

**EMPLOYEE GROUP INSURANCE
TREATMENT OF PROTECTED HEALTH INFORMATION**

Policy 1: Introduction & Definitions	Page: 1 of 9
Effective Date: April 14, 2003	

Purpose

This compilation of policies and procedures governs the treatment of the protected health information of group health plan participants and beneficiaries by Employer Group Insurance (EGI). The policies and procedures are intended to comply with 45 C.F.R. § 164.530(j)(1)(i), which requires EGI to implement and design privacy policies and procedures that comply with the HIPAA Privacy Standards and to maintain such privacy policies and procedures in written or electronic form. (Defined terms are capitalized.)

The HIPAA Privacy Standards govern the confidentiality of individuals' health information maintained in the health care system. An entity covered by the HIPAA Privacy Standards generally must comply with the following obligations: (i) Use or Disclose health information only as permitted by the HIPAA Privacy Standards; (ii) limit requests, Uses, and Disclosures of health information to the minimum necessary; (iii) give individuals a notice of the entity's privacy practices; (iv) provide individuals certain rights with respect to their health information; and (v) establish certain administrative procedures to ensure health information is kept confidential, such as the designation of a privacy official and the establishment of sanctions against workforce members who breach an individual's privacy rights.

It is always the intent of EGI that these policies be interpreted consistently with the HIPAA Privacy Standards.

Self-funded Group Health Plan

These policies and procedures, as they may be amended from time to time, are incorporated into and are made a part of the Self-funded Group Health Plan administered by EGI.

Definitions

Where the following capitalized terms appear in these Policies, they have the definitions set forth below.

(1) **Authorization**: A written document that authorizes a Use or Disclosure of Protected Health Information or PHI and that satisfies Section 4.8 of this Manual.

(2) **Business Associate**: A person who, on behalf of EGI, either (i) performs (or assists in the performance of) a function or activity involving the Use or Disclosure of protected health information or any other function or activity regulated by the HIPAA Privacy Standards; or (ii) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for EGI, where the provision of the service involves the Disclosure of individually identifiable health information from EGI, or from another Business Associate of EGI, to the person.; provided that the term "Business Associate" does not include EGI when it is functioning as the sponsor of a group health plan.ⁱ The relationship between EGI and a Business Associate must be formalized by a written

Business Associate Agreement that binds the Business Associate to comply with all applicable provisions of this Manual as to any PHI collected or held on behalf of EGI and includes a Certification.

(3) **Carrier**: A health insurance carrier, which is an insurance company, insurance service, or managed care organization (including an HMO) that is licensed under and subject to state law that regulates insurance; provided that the term “Carrier” does not include a group health plan.ⁱⁱ

(4) **Certification**: A certification that an entity shall:

- a. Not Use or Disclose PHI other than as permitted or required by the group health plans administered or sponsored by EGI or as required by law;
- b. Agree to the same restrictions and conditions that apply to EGI with respect to such information;
- c. Not Use or Disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of EGI or The University of Texas System Administration;
- d. Take steps to deal with any Use or Disclosure of Plan PHI that is inconsistent with the Uses or Disclosures provided for of which it becomes aware;
- e. Make available PHI in accordance with individuals’ right to access PHI, which right is described in Section 7.2 of this Manual;
- f. Make available PHI for amendment and incorporate any PHI amendments into the Designated Record Sets held by EGI in accordance with individuals’ right to request amendments of PHI, which right is described in Section 7.3 of this Manual;
- g. Make available the information required to provide an accounting of disclosures of PHI in accordance with individuals’ right to receive an accounting of disclosures, which right is described in Section 7.4 of this Manual;
- h. Make EGI’s internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining EGI’s compliance with the HIPAA Privacy Standards;
- i. If feasible, return or destroy all PHI received that EGI still maintains in any form and retain no copies of such information when no longer needed for the purpose for which Disclosure was made, except that, if such return or destruction is not feasible, limit further Uses and Disclosures to those purposes that make the return or destruction of the information infeasible; and
- j. Ensure that any adequate separation of records or PHI is established and maintained.ⁱⁱⁱ

(5) **Contact Person**: The person or office designated in accordance with Section 3.2 of this Manual.

(6) **Covered Entity**: A health plan (as defined by HIPAA), a health care clearinghouse (as defined by HIPAA), or a health care provider (as defined by HIPAA) who transmits any health information in electronic form in connection with a transaction covered by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations.^{iv}

(7) **De-identified Information**: Information that does not identify an individual and that EGI has no reasonable basis to believe can be used to identify an individual.^v Two methods by which EGI can demonstrate that information qualifies as De-identified Information are as follows:

- a. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (i) determines, applying such principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information and (ii) documents the methods and results of the analysis that justify such determination; or
- b. EGI ensures that (i) it does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information and (ii) the following identifiers of the individual, or relatives, employers, or household members of the individual, are removed:
 - Names;
 - All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip code and their geocodes (except that the initial three digits of a zip code may be used if more than 20,000 people reside within the area included in all zip codes sharing those initial three digits, and, if fewer than 20,000 people reside within such area, the number “000” may be used instead);
 - All elements of dates (except the year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death;
 - All ages over 89 and all elements of dates (including the year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
 - Telephone numbers;
 - Fax numbers;
 - Electronic mail addresses;
 - Social Security numbers;
 - Medical record numbers;
 - Health plan beneficiary numbers;
 - Account numbers;
 - Certificate/license numbers;
 - Vehicle identifiers and serial numbers, including license plate numbers;
 - Device identifiers and serial numbers;
 - Web Universal Resource Locators (URLs);
 - Internet Protocol (IP) address numbers;
 - Biometric identifiers, including finger and voice prints;
 - Full face photographic images and any comparable images; and
 - Any other unique identifying number, characteristic, or code (other than a code that enables the information’s creator to re-identify the information).^{vi}

(8) Designated Record Set: The set of information that includes PHI and that either (i) is enrollment, Payment, claims adjudication, and case or medical management record systems maintained by or for EGI or (ii) is used, in whole or in part, to make decisions about individuals.^{vii}

(9) Disclosing, a Disclosure, to Disclose or to be Disclosed: Divulging information *outside* an entity, including release, transfer, or provision of access to information.^{viii}

(10) Employee Group Insurance or EGI: The University of Texas System Administration Office charged by The University of Texas System with implementing the uniform benefit program for its employees and retired employees and administering the insurance coverage and other benefits provided under the State University Uniform Insurance Benefits Act.

(11) Fully-insured Group Health Plan: Group health coverage that is offered to eligible employees, retired employees, spouses and eligible dependents of The University of Texas System pursuant to the State University Employees Uniform Insurance Benefit Act (the Act) that is purchased by The University of Texas System from a carrier.

(12) Group Health Plan: Coverage provided by a Carrier to the employees of an employee. The coverage provided includes coverage for medical services, pharmacy benefits, vision care services, dental services and any other service considered by law to be a health service or benefit that can be provided by a Carrier.

(13) Health Care: Services that prevent, treat, cure or heal human physical and mental conditions and illnesses.

(14) Health Care Component: The portions of a Hybrid Entity that perform functions that are subject to the HIPAA privacy standards.

(15) Health Care Operations: Any of the following activities:

- a. Conducting quality assessment and improvement activities including outcomes evaluation and development of clinical guidelines (provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions other than Treatment;
- b. Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance or health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; and accreditation, certification, licensing, or credentialing activities;
- c. Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits; and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
- d. Conducting or arranging for medical review, legal services, and auditing functions (including fraud and abuse detection and compliance programs);
- e. Business planning and development (including cost-management and planning-related analyses related to managing and operating the entity, formulary development and administration, and development or improvement of methods of payment or coverage policies); and
- f. Business management and general administrative activities of the entity, including (i) management activities relating to implementation of and compliance with the requirements of the HIPAA Privacy Standards; (ii) customer service (including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that PHI is not Disclosed to such policyholder, plan sponsor, or customer);

(iii) resolution of internal grievances; (iv) the sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to such activity; and (v) in accordance with the HIPAA Privacy Standards, fundraising for the benefit of the Covered Entity and creating De-identified Information or a Limited Data Set.^{ix}

(16) **Health Care Provider**: A physician or other provider licensed under the laws of the state to provide health care to an individual.

(17) **Health Oversight Agency**: An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe (or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority) that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.^x

(18) **HIPAA**: The Health Insurance Portability and Accountability Act of 1996, as amended from time to time.

(19) **HIPAA Privacy Standards or Privacy Rule**: The privacy regulations at Part 160 of, and subparts A and E of Part 164 of, Title 45 of the Code of Federal Regulations, as amended from time to time.

(20) **HMO**: A federally qualified health maintenance organization, an organization recognized as a health maintenance organization under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as such a health maintenance organization.

(21) **Hybrid Entity**: A single legal entity that performs both functions that are subject to the HIPAA Privacy Standards and non-HIPAA covered functions and that segregates its covered functions from its non-covered functions for purposes of compliance with the HIPAA Privacy Standards.

(22) **Limited Data Set**: Information that excludes the following direct identifiers of the individual and his relatives, employers, and household members:

- Names;
- Postal address information (but not including town or city, state, and zip code);
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;

- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.^{xi}

(23) **Manual**: This compilation of EGI's HIPAA privacy policies and procedures.

(24) **Medical Record**: Information that is created by a health care provider; identifies or can be readily associated with the identity of an individual; and relates to the health care of the individual.

(25) **Members**: Employees and retired employees who are eligible for and obtaining a benefit or benefits provided by System under the State University Employees Uniform Insurance Benefit Act and the spouses and eligible dependents of these employees and retired employees.

(26) **Memorandum of Understanding or MOU**: An agreement that takes the place of a Business Associate Agreement between EGI and entities that are governmental agencies or subdivisions of governmental agencies with which EGI has a Business Associate relationship.

(27) **Notification Disclosures**: Disclosure of PHI to an individual's relative or close personal friend or other person identified by the individual, if such PHI is directly relevant to such person's involvement with the individual's care or payment for the individual's health care; and Disclosure (or Use) of PHI to notify, or assist in the notification of, a person responsible for the individual's care (such as the individual's family member or personal representative) of the individual's location, general condition, or death.^{xii}

(28) **Payment**: Activities undertaken by a Group Health Plan to obtain premiums or to determine its responsibility for coverage and provision of benefits under the Group Health Plan, and activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Such activities include, without limitation:

- a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
- b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
- d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- e. Utilization review activities, including precertification and preauthorization of services and concurrent and retrospective review of services; and
- f. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name, address, date of birth, Social Security number, payment history, account number, and the health care provider's and/or health plan's name and address.^{xiii}

(29) **Plan Sponsor**: An employer that maintains a Group Health Plan for its employees.^{xiv} A Plan Sponsor is *not* a covered entity under HIPAA and Plan Sponsors are not regulated under HIPAA..

(30) **Privacy Officer**: The individual appointed to serve as the Privacy Officer for The University of Texas System Administration or the Privacy Officer's authorized designee.

(31) Protected Health Information or PHI: any information, transmitted or maintained in any form or medium (including orally), that (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (ii) 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 (iii) either identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; provided that the term “PHI” does not include (A) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, (B) student treatment records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and (C) employment records held by a Covered Entity in its role as employer.^{xv}

(32) Psychotherapy Notes: Notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record, but excluding the following: medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.^{xvi}

(33) Public Health Authority: An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe (or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority), that is responsible for public health matters as part of its official mandate.^{xvii}

(34) Secretary: The Secretary of Health and Human Services (or any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated).^{xviii}

(35) Self-funded Group Health Plan: Group health coverage that is offered to eligible employees, retired employees, spouses and eligible dependents of The University of Texas System pursuant to the State University Employees Uniform Insurance Benefit Act (the Act) and that is self-funded by The University of Texas System and exempt from any insurance law of Texas which does not expressly apply to the Act.

(36) Summary Health Information: Information that summarizes the claims history, claims expenses, or types of claims experienced by individuals to or on whose behalf health benefits have been provided under a Group Health Plan and from which the following information has been deleted:

- Names;
- All geographic subdivisions smaller than a state (including street address, city, county, and precinct), except for the initial five digits of zip codes;
- All elements of dates (except the year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death;
- All ages over 89 and all elements of dates (including the year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;

- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (other than a code that enables the information's creator to re-identify the information)^{xix}

(37) Treatment: The provision, coordination, or management of health care or related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, and the referral of a patient for health care from one health care provider to another.^{xx}

(38) The University of Texas System or The System: The component institutions and other entities, including The University of Texas System Administration that comprise The University of Texas System.

(39) The University of Texas System Administration or System Administration: The offices, including EGI, the Office of General Counsel (OGC) and the Office of Human Resources for System Administration employees (OHRSA), that provide support and other services on behalf of the Board of Regents of The University of Texas System to The University of Texas System.

(40) Using, a Use, or To Use: Both (i) employment, application, utilization, examination, or analysis of information, and (ii) sharing information *within* an entity.^{xxi}

ⁱ 45 C.F.R. § 160.103.

ⁱⁱ *Id.*

ⁱⁱⁱ *Id.* § 164.504(f)(2)(ii).

^{iv} *Id.* § 160.103.

^v *Id.* § 164.514(a).

^{vi} *Id.* § 164.514(b).

^{vii} *Id.* § 164.501

^{viii} *Id.*

^{ix} *Id.*

^x *Id.*

^{xi} *Id.* § 164.514(e)(2).

^{xii} *Id.* § 164.510(b)(1).

^{xiii} *Id.* § 164.501

^{xiv}

^{xv} *Id.* §§ 160.103, 164.501.

^{xvi} *Id.* § 164.501.

^{xvii} *Id.* §164.504(f),

^{xviii} *Id.* § 160.103.

^{xix} *Id.* § 164.504(a).

^{xx} *Id.* § 164.501.

^{xxi} *Id.*