TT

New Developments in Safeguarding Protected Health Information During 2018

As Required by

Texas Government Code

Section 531.0994

Health and Human Services Commission

November 2018

TEXAS
Health and Human Services

Table of Contents

1. Introduction

House Bill 300, 82nd Legislature, Regular Session, 2011 (H.B. 300), added section 531.0994 to the Texas Government Code, 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.

This report is intended to meet the requirement of H.B. 300. The report documents the efforts of HHSC and the health and human services system (collectively, HHS) to explore and evaluate new developments in safeguarding PHI, in coordination with other agencies and entities, and makes recommendations for implementation of PHI safeguards within HHSC.

2. 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.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, as amended and regulated thereunder, in 45 Code of Federal Regulations Parts 160 and 164.
- Texas Medical Records Privacy Act, Texas Health and Safety Code, Chapter 181.
- 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.
- Benefit program use, disclosure, and safeguard requirements, such as required by Medicaid.
- Federal data sharing agreements with the Social Security Administration and the Internal Revenue Service, which contain privacy and security requirements.
- State regulations over information security included in 1 Texas Administrative Code, Chapters 202 (Information Security) and 390 (Information Practices).

HHS must also comply with other confidentiality requirements.

3. New Developments in Safeguarding PHI

Changes in Federal Law and Policy

There have been no relevant changes to HIPAA regulations or guidance in 2018. The enforcement arm for HIPAA, the United States Department of Health and Human Services' Office for Civil Rights (OCR), issued a number of press releases in 2018 highlighting significant HIPAA enforcement efforts by OCR with several high-profile privacy breaches, resulting in large fines and required corrective action[1]. OCR publications noted that security risk assessments were not as comprehensive as required by the United States Department of Health and Human Services. Business Associates and Business Associate Agreements of Covered Entities were a major target for the Phase II Audits performed by OCR during the 2016-2018 time frame[2].

HHS Accomplishments and Initiatives to Improve Safeguard Activities

In 2017, HHS developed and implemented a new risk assessment protocol which brings the agency into alignment with the regular security audits required by HIPAA. In 2018, HHS made a number of improvements for safeguarding PHI through developments in its privacy and security programs, improvements in agency contracting standards, and changes in human resources policy.

Privacy Program

The HHS Privacy Division leads incident response teams investigating actual or suspected privacy breaches, works with program or business areas to self-assess privacy compliance and risks, evaluates compliance with federal and state privacy laws and regulations, and oversees implementation of H.B. 300.

---

[1] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/.
[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

In 2018, HHS Privacy Division crafted a comprehensive privacy program including a compliance and monitoring program designed to complement HHS Information Security advances and activities to safeguard PHI and other agency confidential information. These efforts included:

- Adding a copy of the HHS Notice of Privacy Practices to annual client notices as best practice and in compliance with HIPAA.
- Posting system-wide privacy policies and procedures on the HHS internal website to be utilized as the minimum standard for protecting client confidential information and responding to potential compromises of client PHI.
- The HHS Privacy Division went through a baseline internal audit and is in the process of implementing the recommendations.
- Redesigning the Privacy Division websites, both internal and external, to provide more resources and post required statements.
- Participating regularly in the Cybersecurity Awareness Fair designed to educate employees about the information security and privacy issues affecting the HHS agencies, most recently presenting information about privacy and how it relates to information security.
- Collaborating with IT Security and IT system administrators to improve categorizing HHS systems that receive, create, store or transmit HHS confidential information, including PHI.
- Coordinating with state hospitals and state supported living centers regarding privacy training, privacy incidents and incident reporting.
- Beginning an outreach program to engage with the state hospitals and state supported living centers.
- Working with Procurement and Contract Services to implement a monitoring program of Business Associates and their Data Use Agreements.
- Partnering with HHS Information Security to implement a Privacy Threat Analysis and Privacy Impact Assessment program.

Information Security Program

In 2018, HHSC strengthened Information Technology (IT) safeguards over PHI as follows:

- HHS IT Security continued implementation of an IT Security Risk Assessment tool called the Government Utility for Agency Risk Determinations (GUARD) tool and completed a full risk assessment of all Department of Aging and Disability Services (DADS) legacy systems (systems that transferred to HHS on 9/1/17).
- Information Security began a program to engage with all the DADS legacy systems using the GUARD tool as a baseline for system risk management.

- The GUARD tool was adjusted to be used for information system categorization.
- The GUARD tool will be used system wide to establish security plans for each information system within HHS beginning with DADS legacy systems.

4. Recommendations

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

Appendix A. Texas Medical Records Privacy Act

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 a rule in 1 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
- "Promotors" 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

Appendix B. Texas Medical Records Privacy Act Report FY 2018

Texas Health and Human Services System

I. Total number of Consumer Complaints Received: 183

II. Complaints by Alleged Violations

- Failure to Provide required training: 8
- Failure to Provide Notice: 0
- Failure to provide Access: Health Record: 0
- Unlawful/Unauthorized disclosure of PHI: 175
- Unlawful Marketing: 0

III. Total Disciplinary/Enforcement Actions

- Counseling: 35
- Termination: 1
- Retraining: 19

Total number of actions taken: 55

Texas Health and Human Services Commission: Program 1 (Licensed Providers)

I. Total number of Consumer Complaints Received: 595

II. Complaints by Alleged Violations: 129

- Failure to provide required training: 1
- Failure to provide Notice: 0
- Failure to provide Access: Health Record: 1
- Unlawful/Unauthorized disclosure of PHI: 100
- Unlawful marketing: 27

IV. Total Disciplinary/Enforcement Actions

Total number of actions taken: 181

- Administrative Penalty: 57
- Cease and Desist: 0
- Disciplinary Surrender: 6
- Licensure Expiration: 31
- Probated Suspension: 2
- Probation: 1
- Reprimand: 1
- Revocation: 2
- Suspension: 0
- Voluntary Surrender: 0
- Warning: 74

Texas Health and Human Services Commission: Program 2 (Regulated Health Facilities)

Total Number of Consumer Complaints Received: 0

Texas Health and Human Services Commission: Program 3 (Emergency Medical Services)

Total Number of Consumer Complaints Received: 0

Texas Health and Human Services Commission: Program 4 (Substance Abuse or Narcotic Treatment Facilities)

I: Total Number of Consumer Complaints Received: 2

II: Complaints by Alleged Violations:

- Failure to Provide required training: 0
- Failure to Provide Notice: 0
- Failure to provide Access: Health Record: 1
- Unlawful Marketing: 0
- Unlawful/Unauthorized disclosure of PHI: 1

III. Total Disciplinary/Enforcement Actions: 0