11.1.3 Business Associates

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
Section: 11.1 General Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

I. Purpose

This policy defines the guidelines and procedures that must be followed for Business Associates who come into contact with protected health information to protect the confidentiality and integrity of health information.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held, or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Requirements

All UT Health San Antonio workforce members must observe the following standards when entering into a Business Associate contract:

1. The contract must contain specific language as provided by the Office of Legal Affairs.
2. Limit access to PHI to the minimum necessary to accomplish the intended purpose of the contractual relationship.
3. The contract must include language that provides the Business Associate will:
    a. Acknowledge enforcement and compliance with HIPAA security and privacy regulations.

b. Implement appropriate administrative, physical, and technical safeguards compliant with the HIPAA security rule to ensure the confidentiality, integrity, and security of PHI.

c. Not use or further disclose information other than as permitted or required by the contract or as required by law.

d. Use appropriate safeguards to prevent use or disclosure of information other than as provided for by its contract.

e. Report to UT Health San Antonio without unreasonable delay and in no case later than 10 days any use or disclosure of information not provided for by its contract of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR § 164.410 - *Notification by a business associate*.

f. Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created by or on behalf of, UT Health San Antonio, agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information.

g. Make available PHI in accordance with IHOP policy 11.3.6 Access to Protected Health Information.

h. Make available PHI for amendment and incorporate any amendments in accordance with IHOP policy 11.3.2 Patient Right to Amend Patient Health Information.

i. Make available information required to provide an accounting of disclosures in accordance with IHOP policy 11.3.1 Accounting of Disclosures of Protected Health Information.

j. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created by or on behalf of UT Health San Antonio, available to Department of Health and Human Services (DHHS) for purposes of determining UT Health San Antonio's compliance; and

k. At termination of the contract, if feasible, return or destroy all PHI received from, or created by or on behalf of, UT Health San Antonio that the Business Associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

B. Contract Violations

1. If UT Health San Antonio becomes aware of a practice or pattern that constitutes a material breach of this policy or violation of the Business Associate's obligations under its contract, UT Health San Antonio will take reasonable steps to cure the breach or to end the violation.

2. In the event that the Business Associate cannot or will not remedy the practice or pattern, UT Health San Antonio will terminate the contract. If termination is not feasible, the individual or department involved must contact UT Health San Antonio's Institutional Compliance and Privacy Office for reporting to DHHS as required.

C. Exceptions

Certain parties performing activities involving UT Health San Antonio PHI may not be required to sign a Business Associate Agreement (BAA). UT Health San Antonio personnel should consult with the Institutional Compliance and Privacy Office and the Office of Legal Affairs to make this determination. Some examples of categories of persons who may not be required to sign a Business Associate Agreement include but is not limited to:

1. Workers who are not employed by UT Health San Antonio but work mostly on-site at a UT Health San Antonio controlled site, and who are deemed to be part of UT Health San Antonio's workforce;
2. Entities participating in an Organized Healthcare Arrangement with UT Health San Antonio;
3. Certain affiliates of UT Health San Antonio; or
4. Persons performing legally required functions or activities on behalf of UT Health San Antonio, provided that UT Health San Antonio shall attempt to obtain satisfactory assurances that the PHI shall be held confidential as required by *45 Code of Federal Register (CFR) 164.504(e) Uses and Disclosures: Organizational Requirements*, and, if no such assurance is obtained, UT Health San Antonio shall document its attempts and the reason that assurances could not be obtained.

D. Existing Contracts

1. The Office of Legal Affairs will review existing UT Health San Antonio contracts with outside vendors that involve the use or disclosure of PHI in order to determine whether such contracts need to be amended to include Business Associate Agreement provisions.
2. UT Health San Antonio workforce members have an obligation to forward to the Office of Legal Affairs any existing vendor contract if such contract:
    a. involves the use or disclosure of PHI by the vendor and,
    b. has not already been reviewed and approved by the Office of Legal Affairs.

IV. Definitions

Terms used in this document, have the meaning set forth in the Patient Privacy Policies Glossary *unless a different meaning is required by context.*

V. Related References

For questions regarding this policy, contact the Privacy Program Director at 210-567-2014 or email compliance@uthscsa.edu.

Health Insurance Portability and Accountability Act (HIPAA) of 1996
HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164
HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 1644

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
04/2003	Policy Origination		
04/2010	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review, discretionary edits	ICPO	01/05/23