A Review of

State Entities' Preparedness for Compliance with the Health Insurance Portability and Accountability Act

SAO Report No. 03-048
August 2003

Overall Conclusion

Most state entities we reviewed must intensify their efforts to comply with administrative simplification regulations within the Health Insurance Portability and Accountability Act (HIPAA). The federal government can impose penalties for noncompliance with HIPAA; noncompliance also could lead to litigation that could require entities that are subject to HIPAA to pay substantial damages. The federal government enacted these regulations in 1996 to facilitate the exchange of information through the establishment of standards and requirements for the electronic transmission of certain health information. In addition, these regulations protect the privacy of health information and require that this information be properly secured.

Summary of Our Review

Our review was based on a survey of 76 state entities. The survey focused on the entities' preparedness for compliance with HIPAA administrative simplification regulations. We also asked these entities to submit supporting documentation for their survey answers and performed a limited review of that documentation.

Of the 76 entities we reviewed:

- Twenty-nine (38 percent) reported that they were subject to HIPAA regulations.
- One (1 percent) reported that, although it was not subject to HIPAA regulations, it had chosen to voluntarily comply with HIPAA regulations.
- Forty-six (61 percent) reported that they were not subject to HIPAA regulations. We reviewed the majority of the supporting documentation these entities submitted and determined that it reasonably supported their assertions.

The information in this report is primarily based on self-reported information and has not been subjected to the tests and confirmations that would be performed in an audit.

There are three categories of HIPAA administrative simplification regulations, each with a separate compliance deadline. Our review found that:

- More than half of the entities reviewed reported that they had not fully complied with certain HIPAA privacy regulations by the April 14, 2003, deadline. These entities will need to accelerate their efforts in this area.
- Nearly one-third of entities reviewed reported that they did not anticipate achieving full compliance with HIPAA regulations for transactions and code sets by the October 16, 2003, deadline. These entities may need to make a more concerted effort to comply.
- The deadline for complying with HIPAA security regulations is April 21, 2005, yet many entities reported that they have not started addressing major components of security regulations. It is important to note that the consolidation of Texas health and human services agencies (and the associated transition of information technology functions) will overlap with the time period during which entities will be working to comply with security regulations. This could increase the risk of not achieving compliance with security regulations.

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This review was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0133.

For more information regarding this report, contact Joanna B. Peavy, CPA, Audit Manager, at (512) 936-9500.

Compliance is critical to achieving HIPAA's intent. The federal government can impose penalties of $100 for each violation of HIPAA regulations, up to a $25,000 maximum penalty for all violations of the same requirement during a calendar year. Its enforcement process will be complaint-driven, and the federal government plans to use progressive steps to allow entities to demonstrate compliance or submit corrective action plans.

Individuals who knowingly violate HIPAA regulations are subject to penalties ranging from $50,000 to $250,000 and could be imprisoned for up to 10 years. The damages that entities that are subject to HIPAA could be required to pay as a result of lawsuits arising from the unauthorized disclosure of health information could be substantial.

Key Points

Entities have not conducted all required activities to achieve compliance with HIPAA privacy regulations.

Although more than half of the entities reported that they had not complied with certain privacy regulations by the deadline, many reported they had invested a significant amount of time and effort to conduct activities required to achieve compliance with those regulations. However, there was a noticeable degree of variation among entities, and not all entities have completed all required activities. For example, some entities have not established all required policies and procedures, while others have not provided required employee training. Entities' general efforts to establish safeguards to protect health information do not appear to be as strong as their efforts to address other privacy requirements.

Many entities reported that they have already experienced an increase in inquiries as a result of HIPAA privacy regulations. Some entities also reported that they have already received notice of suspected and confirmed violations of privacy.

Some entities reported that they were still in the process of conducting or had not started conducting certain activities to meet the upcoming deadline for compliance with transactions and code sets regulations.

Although the deadline for entities to begin using standard transactions and code sets is October 16, 2003, some entities reported that they were still in the process of conducting or had not started conducting certain activities to meet that deadline. For example, some entities have not yet assessed their systems that process electronic transactions to identify potential compliance issues. Other entities have not progressed far enough in testing to determine whether their business associates and trading partners will be able to comply with transactions and code sets regulations.

Only six entities reported they had established an overall plan to meet the deadline for compliance with security regulations.

Although the majority of entities anticipate achieving full compliance with security regulations, only six entities (20 percent) reported they had established an overall plan to meet the deadline for compliance. The majority of them also have not performed an overall assessment of the vulnerabilities of their information systems. Overall, entities do

not appear to be making significant progress in implementing HIPAA required and addressable security measures. While entities reported that they had started to implement many of these specifications, they frequently did not provide supporting documentation for that assertion.

The Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, includes certain state agency security requirements that are also included within HIPAA security regulations. Many entities reported that they have not started to address their data backup plans, system audit controls, and emergency procedures, all of which are required by both HIPAA security regulations and the TAC.

State entities reported they faced several challenges in achieving compliance with HIPAA.

Entities reported that they encountered difficulty in determining whether they are required to comply with HIPAA regulations. After making this determination, the primary challenges entities reported included lack of coordination and lack of staff. The complexity of HIPAA regulations contributes to the difficulties entities have experienced. Finding approaches to overcoming these difficulties is critical to entities' ultimately achieving compliance.

Summary of Objectives, Scope, and Methodology

Our objectives were to:

- Determine whether state entities are on schedule in achieving compliance with HIPAA administrative simplification regulations.
- Identify the activities state entities are conducting to help ensure they comply with HIPAA administrative simplification regulations.
- Identify the problems and concerns state entities have regarding achieving compliance with HIPAA administrative simplification regulations.

Our review focused on entities' compliance with HIPAA, Title II, Subtitle F – Administrative Simplification. We surveyed 76 entities in June and July 2003. Thirty entities reported that they were required to comply with or were voluntarily complying with HIPAA regulations. Forty-six reported that they were not required to comply with HIPAA regulations; we reviewed the majority of the supporting documentation these entities submitted and determined that it reasonably supported their assertions.

In addition to compiling the survey results, we also performed a limited review of the supporting documentation entities submitted to substantiate their answers to survey questions. However, the information in this report has not been subjected to the tests and confirmations that would be performed in an audit.