



New Developments in Safeguarding Protected Health Information During 2017

**Submitted to the House Committee on Public Health
and the Senate Committee on Health and Human Services**

Health and Human Services Commission

December 2017

INTRODUCTION

House Bill 300, 82nd Legislature, Regular Session, 2011 (H.B. 300), added Government Code Section 531.0994, requiring the Health and Human Services Commission (HHSC), in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, to explore and evaluate new developments in safeguarding Protected Health Information (PHI). By December 1st of each year, HHSC must report to the legislature about new developments in safeguarding PHI and make recommendations for the implementation of PHI safeguards within HHSC.

BACKGROUND

Numerous state and federal laws require safeguards over PHI. A Texas covered entity, as defined by the Texas Medical Records Privacy Act, Chapter 181, Health and Safety Code, that uses or discloses identifiable PHI, must comply, to the extent possible, with the following confidentiality standards and safeguard requirements.

- The Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, as amended, and its implementing regulations, Title 45 of the Code of Federal Regulations, Parts 160 and 164.
- The Texas Medical Records Privacy Act, Texas Health and Safety Code, Chapter 181.
- The Texas Identity Theft Enforcement and Protection Act, Texas Business and Commerce Code, Chapter 521.
- Laws and regulations governing specific types of information, individuals, facilities, and provider types, as summarized in Appendix A.

The HHS system must also comply with other confidentiality requirements:

- Benefit program use, disclosure, and safeguard requirements, such as those required by federal Medicaid law.
- Federal data sharing agreements with the Social Security Administration and the Internal Revenue Service, which contain specific privacy and security requirements.
- State regulations relating to information security, including Title 1 of the Texas Administrative Code, Chapters 202 (Information Security) and 390 (Information Practices).

NEW DEVELOPMENTS IN SAFEGUARDING PHI

Changes in Federal Law and Policy

There have been no relevant changes to HIPAA regulations or guidance in 2017. However, the U.S. Department of Health and Human Services, Office of Civil Rights (HHS-OCR), which is responsible for enforcing HIPAA, once again issued a number of press releases in 2017 highlighting significant HIPAA enforcement efforts that resulted in large fines and mandatory corrective action¹.

¹ <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/>.

HHS System Initiatives

In 2017, the HHS system continued efforts to improve its privacy and security practices, including:

- Adopting HHS system policy establishing the role of the HHS Privacy Office in creating system-wide policies for safeguarding confidential information; reporting, responding to, and remediating privacy breaches and violations; and providing training to HHS staff and third-party contractors.
- Promulgating privacy policies and procedures to be utilized as the standard for protecting client confidential information and responding to potential compromises of client protected health information.
- Drafting the federally-required Hybrid Covered Entity Statement, acknowledging the HHS system's HIPAA covered and non-covered functions for purposes of the federal Privacy Rule.
- Updating HHS system privacy training to be in compliance with the updated Privacy and Omnibus Rule.
- Holding the annual Cybersecurity Awareness Fair, designed to educate employees about the information security and privacy issues affecting the HHS agencies.
- Reviewing HIPAA training, reporting, compliance with the state hospitals and state supported living centers.
- Updating the information security risk management process to include third parties, which requires all contractors to sign the HHS Data Use Agreement (DUA). The newly-updated DUA better outlines the requirements for contractors to protect and safeguard agency confidential information whether oral, written, or electronically stored or transmitted and requires annual attestation to compliance with the Security and Privacy Initial Inquiry form submitted with the DUA.
- Developing and implementing an IT Security Risk Assessment tool called the Government Utility for Agency Risk Determinations (GUARD) tool.

RECOMMENDATION

HHS Privacy Office recommends that HHSC continue to conduct proactive efforts, as described in this report to safeguard PHI within the system.

Appendix A

Covered entities, such as HHSC, must comply with a number of state or federal laws or regulations that require confidential information to be safeguarded and used or disclosed only for authorized persons and purposes, as applicable.

HHSC promulgated rules in Title 1 of the Texas Administrative Code, Chapter 390, Information Practices, applicable to "covered entities," as defined by the Texas Medical Records Privacy Act, Health and Safety Code, Section 181.001(b)(2). The rule requires covered entities that electronically exchange, use or disclose PHI to comply with the minimum standards for confidential information in any form, and for specific types of information, individuals or facility types.

Specific Types of Confidential Information, include:

- Cancer
- HIV/AIDS
- Genetic
- Sexual assault
- Communicable diseases
- Mental health
- Substance abuse or substance use disorder
- Immunizations
- Bureau of Vital Statistics
- Reports of abuse or neglect
- Federal tax information
- Social Security Administration data
- Occupational diseases
- Family planning
- Recipients of government benefits
- Individuals receiving intellectual and disability services
- Educational records

Specific Types of Providers, Facilities, or Services, such as:

- Hospitals
- Nursing facilities
- Intermediate care facilities for persons with an intellectual disability or related conditions
- Freestanding emergency medical care facilities
- Ambulatory surgical centers
- Emergency medical services
- Physicians
- Chiropractors
- Dentists
- Labs

- Pharmacists
- Podiatrists
- Personal health record vendors
- End stage renal disease facilities
- Special care facilities for AIDS
- Private psychiatric hospitals and crisis stabilization units
- Birthing centers
- Dyslexia therapists and dyslexia practitioners
- "Promotores" or community health workers
- Medical radiologic technologists
- Licensed chemical dependency counselors and treatment facilities

Specific Types of Individuals, such as:

- Minors and Children with Special Health Care Needs Services Program
- Early and Periodic Screening, Diagnosis, and Treatment