only to the information needed to perform their job description. For example, mail-opening personnel have a need to know sufficient information

to properly route the mail and to identify misdirected mail and may have a need to physically open PHI contained in the mail. However, there is no need for mailroom personnel to view details contained within the PHI.

5. Supervisors/Senior Managers

   Supervisors and Senior Managers shall have access to PHI as needed in performance of oversight and administrative functions of personnel and quality review of the various classes of users they supervise.

6. Finance and Accounting

   Financial analysts shall have access to PHI as necessary to reconcile banking and other financial statements and to process financial functions to enhance the plan health and where necessary view summary and individual data to assist in determining plan obligations and potential future obligations.

7. Plan/Benefit Contracts

   This class of individuals shall have access to PHI as necessary to perform their functions of managing contracts with various business associates and vendors and renewing or negotiating contracts of service and resolving plan administration issues. Additionally, the class of Plan/Benefit Contracts personnel shall have access to PHI as necessary to properly supervise and evaluate business associate and vendor performance.

8. Call Center Specialist

   Call Center Specialists shall have access to PHI as necessary. The request for assistance shall be instigated at the patient's request for assistance as needed for processing health claims, eligibility, benefits and facilitating health care operations. Analysts include those who assist patients in making contact with carriers and administrators and where necessary facilitating resolution of issues. These include those responsible for interacting with participants, employees, providers, business associates and others in resolving eligibility, benefits, claims, coordination of benefits and other benefit issues. This class also includes the sub-class of claim specialists who assist in resolving complex or difficult claim or eligibility issues. This sub-class shall have access to PHI as necessary to facilitate resolution of difficult or complex issues.

9. Internal Audit

   Internal Auditors shall have access to PHI as necessary to perform their function of assuring financial accuracy and fraud detection.

10. Legal

Attorneys and legal support staff shall have access to PHI as necessary to perform their function of providing legal advice to ERS and the health plan and handling grievances, appeals, litigation and fraud prevention.

11. Executives, Directors, Trustees

Executives, directors, and members of the ERS Board of Trustees, and their support staff, shall have access to PHI as necessary to perform their function in overseeing the solvency and viability of the health plan and all operations of the plan, and in their function of responding to participant, legislative and executive branch inquiries.

## X. PROTECTION OF PROTECTED HEALTH INFORMATION

A. Access by the various classes of PHI users shall be limited to the minimum necessary amount of PHI information reasonably calculated to allow performance of their duties.

B. Access by the various classes of PHI users shall be limited and controlled by network passwords. Access to PHI will be limited to those classes of users requiring the information.

C. Appropriate administrative, technical and physical safeguards shall be observed. Administrative safeguards include implementing procedures for use and disclosure of PHI. Technical safeguards include limiting access to information by creating computer firewalls. Physical copies of records and reports containing PHI shall be maintained in secure filing cabinets, locked drawers or locked rooms and not left open or available for inadvertent exposure.

1. Documents containing PHI shall not be left out on desks or in other areas where there is a significant risk of inadvertent disclosure.

2. At the end of the work day, documents containing PHI shall be filed in locked filing cabinets, locked desks or locked offices. Documents to be discarded that contain PHI will be shredded or placed in locked bins.

3. Staff involved in opening and sorting mail shall identify mail that contains PHI and shall route it to appropriate personnel. Mail or other documents containing PHI shall be processed timely and not left out where there is significant danger of inadvertent disclosure.

## XI. ROUTINE DISCLOSURES AND REQUESTS OF PROTECTED HEALTH INFORMATION

A. The health plan generally discloses PHI only in furtherance of providing the medical and/or dental benefits described in the health plan's specific benefit documents. The health plan discloses PHI (i) to conduct payment functions that include billings, claims management, collection activities and

related health care data processing, (ii) to respond to eligibility and benefit inquiries from providers, and (iii) for other reasons related to the operation of the specific benefit plan (these reasons are described in the Notice as "health care operations"). Health care operations may include any of the following activities: conducting quality assessment and improvement activities, reviewing health plan performance, conducting or arranging for medical review, legal services and auditing functions, business planning and development, business management and general administrative activities, and other health care operations permitted by the HIPAA Privacy Regulations. The health plan contracts with business associates to perform various services or to perform certain specified functions, such as administration of claims, member service support, utilization management, coordination of benefits, subrogation, pharmacy benefit management, and other similar functions. The health plan utilizes these business associates to receive, create, maintain, use, and disclose relevant PHI for the purposes of treatment, payment of health claims and health care operations. The health plan must obtain assurances from the business associate that it will appropriately safeguard the information through a business associate agreement in accordance with 45 C.F.R. § 164.314.

B. Periodically the health plan requests proposals from third-party administrators, pharmacy benefit managers, insurance and stop-loss companies to ensure the viability of the health plan. In the course of developing proposals, occasionally specific PHI is required by these companies. The health plan assists in providing the required information in furtherance of its responsibility to maintain plan integrity and fiscal health. These companies are the health plan's business associates and, as such, will comply with the rules set forth in these policies and procedures for business associates.

C. The health plan may disclose PHI to various health care providers for the purpose of treatment, payment, services to plan participants, or in furtherance of disease management or other health care operations of the health plan.

D. The health plan discloses information to the plan sponsor for the purpose of funding benefits and determining the health and viability of the health plan. The plan sponsor has certified that, among other actions, it has limited the access to PHI to relevant personnel and that PHI will not be used in any employment action or in connection with any other plan sponsor benefit.

E. In general, the health plan will request PHI on a routine basis only for those purposes described in paragraphs A through D above. Where the health plan requests PHI from a participant, a non-covered entity, or another covered entity, it will limit its request to the amount of PHI necessary to accomplish those purposes outlined above (i.e., in paragraphs A through D).

F. The health plan will not disclose or request an entire medical record unless the entire record is reasonably necessary to accomplish the purpose of the

disclosure or request.

G. The health plan may disclose PHI to authorized parties as necessary to carry out the legally mandated administrative appeal process or judicial process related to benefit determinations, payment of claims, health care treatment and enrollment/coverage determinations.

## XII. NON-ROUTINE DISCLOSURES AND REQUESTS OF PROTECTED HEALTH INFORMATION

A. The Privacy Officer will review each non-routine disclosure on an individual basis. The Privacy Officer will determine the minimum amount of PHI necessary for the disclosure, using established criteria that includes, but is not limited to:

1. Identifying the type of PHI requested (e.g., demographic, diagnosis, or procedures information); and

2. Evaluating the purpose for the disclosure (e.g., treatment, payment or health care operations).

B. The health plan may rely on public officials and other covered entities under the Privacy Regulations to request only the minimum necessary amount of PHI.

C. Where the health plan is requesting PHI on a non-routine basis, the Privacy Officer will review the request to ensure that the health plan is limiting its request to only the information it reasonably needs to accomplish the purpose of the disclosure or request.

D. The health plan will not disclose or request an entire medical record unless the entire record is reasonably necessary to accomplish its purpose.

## XIII. VERIFYING IDENTITY AND AUTHORITY PRIOR TO DISCLOSURES

A. Where the health plan does not know the identity of the individual or entity (including public officials), it shall use its professional judgment to verify the identity and the authority of the individual or entity before disclosing the requested PHI unless the disclosure is for one of the reasons identified in § 164.510 of the Privacy Rule (e.g., in an emergency).

B. If the Privacy Regulations require documentation, statements, or representations (e.g., subpoena, authorization, and government letterhead) as a condition of making a disclosure, the health plan may rely on such materials to make the disclosure of PHI without performing additional verification, unless otherwise required by the Privacy Regulations or other law.

C. With respect to disclosures to public officials, the health plan may rely on the following to verify:

1. Public official's identity:

a. If the request for PHI is made in person, agency identification, badge, or other proof of government status;

b. If the request for PHI is made in writing, the request is on government letterhead; or

c. If the request is to an entity or individual acting on behalf of a government entity, documentation that the entity or individual is acting on behalf of the government entity.

2. Public official's authority:

a. A written or oral statement of legal authority for the disclosure of PHI; or

b. A warrant, subpoena, administrative or court order, or other legal process that provides legal authority for the disclosure.

## XIV. DISCLOSURES TO BUSINESS ASSOCIATES

A. The health plan uses business associates that are not part of the health plan workforce to carry out various health plan functions of payment for medical services and health care operations. These functions may include, but are not limited to, administration of claims, member service support, provider relations, utilization review, pharmacy benefit managers, coordination of benefits, subrogation, stop-loss companies, and other necessary activities.

B. Business Associate Procedures

1. Each business associate will adopt privacy policies and procedures acceptable to the health plan. The policies and procedures will be referenced in the business associate agreement and will be either identical to these policies and procedures or approved by the Privacy Officer as complying with the HIPAA Privacy Regulations and HITECH.

2. It is reasonable to presume the PHI requested by a business associate is the minimum information necessary that is required to perform the business associate task(s). The Privacy Officer may rely on requests of business associates as being requests for the minimum necessary amount of PHI.

3. Each business associate agreement or subcontract shall contain an obligation to use the PHI only for the purposes and functions required by the health plan, and only as long as there is relation to the health plan.

4. Each business associate agreement or subcontract shall contain an obligation that the business associate must comply with the Privacy Rule and the Security Rule of the HIPAA Regulations and as set forth in HITECH, including notifying the health plan of a breach.

5. The Privacy Officer shall review at least annually the business associate's policies and procedures regarding recurring information

disclosures for appropriateness and to ascertain that the minimum necessary is being disclosed.

6. The Privacy Officer will consider the following factors in reviewing and approving the business associate's policies and procedures regarding recurring disclosures of PHI:

   a. The nature of the PHI: such as whether it is benefit information, claims history, eligibility, diagnoses, procedures, or other relevant categorizations;

   b. The functions performed by the business associate; and

   c. Whether the entity or business associate is engaged in a pattern of activity that constitutes a material breach or violation of the business associate agreement.

## XV. DISCLOSURES TO PLAN SPONSOR AND PLAN SPONSOR AGENTS

A. The health plan will not disclose PHI to the plan sponsor except upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions or other provisions that achieve the same HIPAA and HITECH compliance objectives, and that the plan sponsor agrees to:

   1. Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

   2. Ensure that any agents, including a subcontractor, to whom it provides PHI received from the health plan agree to the same restrictions and conditions that apply to the plan sponsor through a written contractual agreement that complies with 45 C.F.R. § 164.314;

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

   4. Report to the health plan any inappropriate use or disclosure of which it becomes aware that is inconsistent with the uses or disclosures provided for.

   5. Report to the health plan any Security Incident or breach of unsecured PHI of which it becomes aware.

   6. Not use genetic information for underwriting decisions.

B. The plan document must:

   1. Describe permitted uses of PHI;

   2. Specify that the plan sponsor has provided required certification, which includes the ten points identified below;

   3. Ensure firewalls have been established. A firewall, in this regard, means procedural and policy limitations on which personnel of the

plan sponsor can receive PHI and the specific limits on use of the PHI. A firewall is a clear delineation of the permissible uses of, and individual authority to use, PHI;

4. The health plan will rely on a certification from the plan sponsor that the plan sponsor will handle disclosures of PHI to the plan sponsor as follows:

   a. No further use or disclosure of PHI other than as permitted or required by plan document or as required by law;

   b. Ensure subcontractors agree to the same through a written contractual agreement in accordance with 45 C.F.R. § 164.314;

   c. Not use PHI for employment-related actions;

   d. Report any inconsistent use or disclosure;

   e. Make PHI accessible to the individuals who are the subject of the PHI;

   f. Allow individuals to request amendments of their PHI;

   g. Provide an accounting of disclosures as requested by an individual;

   h. Notify the health plan of any Security Incident or breach of unsecured PHI;

   i. Make practices available to the Secretary of HHS for compliance;

   j. If feasible, return or destroy all PHI when use is finished;

   k. Ensure firewalls are established. Firewalls will establish the classes of individuals at the plan sponsor that have access to PHI and the criteria to determine use of PHI; and

   l. Not use or disclose genetic information for underwriting purposes.

## XVI. JUDICIAL, ADMINISTRATIVE AND GOVERNMENTAL DISCLOSURES

A. Disclosures of PHI may be made in the following instances:

1. In response to a court order or administrative tribunal, provided that only the PHI expressly authorized by the order will be disclosed.

2. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

   a. The health plan receives satisfactory assurance from the party seeking the information that reasonable efforts have been

made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request. Satisfactory assurance means:

(i) The requesting party has mailed a written notice to the individual's last known address;

(ii) The requesting party provides the health plan a written statement, with accompanying documentation, demonstrating that the notice was given and that it contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection with the court or tribunal; and no objections were raised or all objections were resolved.

b. The health plan receives satisfactory assurance that the party requesting the PHI has made reasonable efforts to obtain a protective order. A qualified protective order means that the parties involved in the dispute are:

(i) Prohibited from using or disclosing the PHI for any purpose other than the proceeding for which the information was requested; and

(ii) Required to return to the health plan or to destroy the PHI at the end of the proceeding.

3. In response to authorized public health requests;

4. For purposes of health oversight activities;

5. For purposes of HHS enforcement of Privacy Regulations;

6. About decedents;

7. For cadaveric-, eye- and tissue-donation purposes;

8. For certain limited research purposes;

9. To avert a serious threat to health or safety; and

10. For specialized government functions.

B. PHI may not be disclosed for marketing purposes if direct or indirect financial remuneration not reasonably related to the cost of making the communication is involved.

C. PHI may not be sold to third parties; however, the sale of PHI does not include a disclosure for public health purposes, for research purposes, where only remuneration for the cost to prepare and transmit the PHI is received, for treatment and payment purposes, for a business associate or its subcontractor to perform health care functions in accordance with an applicable business associate agreement, or for other purposes as required and permitted by law.

## XVII. DISCLOSURES TO PARTICIPANTS IN FURTHERANCE OF TREATMENT, CLAIM ADJUDICATION, PRECERTIFICATION, AND OTHER PAYMENT ISSUES

A. Generally, health plan personnel may use, disclose, and discuss an individual's PHI with the individual. There are exceptions for psychotherapy notes and certain institutional requests.

B. Procedure for identifying participants: A participant may be identified in person by personal knowledge, government issued identification or other similar documentation. A person may be identified over the telephone. Before discussing PHI by telephone with a member or personal representative, the identity of the individual must be ascertained:

1. Identify the member. A participant may be identified over the phone if he or she has the following minimum required personal information:

   a. Participant's Social Security Number, or a participant-unique identification number assigned by the health plan or health plan administrator;

   b. Participant's address;

   c. Participant's phone number.

2. In the course of a participant service call or other contact with a participant, the participant should have knowledge available to the participant of information such as:

   a. Provider's name;

   b. Past services;

   c. Prior contacts, etc.

3. If a participant's identity is not certain or becomes suspect, no PHI should be disclosed.

4. If the caller is inquiring about another individual, verify the right of the caller to access the requested PHI.

5. Generally, parents have a right to access the PHI of minor children. If there are notes in the record addressing the issue of parental rights such as limiting a non-custodial parent's right of access, the notes should be followed when determining what access a parent should have to a minor child's PHI.

6. As permitted by state law, if a dependent child has established with the health plan an approved mode of alternate confidential communications, disclosure of PHI to the parent may not be permitted.

7. It is the obligation of the requesting individuals to prove their right to the PHI. This may not be possible over the phone.

## XVIII. DISCLOSURES TO PROVIDERS IN FURTHERANCE OF CLAIM ADJUDICATION, PRECERTIFICATION, AND OTHER PAYMENT ISSUES

A. PHI may be discussed with or disclosed to a participant's health care providers in furtherance of treatment, health care operations and payment.

B. Procedure for identifying provider in provider phone conversations.

1. Verify the identity of the individual as a provider authorized to request information or discuss the PHI. If ERS personnel originate the phone conversation, it may be assumed the call recipient is appropriate. For example, when calling the listed number of a hospital business office, it may be initially presumed the answering person is an authorized representative of the provider. A provider may be identified over the phone if the provider is known from prior contacts or has the correct:

   a. Participant's name and identifying demographic information; or

   b. The participant's social security number or participant-unique identification number assigned by the health plan or health plan administrator; or

   c. Demonstrates knowledge of the relevant participant and history.

2. If the identity or authority of the provider personnel is in doubt, information should not be disclosed.

## XIX. PROCEDURE FOR SENDING PHI VIA FAX

1. The health plan FAX machines for sending and/or receiving PHI at each location are in secure designated locations.

2. An individual at each location has been trained and tasked to identify PHI-related faxes and distribute them appropriately.

3. If the FAX machine used for PHI at any location is not secure, then PHI may be sent only with an advance call to make sure the recipient is waiting for the FAX to minimize inadvertent disclosures.

4. A Confidential Fax Coversheet to provide extra protection for PHI has been developed. The headline of the coversheet states in large bold type: "Confidential Health Information Enclosed." Beneath this headline is a statement: "Health Care Information is personal and sensitive information related to a person's health care. It is being faxed to you after appropriate authorization from the patient/participant or under circumstances that do not require patient/participant authorization. You, the recipient, are obligated to maintain the health care information in a safe, secure and confidential manner. Re-disclosure of the health care information transmitted without additional patient/participant consent or as permitted

by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law."

5. Included at the bottom of the fax coversheet is a warning: "IMPORTANT WARNING: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this information is STRICTLY PROHIBITED. If you have received this message by error, please notify us immediately and destroy the related message."

6. In addition to the warnings described in (4) and (5) above, the fax coversheet contains standard information including:

   a. Date and time of the fax;

   b. Sender's name, address, telephone number and fax number;

   c. The authorized recipient's name, telephone number and fax number;

   d. Number of pages transmitted; and

   e. Information regarding verification of receipt of the fax.

7. Staff shall make certain the fax transmittal has received the proper authorization as required by law (i.e., that an appropriate release or authorization is on file) or that there is implied consent because the transmittal is in furtherance of treatment, health care operations or payment.

8. Faxing of sensitive health information, such as that dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information, is prohibited without supervisor approval.

9. When expecting the arrival of a fax containing PHI, coordinate with the sender whenever possible so the faxed document can be promptly retrieved upon arrival.

10. As with other PHI that arrives in the mail or by other means, make sure faxes that contain PHI are placed in the designated secure/confidential location when they are delivered, and not left in an in-box in view of passers-by.

11. Confirm the accuracy of fax numbers. It should be presumed the fax numbers provided by business associates are correct and secure. The numbers provided by recipients generally may be relied upon as valid. If there is reason to believe a number is not valid or security is suspect, the number, or security of recipient machines, should be checked by calling the intended recipients to double-check the numbers. In instances where faxes are regularly sent to the same recipients, program these fax numbers into the machine's memory, using the speed-dial numbers. Programmed

numbers should be tested at regular intervals.

12. Make sure fax machine prints a confirmation of each outgoing transmission and require machine operators to: (a) make sure the intended destination matches the number on the confirmation, and (b) staple the confirmation to the document that was faxed.

13. In the event of a misdirected fax, be sure that improperly faxed documents are either immediately returned or destroyed by the recipient. Document that the fax was misrouted and take (and document) steps to prevent a reoccurrence of the error.

14. Proof of delivery of PHI that is faxed will be retained as evidence of the time/date of the transmittal, the intended recipient, its contents, and the fax number at which it was confirmed to have been received.

15. Included in the business associate agreements or two-way covered entity agreements are provisions requiring organizations that will receive your faxes to place their fax machines in secure areas.

16. As with all other paper documents that contain PHI, faxes that contain PHI are handled and stored in the regular secure manner and shredded when they have outlived their usefulness.

## XX. PROCEDURE FOR SENDING AND RECEIVING EMAIL CONTAINING PHI

A. Email internal to the ERS network.

1. Before sending PHI in an internal email the appropriateness of the communication shall be considered. The criteria used to determine appropriateness of the communication are the same as apply to any communication of PHI.

2. Before sending PHI via internal email, the email address and recipient should be verified.

3. Emails containing PHI should be deleted from the system after they are no longer required.

B. Email external to the ERS network over the Internet.

Emails sent via the Internet shall be encrypted to reduce the risk of inadvertent disclosure of PHI. If encryption is not available then another secure means of communication must be used.

1. The email address of the recipient should be verified prior to sending the email.

2. The criteria used in determining the appropriateness of whether to send PHI via email over the Internet are the same as determining whether to send internal email to other health plan employees or plan sponsor employees. Consideration should be given to the sensitivity of the information and the potential of inadvertent

disclosure.

3. Where possible, verification that the recipient received the email should be obtained.

4. The email shall contain a notice that the email contains PHI.

## XXI. CONVERSATIONS CONCERNING PHI

A. Employees should conduct conversations concerning PHI in a manner that limits the risk of inadvertent disclosure of PHI through casual overhearing. Some conversations, because of their sensitive nature or the PHI or concerns by the participant of inadvertent disclosure, may only be possible in a private office or location.

B. Personnel initiating conversations or phone calls concerning PHI should be aware of their surroundings. For example, a call concerning PHI made by a call center specialist to a business associate to discuss whether a diagnosis supports a certain medical procedure should not be made from a reception area with people in the waiting area.

C. Personnel initiating a call concerning PHI should be aware of the surroundings of the call recipient. Inquiry may need to be made as to whether the recipient can converse without danger of PHI being inadvertently disclosed to individuals in the immediate area of the call recipient.

D. When plan members initiate discussion of PHI with plan personnel, the plan personnel shall be cognizant of the potential for inadvertent disclosure of PHI when discussion takes place in reception or common areas of offices. Plan personnel shall move appropriate conversations to offices or other quieter locations that reduce the potential for inadvertent disclosure.

E. Leaving voice mail or forwarding voice mail containing PHI should be done with the same considerations as engaging in conversations concerning PHI.

## XXII. TRAINING

A. Policy:

All personnel shall be trained in the requirements of protecting, using and disclosing PHI.

B. Procedures:

1. All personnel shall be trained in the requirements and procedures necessary to implement the privacy policies contained herein as relates to their respective jobs.

2. Training shall consist of content sufficient to provide:

   a. An overview of HIPAA, HITECH and the Privacy Regulations; and

   b. Detailed training on the policies and procedures relevant to the person's responsibilities.

C. The training materials will be maintained by the health plan on its website or Intranet for reference and review. In-service, refresher trainings will be conducted upon determination by the Privacy Officer that the policies, procedures and laws have changed sufficiently to require further training or, that compliance would be enhanced by additional training.

D. New employees and employees changing assignments will be required to undergo relevant privacy training as a condition of their assuming their responsibilities.

E. A log shall be maintained that tracks the initial training given to all employees, as well as updates and in-service refresher training modules.

## XXIII. SANCTIONS AND MITIGATION

A. The health plan may discipline any employee who has violated these policies and procedures or the Privacy Regulations. Depending on the severity of the violation, employee discipline may include all disciplinary action available under ERS' Personnel Policy and Procedure Manual, including, but not limited to, verbal warning, letter of reprimand, retraining, suspension or termination as appropriate. The Privacy Officer will document and maintain any sanctions that are imposed pursuant to the Retention of Documentation policy and procedures referenced in Article VI above.

B. The health plan will not discipline an employee who:

1. Testifies or assists in an investigation, compliance review, or hearing regarding the health plan's compliance with the Privacy Regulations; or

2. Opposes any act or practice that the employee believes, in good faith, is in violation of the law, and if the employee has not disclosed the PHI in violation of the Privacy Regulations and if the opposition is reasonable.

C. The health plan will take the appropriate and necessary steps to limit the harm of a use or disclosure by an employee or business associate in violation of these policies and procedures or the Privacy Regulations.

## XXIV. RESERVATION OF RIGHT TO CHANGE POLICIES, PROCEDURES OR NOTICE

The health plan reserves the right to change these privacy policies and procedures and the Notice of Privacy Practices as the laws change or as circumstances dictate. When necessary, a revised Notice of Privacy Practices will be distributed to members.

No third-party rights (including, but not limited to, rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by these privacy policies and procedures. To the extent these privacy policies and procedures establish requirements and obligations above and beyond those required by HIPAA, they shall be aspirational and shall not be binding upon the health plan or ERS. To the extent

these policies and procedures are in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

* * * * *

The Employees Retirement System of Texas originally adopted these Privacy Policies and Procedures on behalf of the Texas Employees Group Benefits Program on April 14, 2003 and subsequently revised them effective February 17, 2010, and September 23, 2013.