| **Policy Name:** Business Associate Agreements for HIPAA Compliance | |
|---|---|
| **Originating Officer (Title), Council, or Committee:**<br>Texas Health Chief Compliance Officer | **Effective Date:**<br>03/09/2017 |
| **Approved By:**<br>System Leadership Council | **Last Reviewed Date:**<br>03/09/2017 |
| **Page 1 of 9** | |

## *1.0* Scope:

*1.1* Applicable Entities:
This policy applies to Texas Health Resources and its member entities, Texas Health Group Health Plans, and excludes the Texas Health joint venture entities.

*1.2* Applicable Departments:
This policy applies to all departments.

## *2.0* Purpose:

*2.1* Provide guidelines for Uses by and Disclosures of Protected Health Information (PHI) to Business Associates (see Attachment A, Business Associate Decision Tree).

## *3.0* Policy Statement(s):

*3.1* An entity may disclose PHI to a Business Associate and allow the Business Associate to create, receive, maintain, or transmit PHI on its behalf if satisfactory assurances are obtained that the Business Associate will appropriately safeguard the information. An entity is not required to obtain such satisfactory assurance from a Business Associate's Subcontractors.

*3.2* A Business Associate may disclose PHI to a Subcontractor and allow the Subcontractor to create, receive, maintain, or transmit PHI on its behalf, if satisfactory assurances are obtained that the Subcontractor will appropriately safeguard the information.

*3.3* Such assurances must be documented through a written contract with the Business Associate that meets the requirements of this policy.

*3.4* This policy does not apply to Disclosures by the entity to a Health Care Provider concerning the Treatment of the Individual.

## *4.0* Policy Guidance:

*4.1* Business Associate Agreements

*4.1.1* A Business Associate agreement will establish the permitted and required Uses and Disclosures of PHI by the Business Associate (Privacy Rule and Security Rule). The agreement may not authorize the Business

Associate to use or further disclose the PHI in a manner that would violate the Privacy Rule requirements if done by the covered entity, except that the agreement may permit the Business Associate to:

a. Use and disclose PHI for its proper management and administration; and

b. To provide data aggregation services relating to the health care operations of the entity.

*4.1.2* An entity may disclose PHI to a Business associate for De-identification purposes, whether or not the De-identified information is to be used by the covered entity.

*4.1.3* The Business Associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

*4.1.4* The agreement will be in the format provided by Texas Health Legal Services and at a minimum will provide that the Business Associate will:

a. Not Use or further Disclose the PHI other than as permitted or required by the agreement or as required by law (Privacy Rule);

b. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic PHI, to prevent Use or Disclosure of the PHI other than as provided for by the agreement (Privacy Rule);

c. Report to the entity any Use or Disclosure of the PHI not provided for by the agreement of which it becomes aware (Privacy Rule), including breaches of unsecured PHI as required. (Breach Notification Rule);

1) If a business associate is acting as an agent of the entity (as determined under the Federal common law of agency), then the business associate's discovery of the breach will be imputed to the entity for purposes of starting the sixty day clock on the entity's required breach notifications.

2) If the business associate is not acting as an agent of the entity, then the entity is required to provide the breach notifications no later than sixty days from when the business associate notifies the entity of the breach.

d. Report to the entity any Security Incident of which it becomes aware (Security Rule);

e. Ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate (Privacy Rule and Security Rule);

f. Make available the PHI as needed to comply with requests by Individuals for Access to (including electronic copies) or amendment of their PHI, or for an accounting of Disclosures of their PHI (Privacy Rule);

g. To the extent the Business Associate is to carry out an entity's obligation under the Privacy Rule, comply with the Privacy Rule requirements that apply to the entity in the performance of such obligation.

h. Make its internal practices, books and records relating to the Use and Disclosure of PHI received from the entity available to the Secretary of Health and Human Services as needed to determine the entity's or Business Associate's compliance with the Business Associate requirements. (Privacy Rule).

i. The Business Associate agreement must provide for return or destruction, if feasible, of all PHI received from the entity, at termination of the agreement. If such return or destruction is not feasible, the protections of the agreement will be extended to the information and limit further Uses and Disclosures (Privacy Rule).

*4.1.5* The Business Associate agreement must authorize termination of the agreement by the entity if it has been determined that the Business Associate has violated a material term of the agreement (Privacy Rule and Security Rule).

*4.2* Business Associate Agreement Compliance

*4.2.1* If the entity becomes aware of an activity or practice of the Business Associate that constitutes a material breach or violation of the terms of the agreement, the entity must take reasonable steps to cure the breach or end the violation (Privacy Rule and Security Rule).

*4.2.2* If the Business Associate becomes aware of an activity or practice of a Subcontractor that constitutes a material breach or violation of the terms of the agreement, the Business Associate must take reasonable steps to cure the breach of end the violation.

*4.2.3* If such steps are unsuccessful, the entity or Business Associate must terminate the agreement if feasible.

*4.2.4* Reporting of potential breaches or Security Incidents should be performed according to the Texas Health policy on Information Privacy and Security Inquiries, Complaints and Breaches. Prior to contract renewal with Business Associates, the entity should review any reported breaches involving that Business Associate.

*4.3* HIPAA Effective Date: This policy will become effective September 23, 2013.

***5.0*** **Definitions:**

*5.1* Access - Inspect and/or obtain a copy of PHI in a Designated Record Set.

*5.2* Breach

*5.2.1* Means the acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI. Breach excludes:

a. Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of the entity or a Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure.

b. Any inadvertent disclosure by a person who is authorized to access PHI at an entity or Business Associate to another person authorized to access PHI at the same entity or Business Associate, or Organized Health Care Arrangement in which the entity participates, and the information received as a result of such disclosure is not further used or disclosed.

c. A disclosure of PHI where the entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

*5.2.2* An acquisition, access, use or disclosure of PHI is presumed to be a breach unless the entity or business associate demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, included the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk to the PHI has been mitigated.

*5.3* Business Associate - Any third party who performs or assists in the performance of a function or service on behalf of Texas Health that creates, receives, maintains, or transmits PHI. Such participation is not in the capacity of a member of the Workforce, and may involve claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing.

Business Associates include third parties who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where such provision involves the Disclosure of PHI, and is not conducted in the capacity of a member of the Workforce.

Business Associates also include Health Information Organizations, E-prescribing Gateways, or other persons that provides data transmission services with respect to PHI to a Texas Health entity and that requires access on a routine basis to PHI; a person that offers a personal health record to one or more individuals on behalf of Texas Health; or a Subcontractor that creates, receives, maintains or transmits PHI on behalf of the Business Associate.

*5.4* Covered Entity - Health care provider, plan or clearinghouse covered by the HIPAA Privacy Rule.

*5.5* De-identification - Assurance that health information is not individually identifiable by either: (1) removal of specified identifiers of the individual or relatives, employers, or household members of the individual; or (2) determination by a knowledgeable individual 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. (See Texas Health Policy on De-Identification of Health Information for full definition.)

*5.6* Disclosure - Any release, transfer, provision of access to, or divulging of PHI outside the entity holding the information.

*5.7* Group Health Plan - Texas Health -sponsored group health plan (GHP) providing for medical, dental, vision or health care spending reimbursement. Certain functions of the GHP may be delegated to Third Party Administrators (TPA).

*5.8* Health Care Provider - A provider of medical services including: institutional providers (such as hospitals, skilled nursing facilities, home health agencies, comprehensive outpatient rehabilitation facilities); facilities and practitioners (including clinics and centers, physicians, clinical laboratories, pharmacies, nursing homes, licensed/certified health care practitioners and suppliers of durable medical equipment); and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

*5.9* Health Information - Any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a provider, plan, employer or clearinghouse; and that relates to the past, present, or future health condition of an Individual as well as the provision of healthcare to the Individual.

*5.10* Individual - The subject of Health Information. This includes patients, Group Health Plan participants and their covered dependents. Legally Authorized Representatives will be accorded the same rights regarding Uses and Disclosures of Health Information as the Individual.

*5.11* Individually Identifiable Health Information (IIHI) - Health Information that identifies the Individual or provides a reasonable basis for doing so, by virtue of containing one or more of the eighteen identifiers specified by the Privacy Rule.

*5.12* Legally Authorized Representative -

*5.12.1* A parent or legal guardian, if the patient is a Minor;

*5.12.2* A legal guardian, if the patient has been found by a court to be incapable of managing the patient's personal affairs;

*5.12.3* An agent of the patient authorized under a Medical Power of Attorney for the purpose of making a health care decision when the patient is incompetent;

*5.12.4* An attorney ad litem and/or guardian ad litem appointed for the patient by a court;

*5.12.5* A person authorized to consent to medical treatment on behalf of the patient under Chapter 313 of the Texas Consent to Medical Treatment Act

*5.12.6* A personal representative or heir of the patient, if the patient is deceased;

*5.12.7* An attorney retained by the patient or by the patient's legally authorized representative;

*5.12.8* A person exercising a power granted to the person in the person's capacity as an attorney-in-fact or agent of the patient by a Statutory Durable Power of Attorney that is signed by the patient as principal. (See Texas Health Policy on Health Information Uses and Disclosures for full definition.)

*5.13* Privacy Rule - The Health Insurance Portability and Accountability Act of 1996 Final Privacy Rule.

*5.14* Protected Health Information (PHI) - Individually Identifiable Health Information that is protected by the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

*5.15* Security Rule - The Health Insurance Portability and Accountability Act of 1996 Final Security Rule.

*5.16* Security Incident - Any adverse event that comprises some aspect of computer or network security. Examples of incident categories are: loss of confidential information, compromise of the integrity of the information, denial of service, misuse of service, systems or information, or damage to systems.

*5.17* Subcontractor - Means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a Workforce member of the Business Associate.

*5.18* Treatment - The provision, coordination, or management of health care and 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; or the referral of a patient for health care from one Health Care Provider to another.

*5.19* Use - The sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains the information.

*5.20* Workforce - Employees, volunteers, persons involved in Texas Health training programs or those sponsored by its wholly owned or wholly controlled entities, and other persons who conduct, in the performance of work for an entity or Business Associate, is under the direct control of such entity or Business Associate, whether or not they are paid by the entity or Business Associate.

## *6.0* Responsible Parties:

*6.1* Entity Privacy Officer

*6.1.1* Implementation and oversight of this policy is the responsibility of the entity privacy officer at the entity level.

*6.2* Workforce Members

*6.2.1* It is the responsibility of all Workforce members to comply with this policy.

## *7.0* External References:

*7.1* HIPAA Breach Notification of Unsecured PHI. 45 C.F.R. Part 160 and Part 164, Subpart D §164.410.

*7.2* HIPAA Privacy Rule. 45 C.F.R. Part 160 and Part 164, Subpart E §164.502(a) and (e), §164.504(e), §164.505(b).

*7.3* HIPAA Security Rule. 45 C.F.R. Part 160 and Part 164, Subpart C.

## *8.0* Related Documentation and/or Attachments:

*8.1* Accounting of Disclosures of Health Information Policy - THR System Policy

*8.2* Amending Health Information - THR System Policy

*8.3* Breach Notification - THR System Policy

*8.4* Business Associate Decision Tree - Attachment A

*8.5* De-Identification of Health Information - THR System Policy

*8.6* Health Information Uses and Disclosures - THR System Policy

*8.7* Information Privacy and Security Incidents, Inquiries, Complaints and Breaches Policy - THR System Policy

*8.8* Minimum Necessary Use and Disclosure of Health Information Policy - THR System Policy

*8.9* Patient Access to Health Information - THR System Policy

*8.10* Safeguarding Health Information and Sensitive Personal Information - THR System Policy

## *9.0* Required Statements:

Not Applicable

**Attachment A**

**Business Associate Decision Tree**

Use the following decision tree to determine if the recipient of PHI is a business associate.