

**Audits of Covered Entities  
And  
New Developments in  
Safeguarding Protected  
Health Information  
During Fiscal Year 2020**

---

**As Required by  
Health and Safety Code,  
Section 181.206**

**and**

**Government Code,  
Section 531.0994**

**Health and Human Services Commission**

**September 2020**



**TEXAS**  
Health and Human  
Services

## **1. Introduction**

Pursuant to House Bill 300, 82nd Legislature, Regular Session, 2011, HHSC submits this combined report on audits of covered entities and new developments in safeguarding protected health information in fiscal year 2020.

## 2. Background

House Bill 300, 82nd Legislature, Regular Session, 2011 (H.B. 300), amended Chapter 181 of the Health and Safety Code (the Texas Medical Records Privacy Act) and Chapter 531 of the Government Code.

Citing the increased adoption of electronic health record systems and the associated expansion of the electronic exchange of protected health information, H.B. 300 was intended to increase privacy and security protections under state law for protected health information. To this end, H.B. 300 required the Health and Human Services Commission (HHSC) to prepare and submit two annual reports.

The reporting requirement in Chapter 181 concerns audits of "covered entities," as that term is defined in federal law. The current text of Section 181.206 reads:

Sec. 181.206. AUDITS OF COVERED ENTITIES.

- (a) The commission, in coordination with the attorney general and the Texas Department of Insurance:
  - (1) may request that the United States secretary of health and human services conduct an audit of a covered entity, as that term is defined by 45 C.F.R. Section 160.103, in this state to determine compliance with the Health Insurance Portability and Accountability Act and Privacy Standards; and
  - (2) shall periodically monitor and review the results of audits of covered entities in this state conducted by the United States secretary of health and human services.
- (a-1) Notwithstanding Subsection (a), the commission shall also coordinate with the Texas Health Services Authority when requesting an audit or monitoring and reviewing the results of an audit under Subsection (a). This subsection expires September 1, 2021.
- (b) If the commission has evidence that a covered entity has committed violations of this chapter that are egregious and constitute a pattern or practice, the commission may:
  - (1) require the covered entity to submit to the commission the results of a risk analysis conducted by the covered entity if required by 45 C.F.R. Section 164.308(a)(1)(ii)(A); or
  - (2) if the covered entity is licensed by a licensing agency of this state, request that the licensing agency conduct an audit of the covered entity's system to determine compliance with the provisions of this chapter.

- (c) The commission annually shall submit to the appropriate standing committees of the senate and the house of representatives a report regarding the number of federal audits of covered entities in this state and the number of audits required under Subsection (b).

The reporting requirement in Chapter 531 of the Government Code concerns HHSC's efforts to explore and evaluate new developments in safeguarding protected health information. The current text of Section 531.0994 reads:

Sec. 531.0994. STUDY; ANNUAL REPORT.

- (a) The commission, in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, shall explore and evaluate new developments in safeguarding protected health information.
- (b) Not later than December 1 each year, the commission shall report to the legislature on new developments in safeguarding protected health information and recommendations for the implementation of safeguards within the commission.

### **3. Audits of Covered Entities**

#### **Federal Audits of Covered Entities**

The U.S. Department of Health and Human Services, Office for Civil Rights (DHHS-OCR), is responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA) and federal audits of HIPAA-covered entities. DHHS-OCR does not release the identity of the entities it audits or the results of those audits.

Because DHHS-OCR does not release this information, HHSC is unable to accurately report the number of federal audits of covered entities in Texas. The only circumstance where HHSC would learn of action by DHHS-OCR is when that action involves HHSC, a health and human services system (HHS) agency, or an HHS agency's business associate doing business on behalf of the agency.

HHSC is not aware of any federal audit of HHSC, an HHS agency, or an HHS agency's business associate.

#### **State Required Audits and Security Risk Analyses by Covered Entities**

HHS system contractors are required to provide security risk assessments to HHS upon request following a privacy breach of electronic PHI to demonstrate compliance with HIPAA's administrative, physical, and technical safeguards.

In Fiscal Year 2020 there were no unauthorized releases of electronic protected health information by HHS system contractors that rose to the level of requiring a security audit. In Fiscal Year 2020 there was a ransomware attack on a subcontractor that involved HHSC client information. The attack was perpetrated on the company BRSI, a subcontractor of Accenture, the HHSC contracted administrator of Texas Medicaid & Healthcare Partnership. The number of affected Texas Medicaid & Healthcare Partnership clients notified by BRSI was 270,666. BRSI also sub-contracts for another HHSC covered entity contractor, Superior Health. The number of affected Texans notified by Superior Health was 122.

## 4. New Developments in Safeguarding Protected Health Information

### Changes in Federal Law and Policy

There have been no relevant changes to HIPAA regulations or guidance in 2019. The federal enforcement arm for HIPAA, DHHS-OCR, issued a number of notices to covered entities in 2020 giving guidance for disclosures of protected health information during the COVID-19 pandemic.

### HHS Accomplishments and Initiatives to Improve Safeguard Activities

In the middle of Fiscal Year 2020, HHS migrated much of its workforce to temporary teleworking status as part of the HHS system's response to the COVID-19 pandemic. HHS Information Security and the HHS Privacy Division continue to work together providing guidance, both technological and administrative, to HHS departments, divisions, units, programs and workforce.

### Privacy Program

The HHS Privacy Division investigates actual and suspected privacy breaches involving HHS agencies, 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.

In 2020, HHS Privacy Division continued developing its comprehensive privacy program, including compliance and monitoring programs designed to complement HHS Information Security advances and activities to safeguard PHI and other agency confidential information. These efforts included:

- Updating privacy training and obtaining permission for privacy training to be included in the mandatory annual training list.
- Collaborating with IT Security and IT system administrators to improve categorization of HHS systems that receive, create, store or transmit HHS confidential information, including PHI.
- Continuing to conduct on-site visits at the state hospitals and state supported living centers to engage and support privacy efforts at HHS facilities.
- Updating the privacy compliance program to accommodate developing programs and assist IT Security in Privacy Risk assessment for software.
- Continued review of Privacy Threat Analysis and implementing Privacy Impact Assessment Protocols.

## **Information Security Program**

In 2020, HHSC has improved Information Technology (IT) safeguards over PHI as follows.

- HHS IT Security has fully automated the IT Security Risk Assessment process within a nationally recognized Governance, Risk, and Compliance (GRC) solution.
- Information Security engages with all current and legacy systems within HHS. With the Legacy DADS systems they completed the inventory of all electronic equipment, data systems, and applications that contain or store ePHI and conducted a comprehensive Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI.
- All information system categorization is now automated
- The GRC solution is now fully implemented and is being used system-wide to establish security plans for each information system within HHS.

## **5. Recommendations**

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

## **List of Acronyms**

<b>Acronym</b>	<b>Full Name</b>
HHSC	Health and Human Services Commission
H.B.	House Bill
C. F. R.	Code of Federal Regulation
U.S.	United States
O.C.R.	Office for Civil Rights
PHI	Protected Health Information
HIPAA	Health Insurance Accountability and Accountability Act
BRSI	Business Recovery Services, Inc.
IT	Information Technology
GRC	Governance, Risk and Compliance
DADS	Department of Aging Disability Services