POLICY 1: Introduction & Definitions	**Page:**1 of 12
Effective Date: September 23, 2013	

Introduction

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 certain rights to individuals 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.

Purpose

This compilation of policies and forms ("the Manual") constitute official policies of The University of Texas System Administration (System). They are cross-referenced in the System Policy Library,
http://www.utsystem.edu/bor/procedures/policy/
collectively as System Administration Internal Policy INT 166.

They are adopted to govern the treatment of the Protected Health Information by System. The policies and procedures are intended to comply with 45 C.F.R. §§ 164.530(i) and (j)(1)(i), which require System, as a HIPAA Hybrid Entity that has an office that houses Self-funded Group Health Plans that are Covered Entities, as well as offices that function as Business Associates (collectively "the Health Care Component"), 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. Additionally, these policies address System's duties as a Plan Sponsor to other Fully-insured Group Health Plans through which employees, retirees and their eligible dependents are insured.

Effective Date

The policies and forms in this Manual take effect on September 23, 2013. They replace and supersede all previous policies and forms adopted by System or any System office to comply with HIPAA, other than INT 165, Breach Notification Policy, including Chapter 400 of the Office of Employee Benefit's Employee Group Insurance Policy Manual, Health Insurance Portability and Accountability Act (HIPAA) in place at the time these Policies take effect.

Incorporation into The University of Texas System's Self-Funded Group Health Plans

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 Plans administered by The University of Texas System through the Office of Employee Benefits within System.

Definitions

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

Authorization: A written document that authorizes a Use or Disclosure of PHI and that satisfies the requirements of this Manual.

Breach: Acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI information.

Business Associate: A person who, on behalf of System Administration or a System Institution that is a Covered Entity (including all Hybrid Entities), either (i) performs (or assists in the performance of) a function or activity involving the Use or Disclosure of individually identifiable 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 System Administration or a System Institution that is a Covered Entity , where the provision of the service involves the Use or Disclosure of individually identifiable health information from a Covered Entity, or from another Business Associate of the Covered Entity.[i] Business Associates include persons or entities who have periodic contact with PHI (e.g., outside auditors), or that have contact with PHI or (e.g., vendors providing software or hosting services) that require the vendor to persistently store PHI even if the vendor does not access the PHI. The terms does not include System or a University of Texas System institution when it is functioning as a Plan Sponsor.

Carrier: A health insurance carrier, which is an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in the state and is subject to state law that regulates insurance; the term "Carrier" does not include a Group Health Plan. [ii]

Certification: A statement by the Self-funded Group Health Plan that it shall:

a. Not Use or Disclose PHI other than as permitted or required by the Group Health Plans administered or sponsored by System or as required by law;

b. Ensure that any agents, including subcontractors, to whom System Administration provides PHI agree to the same restrictions and conditions that apply to System Administration 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 The University of Texas System or System Administration;

d. Take steps to deal with any Use or Disclosure of 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 as set forth in this Manual;

f. Make available PHI for amendment and incorporate any PHI amendments into any Designated Record Sets held by System Administration in accordance with individuals' right to request amendments of PHI as described in 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 as described in this Manual;

h. Make System Administration's internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining System Administration's compliance with the HIPAA Privacy Standards;

i. If feasible, return or destroy all PHI received that System Administration 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 required adequate separation of records or PHI is established and maintained. [iii]

Contact Person: A person or office designated to act on behalf of the Privacy Officer within a particular System office that is part of the Health Care Component.

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]

De-identified Information: Information that does not identify an individual and that System Administration has no reasonable basis to believe can be used to identify an individual. [v] Two methods by which System 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. System 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]

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 a Covered Entity or (ii) is used, in whole or in part, to make decisions about individuals.[vii] System does not make Treatment decisions about individuals.

Disclosing, a Disclosure, or to Disclose: Divulging information *outside* the Health Care Component, including release, transfer, or provision of access to information.[viii]

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 Uniform Insurance Benefits Act for Employees of The University of Texas System and The Texas A&M System that is purchased by The University of Texas System from a carrier.

Genetic Information: Information about an individual's genetic tests; the genetic tests of family members of an individual; and the manifestation of a disease or disorder in family members of an individual (i.e., family medical history). It includes the genetic information of a fetus carried by the individual or family member who is a pregnant woman; and any embryo legally held by an individual or family member utilizing an assisted reproductive technology. It excludes information about the sex or age of any individual.

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.

Health Care Component: The portions of a Hybrid Entity that perform functions that are subject to the HIPAA Privacy Standards.

Health Care Operations: Activities related to a Covered Entity's functions as a health plan, health provider, or health care clearinghouse. They include, but are not limited to, quality assessment and improvement activities including outcomes evaluation and development of clinical guidelines provided that obtaining 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, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, business planning and development (such as cost management), customer service, grievance and appeals resolution, vendor evaluations, legal services; business management and general administrative activities of the entity, including but not limited to (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, provided that PHI is only Disclosed in accordance with the HIPAA Privacy Standards; (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, creating De-identified Information or a Limited Data Set.[ix]

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]

HIPAA: The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Privacy, Security and Breach Notification Regulations at 45 CFR §§ 160 and 164 (hereinafter collectively, "HIPAA") and as otherwise amended from time to time.

HIPAA Breach Notice Rule: Regulations that mandate notice to individuals in some cases if their PHI is improperly accessed, used, or disclosed, as well as a report to HHS of such incidents. Media notice may also be required. The notice/report contents, timing, and distribution requirements are prescribed by the Breach Notice Rule.

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.

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.

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.

Individual: Except where the context plainly indicate otherwise, a reference to an "Individual" refers to the person to whom PHI that is maintained by System and subject to this Manual. "Members" are also "Individuals" for purposes of this Manual. Unless the specific terms of a policy in this Manual clearly indicate otherwise, for purposes of this Manual, any reference to an Individual" with regard to an Individual's rights regarding their PHI, also refers to a Personal Representative of the Individual.

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]

Manual: The compilation of System's HIPAA privacy policies and procedures.

Marketing: Communications about a product or service that encourage recipients of the communication to purchase or use the product or service, excluding face to face communications, or any communications for which System or a Plan receives no direct or indirect remuneration such as refill reminders, treatment plans, alternatives to treatment, case management, value added services provided in connection with a Plan, and other purposes related to treatment and health operations care. Marketing excludes promotional gifts of nominal value provided by the Plan and refill reminders provided by a covered entity.[xii]

Members: Employees, retired employees and other individuals 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, retired employees and individuals. Unless the specific terms of a policy in this Manual clearly indicate otherwise, for purposes of this Manual, any reference to a "Member" for purposes of a Member's rights regarding their PHI, also refers to the Personal Representative of the Member. A Member is an "Individual" as defined herein.

Minimum Necessary Standard: The requirement that a Use or Disclosure of PHI must be limited to only the specific PHI from the individual's medical record that is reasonably necessary to accomplish the purpose for which the Use or Disclosure is sought, as opposed to the Use or Disclosure of the individual's entire medical record.

Notice of Privacy Practices. Privacy Notice, or NOPP: A description, provided to Members or patients at specific times, and to other persons upon a request of the Covered Entity's practices concerning its uses and disclosures of PHI, which also informs Members or patients of their rights and of the Covered Entity's legal duties, with respect to PHI. To the extent that the NOPP contradicts the terms a term of this Manual or includes a term not otherwise addressed herein, the NOPP governs as to applicable System policy as to the System's Self-funded Group Health Plans.

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.[xiii]

Office of Employee Benefits or OEB: The System office charged by The University of Texas System with implementing the uniform benefit program, including a Self-funded Group Health Plan subject to HIPAA, for its employees and retired employees and administering the insurance coverage and other benefits provided under the Uniform Insurance Benefits Act for Employees of The University of Texas System and The Texas A&M System.

Payment: Activities undertaken by a Health Plan or other Covered Entity to obtain premiums or to determine its responsibility for coverage and provision of benefits under the 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.[xiv]

Personal Representative: A person with authority under applicable state or federal law to act on an Individual's behalf in connection with the Individual's PHI, including a person with authority to act on behalf of a deceased Individual or the Individual's estate.

Plan Sponsor: An employer that maintains a group health plan for its employees.[xv] A plan sponsor is *not* a covered entity under HIPAA. Thus HIPAA does not regulate plan sponsors.

Privacy Officer: The person designated to serve as the Privacy Officer for The University of Texas System Administration or the person's authorized designee.

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.[xvi]

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.[xvii] The System's Self-funded Health Plans do not maintain psychotherapy notes. However, other System office's within the System Health Care Component may retain Psychotherapy Notes on behalf of another Covered Entity as its Business Associate.

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.[xviii]

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 of the Secretary has been delegated).[xix]

Self-funded Health Plan(s) or Plan(s): Group Health Plan coverage that is offered to Members of The University of Texas System pursuant to the Uniform Insurance Benefit Act for Employees of The University of Texas System and The Texas A&M University System, *Texas Insurance Code* Chapter 1601 (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.

Summary Health Information: Information that summarizes the claims history, claims expenses, or types of claims experienced by individuals to or on whose behalf the Company has provided health benefits under the 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).[xx]

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.[xxi]

Underwriting Purposes Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); the computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); the application of any pre-existing condition exclusion under the plan, coverage, or policy; and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

The University of Texas System: The institutions and other entities, including The University of Texas System Administration, that comprise The University of Texas System.

The University of Texas System Administration or System: The offices 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.

Using, a Use, or To Use: Both (i) employment, application, utilization, examination, or analysis of information, and (ii) sharing information *within* an entity.[xxii]

---

[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.* § 164.501.

[xiii] *Id.* § 164.510(b)(1).

[xiv] *Id.* § 164.501.

[xv] *Id.* § 164.504(f).

[xvi] *Id.* §§ 160.103, 164.501.

[xvii] *Id.* § 164.501.

[xviii] *Id. §*164.504(f).

[xix] *Id.* § 160.103.

[xx] *Id.* § 164.504(a)..

[xxi] *Id.* § 164.501.

[xxii] *Id.*