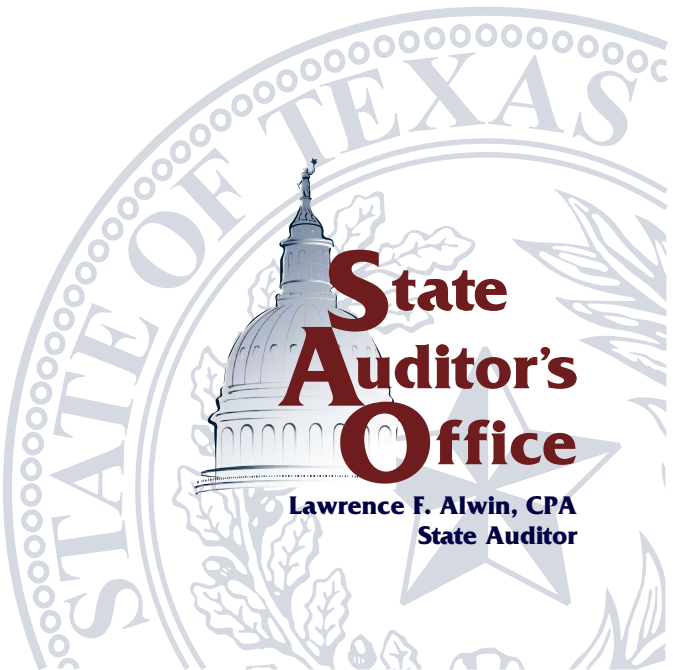
A Review of

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

August 2003

SAO Report No. 03-048



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.

Contents

Detailed Results

Appendices

Detailed Results

Introduction and Summary of Review

Introduction

Enacted in 1996, the Health Insurance Portability and Accountability Act's (HIPAA) purpose is to improve the portability and continuity of health insurance; combat waste, fraud, and abuse; promote the use of medical savings accounts; improve access to long-term care and coverage; and simplify the administration of health insurance.

Our review focused on entities' compliance with HIPAA, Title II, Subtitle F – Administrative Simplification. The goal of administrative simplification regulations is 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. Entities that must comply with HIPAA regulations are referred to as covered entities (see text box).

HIPAA Covered Entities and Hybrid Entities

Health plans, health care clearinghouses, and health care providers that conduct certain financial and administrative transactions electronically (such as eligibility, referral authorizations, and claims processing) are required to comply with HIPAA. Other entities may voluntarily comply with HIPAA.

An entity whose entire operations must comply with HIPAA regulations is referred to as a covered entity.

If only a portion of an entity's operations must comply with HIPAA regulations, the entity is referred to as a hybrid entity.

HIPAA administrative simplification regulations are grouped into three categories, each of which has a specific deadline for compliance:

- HIPAA privacy regulations (deadline for compliance was April 14, 2003). These regulations were designed to protect the privacy of individually identifiable health information.

- HIPAA transactions and code sets regulations (deadline for compliance is October 16, 2003). These regulations specify standards for electronic transactions and the code sets that entities must use within those transactions.

- HIPAA security regulations (deadline for compliance is April 21, 2005). These regulations specify standards for the security of health information and electronic signatures. Entities must adhere to these standards when developing and maintaining the security of all electronic individual health information.

Compliance with HIPAA regulations is critical to achieving HIPAA's purpose. 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. Individuals who knowingly violate HIPAA regulations are subject to penalties ranging from $50,000 to $250,000 and could be imprisoned for a maximum of 10 years.

In addition to penalties the federal government can impose, the damages that entities could be required to pay as a result of lawsuits arising from the unauthorized disclosure of health information could be substantial. The improper release of health information can expose individuals to serious risks, as cases outside of Texas have already illustrated:

- In Pennsylvania, authorities are investigating why hard copies of a hospital's patient records (containing patients' names, addresses, Social Security numbers, drug records, and test results) were found scattered on a street corner.[1]

- Published reports have described instances in which individuals assert they have been fired from their jobs based on information their employers learned about their medical conditions.[2]

- Hospitals have reported that hackers have altered electronic records regarding patients' drug dosages and medical tests.[3]

The federal government is relying on entities to comply with HIPAA, and its enforcement process will be complaint-driven. After violations of regulations come to its attention, the federal government plans to use progressive steps to allow entities to demonstrate compliance or submit corrective action plans.

Summary of 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. Twelve reported they were covered entities, while 17 reported they were hybrid entities.

- 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.

---

[1] Ann Wlazelek, "Law Requires Security for Medical Records, But Doesn't Specify How to Ensure It; Area Hospitals Take Somewhat Differing Approaches," *The Morning Call* (Allentown, PA), 9 August 2002, p. A2.

[2] Tom Abate, "Beef Up Patient Privacy Rules, Health Groups Say," *San Francisco Chronicle*, 11 November 1998, p. C4. Carol Kleiman, "Firms Challenge Medical Record Privacy," *The Record* (Bergen County, NJ), 27 December 1998, p. 5.

[3] "Patients' Computer Records at Risk," *Sunday Herald Sun* (Melbourne, Australia), 9 March 1997, p. 25.

Except where specifically noted otherwise, the results presented in Chapters 1 through 3 of this report cover the 30 entities that are required to or have chosen to voluntarily comply with HIPAA.

Several of the entities informed us that this review was the first inquiry they had received about the status of their compliance with HIPAA. Some expressed appreciation for the comprehensive nature of our survey instrument and stated that they planned to use it as a checklist to help ensure compliance with HIPAA. We are grateful to the entities for the efforts they made to complete our survey.

In addition to compiling entities' answers to survey questions, we performed a limited review of documentation entities submitted to substantiate their answers. However, the information in this report is primarily based on entities' self-reported information; it has not been subjected to the tests and confirmations that would be performed in an audit.

We plan to post aggregate information about responses to individual survey questions on the State Auditor's Office Web site (www.sao.state.tx.us) by September 30, 2003.

Chapter 1

Most Entities We Reviewed Must Intensify Their Efforts to Comply with HIPAA Regulations

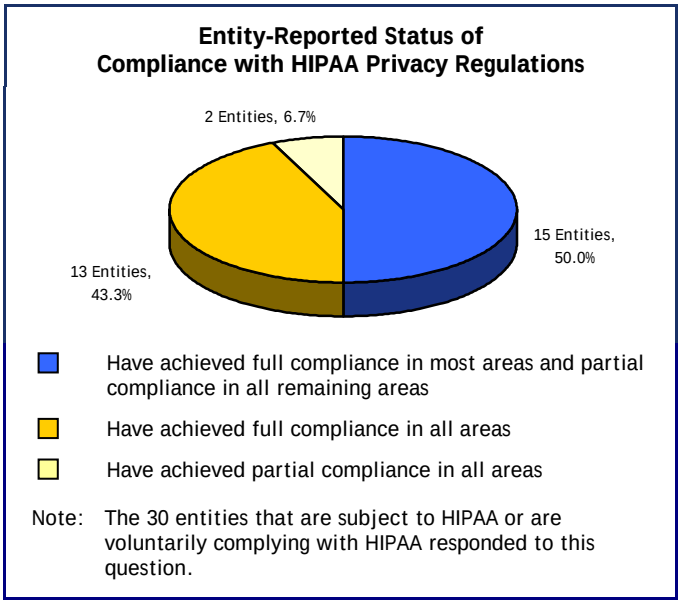
The results of our review indicate that more than half of the entities are behind schedule in complying with certain HIPAA privacy regulations and, therefore, will need to accelerate efforts to comply with those regulations. The deadline for compliance with transactions and code sets regulations was four months away when entities responded to our survey, yet nearly one-third of entities reported that they did not anticipate achieving full compliance by the deadline for those regulations. The results of our review in this area also dovetail with concerns expressed at the national level about entities' ability to achieve compliance with transactions and code sets regulations.

The deadline for compliance with security regulations was less than two years away when entities responded to our survey. While most entities reported that they anticipated achieving full compliance with security regulations by the deadline, many of them have not started addressing major components of the security regulations such as administrative, technical, and physical specifications. Promptly initiating efforts to address these components will be critical in achieving compliance by the deadline for security regulations.

The Deadline for Complying with Privacy Regulations was April 14, 2003, and Many Entities Need to Accelerate Their Efforts to Comply

More than half of the entities we reviewed are behind schedule in complying with privacy regulations and will need to accelerate their efforts in this area. As Figure 1 shows, only 13 entities (43.3 percent) reported that they had achieved full compliance with HIPAA privacy regulations as of the April 14, 2003, deadline. Fifteen entities (50 percent) reported that they were in full compliance in most areas of the privacy regulations and had achieved partial compliance in remaining areas such as training and the development of policies and procedures.

Figure 1



The remaining two entities (6.7 percent) reported that they were only partially compliant with privacy regulations as of the deadline. At the time these two entities responded to our survey, they were still in the process of providing training, establishing policies and procedures, and finalizing forms required by privacy regulations.

National Concerns Regarding Entities' Ability to Comply with Transactions and Code Sets Regulations

The Workgroup for Electronic Data Interchange (WEDI), an advisory body for the implementation of transactions and code sets regulations, has expressed concern at the national level that a substantial number of entities will not be able to comply with transactions and code sets regulations by the deadline. WEDI expressed a concern that many entities may have to revert to using hard copies, which is counter to HIPAA's intent.

In addition, WEDI's analysis led it to conclude that noncompliance with HIPAA transactions and code sets regulations could disrupt business transactions and payments. WEDI has pointed out that if only 5 percent of all transactions do not comply with HIPAA regulations, the associated disruption in payments to providers would have an adverse impact on the health care industry.

The Deadline for Complying with Transactions and Code Sets Regulations was October 16, 2003, and Some Entities May Need to Make a More Concerted Effort to Comply

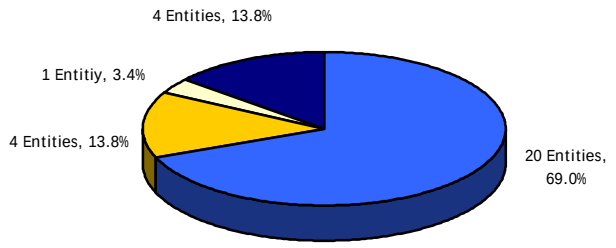
The transactions and code sets regulations deadline was four months away when entities responded to our survey. However, nearly one-third of these entities reported that they did not anticipate achieving full compliance by the October 16, 2003, deadline. Because the deadline is approaching, those entities may need to make a more concerted effort to comply. The results of our review also align with concerns expressed at the national level about entities' ability to achieve compliance with transactions and code sets regulations (see text box).

As Figure 2 shows:

- Twenty entities (69 percent) reported that they anticipated achieving full compliance with all transactions and code sets regulations by the deadline.
- Four entities (13.8 percent) reported that they anticipated achieving full compliance in most areas and will achieve only partial compliance in other areas. One of those four, for example, reported that it will not be able to accept all transactions electronically by the deadline.

Figure 2

Entity-Reported Status of Compliance with HIPAA Transactions and Code Sets Regulations



- Will achieve full compliance in all areas
- Will achieve full compliance in most areas and partial compliance in all remaining areas
- Will achieve partial compliance in all areas
- Other (These entities rely on contractors to comply with transactions and code sets regulations or report that it is not applicable to them.)

Note: Twenty-nine entities responded to this question; the remaining entity is relying on another entity for transactions and code sets work.

- One entity (3.4 percent) reported that it will be in partial compliance with all transactions and code sets regulations. Although it will not have completed system changes by the deadline, it plans to use a clearinghouse for the transmission of transactions until those changes are completed.
- Four entities (13.8 percent) are relying on contractors to comply with transactions and code sets regulations or reported that transactions and code sets regulations are not applicable to their operations.

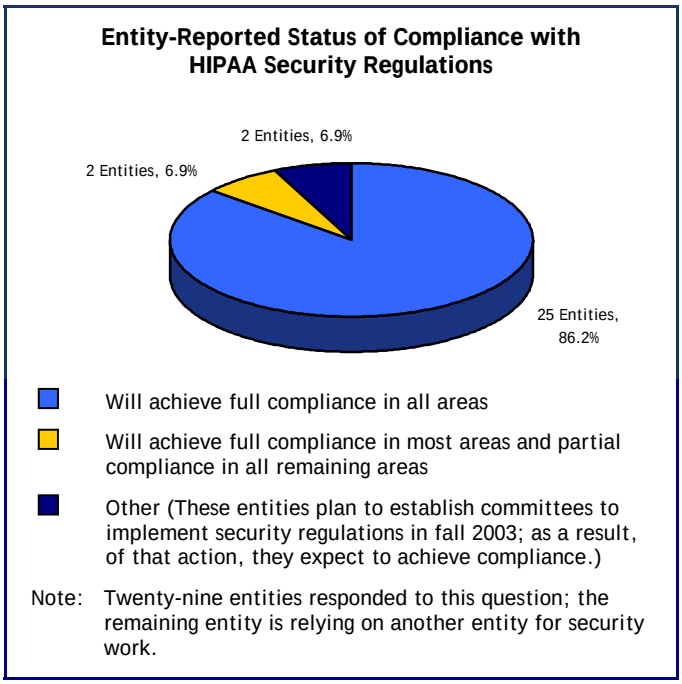
(The remaining entity is relying on another entity for transactions and code sets work; however, we noted that this entity has no formal agreement with the other entity regarding this work.)

It is important to note that 26 entities (89.7 percent) reported that they do not have a well-developed contingency plan in case they do not achieve compliance by the deadline. Several of them indicated that they would switch to using hard copy files; however, this would require entities to adjust their operations and allow more time for functions such as claim processing. Some entities reported that they would begin developing contingency plans closer to the deadline; others are considering using clearinghouses to create transactions that comply with HIPAA. This option, however, still requires planning and research to ensure that the selected clearinghouse complies with HIPAA regulations and has the capacity to handle the entities' transactions.

The Deadline for Complying with Security Regulations Is April 21, 2005, Yet Many Entities Have Not Started Addressing Major Components of the Security Regulations

The security regulations deadline was less than two years away when entities responded to our survey. As Figure 3 shows, 25 entities (86.2 percent) reported that they anticipated achieving full compliance with security regulations by the April 21, 2005, deadline. Two entities (6.9 percent) reported that they anticipated achieving full compliance in most areas of security regulations, with partial compliance in the remaining areas. Two (6.9 percent) entities reported that they are establishing committees or project teams to implement security regulations. (The remaining entity is relying on another entity for security work; however, we noted that this entity has no formal agreement with the other entity regarding this work.)

Figure 3



While the majority of entities reported that they anticipate achieving compliance with security regulations, the supporting documentation they submitted indicated that many of them have not started addressing major components of the security regulations such as administrative, technical, and physical specifications. In addition, most entities reported that they had not established an overall plan to comply by the deadline. Promptly initiating efforts to address security regulations is critical in achieving compliance with security regulations by the deadline.

It is also important to note that the consolidation of health and human services agencies in Texas could have an impact on these agencies' ability to comply with security regulations by the deadline. This consolidation introduces additional risks because the consolidation transition period overlaps with the deadline for compliance with security regulations. In addition, the associated transfer of functions and staff among those agencies could further complicate efforts to achieve compliance.

Many entities reported they had invested a significant amount of time and effort to conduct activities required to achieve compliance with privacy regulations by the April 14, 2003, deadline. However, there was a noticeable degree of variation among entities, and not all entities have completed all required activities. In addition, while 86.7 percent of entities reported that they have implemented policies and procedures to comply with privacy regulations, the achievement of full compliance with HIPAA privacy regulations depends on whether entities actually follow their policies and procedures. Although we reviewed supporting documentation related to entities' policies and procedures, we did not confirm whether entities actually are following their policies and procedures. 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.

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. Most entities reported that they do not have well-established contingency plans in case they do not achieve compliance by the deadline.

Although the majority of entities anticipate achieving full compliance with security regulations by the April 21, 2005, deadline, most reported that they had not established an overall plan to comply by that deadline. 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 specifications.

Chapter 2-A
Activities to Achieve Compliance with Privacy Regulations

Many entities reported they had invested a significant amount of time and effort to conduct activities required to achieve compliance with privacy regulations. However, there was a noticeable degree of variation among entities, and not all entities have completed all required activities. For example, as discussed in more detail below, some entities have not established all required policies and procedures, while others have not provided required employee training.

In addition, 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. Our review of the supporting documentation entities provided also indicated that the depth of issues covered in entities' policies and procedure varied. Furthermore, some entities that reported achieving only partial compliance with privacy regulations had more comprehensive policies and procedures than entities that reported achieving full compliance.

Twenty-nine entities (96.7 percent) reported that they had established an overall plan for meeting the HIPAA privacy regulations deadline of April 14, 2003. However, as Chapter 1 discusses, only 43.3 percent reported they were in full compliance by that deadline.

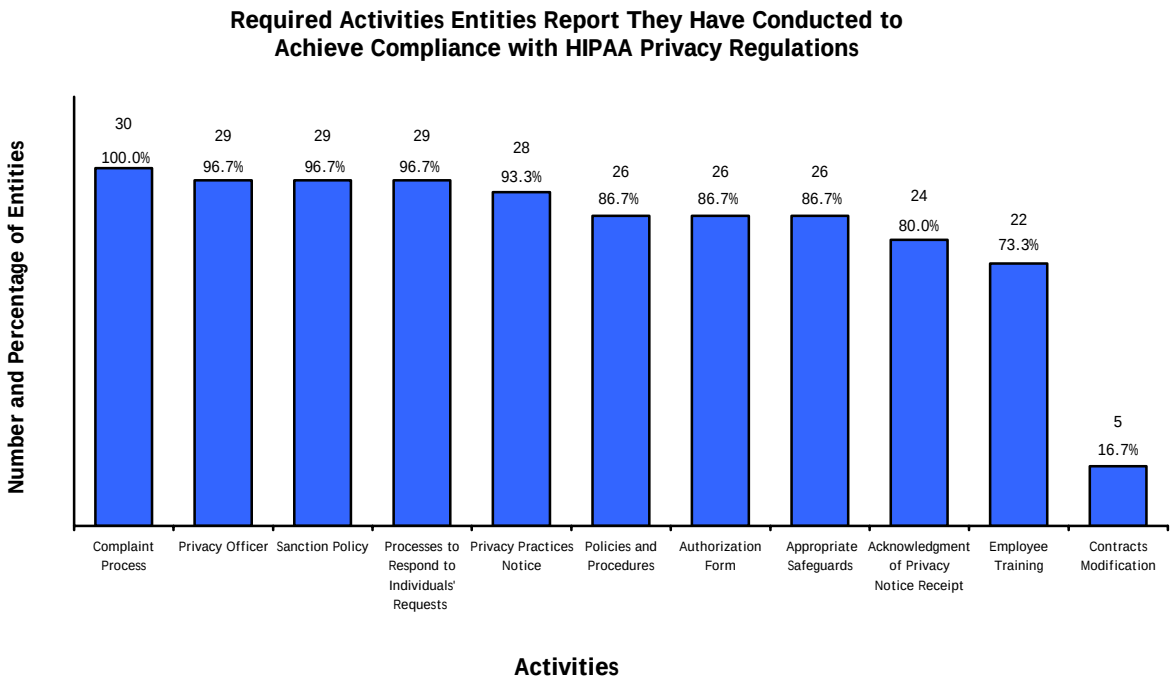
Entities Have Not Conducted All Required Activities to Achieve Compliance with Privacy Regulations

Table 1 summarizes the activities entities are required to conduct to comply with privacy regulations, but Figure 4 shows that not all entities have conducted these activities.

Table 1

Activities Required to Achieve Compliance with Privacy Regulations	
Activity	**Description**
Establishment of a complaint process	This process must set forth how complaints concerning privacy are reported, addressed, and documented.
Appointment of a privacy officer	A privacy officer is responsible for developing and implementing policies and procedures.
Establishment of a sanction process	Sanctions must be established and imposed on employees who fail to comply with privacy policies and procedures.
Establishment of processes to respond to requests regarding protected health information	These processes include processes to respond to an individual's request to restrict, inspect, copy, amend, and receive an accounting of disclosures of protected health information.
Development and use of notice of privacy practices	These notices explain individuals' rights and the entity's legal duties with respect to protected health information.
Establishment of privacy policies and procedures	These policies and procedures must consider the size and types of activities that relate to an entity's protected health information.
Establishment of an authorization form for use or disclosure of protected health information	In certain cases, entities must use this form in order to use or disclose protected health information.
Establishment of appropriate safeguards	Entities must establish appropriate administrative, technical, and physical safeguards to protect the privacy of health information.
Acknowledgement of notice of privacy practice	Entities must (1) make an effort to obtain written acknowledgement that individuals received this notice or (2) document why they did not obtain this acknowledgement.
Employee training	Employees must receive training on policies and procedures regarding protected health information no later than April 14, 2003, or the date the entity becomes a covered entity.
Modification of contracts with the business associates	Entities must have satisfactory assurance that business associates that perform work on their behalf will appropriately safeguard protected health information.

Figure 4



Areas in Which Entities May Need to Intensify Their Efforts

While entities reported having conducted a variety of activities to comply with privacy regulations, they may need to intensify their efforts in the following areas:

- Privacy policies and procedures. Although most entities reported they have implemented privacy policies and procedures, only 13 of them reported that they have established policies for all 11 required standards regarding issues such as what information should be disclosed, to whom it should be disclosed, and what minimum information to disclose. If entities do not establish policies and procedures relevant for their operations, this increases the risk that they may violate privacy regulations. Nine entities (30.0 percent) reported that they have already received notice of an average of approximately seven suspected violations of privacy, with an average of two confirmed violations per entity.

  Our review of the supporting documentation entities provided also indicated that the depth of issues covered in entities' policies and procedures varied. In addition, some entities that reported achieving only partial compliance with privacy regulations had more comprehensive policies and procedures than entities that reported achieving full compliance.

- Notice of privacy practices. Although most entities reported that they have developed notices that address all requirements, at least four of these entities' notices did not cover all requirements. Another entity reported that it believed the client is only required to sign the acknowledgement of receipt of the notice (but not understand the notice). This, however, may contradict HIPAA's intent.

- Authorization form for use and disclosure of the health information. While most entities reported that they established authorization forms that are consistent with the regulations, one entity's form did not contain all required elements. Three entities reported they were in full compliance with privacy regulations, but they did not provide their authorization forms.

- Response to requests regarding protected health information. While all covered entities reported that they have established required processes to respond to individuals' requests, two entities stated that their policy is not to grant any restrictions on the uses and disclosures of protected health information. It is also important to note that tracking such disclosures can represent a significant administrative task. Most entities reported using hard copy files, while only some reported that they track disclosures using either a database or tracking software.

- Employee training. Some entities are behind schedule in providing required employee training on privacy. Eight entities reported they are still in the process of providing this training to their employees. Entities that reported that they had provided training stated that this training ranged in length from 1 to 12 hours per employee.

- Appropriate safeguards. HIPAA regulations do not identify the specific safeguards entities should have, yet the descriptions of the safeguards that entities provided did not always indicate that their safeguards were adequate. For example, one entity reported it had established these safeguards, but it had not yet established associated policies and procedures.

- Modification of contracts with the business associates. While 27 entities (90 percent) reported that they had business associates, only about half of them had identified all business associates that are affected by HIPAA regulations. The number of business associates entities reported having ranged from 1 to 185.

  The majority of entities reported that they will update their contracts with business associates to ensure compliance with HIPAA privacy regulations when these contracts are renewed, a practice that HIPAA regulations permit.

  Government entities that exchange information are required to sign memoranda of understanding. Twelve entities (40.0 percent) reported that they have executed these memoranda.

Entities Have Voluntarily Conducted Other Activities to Comply with Privacy Regulations

Nearly all entities reported that they are assigning additional staff to implement privacy regulations. The number of full-time equivalent (FTE) employees entities reported assigning varied from one to eight FTEs.

HIPAA regulations do not specifically require entities to monitor business associates to ensure that they safeguard protected health information. However, nine entities

(30.0 percent) reported that they monitor business associates' compliance with contract terms regarding the safeguarding of protected health information.

In addition, ten entities (33.3 percent) reported they had established separate budgets for the implementation of privacy regulations. Table 2 summarizes the budgets they reported. Entities that did not establish a separate budget reported that their departments absorbed the cost of implementing privacy regulations in their individual budgets.

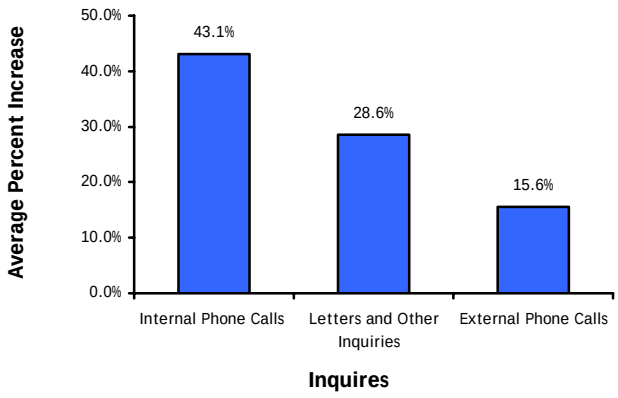
Table 2

Entity-Reported Budgets for Implementation of Privacy Regulations					
Entity	Budget Amount	Estimated Percent of Budget Spent	Estimated Percent of Implementation Plan Achieved	Number of Employees Affected by HIPAA	Percent of Total Employees Affected by HIPAA
Entity 1	$ 12,000	100%	100%	400	34%
Entity 2	$ 50,000	100%	100%	276	90%
Entity 3	$ 110,000	90%	100%	4,000	85%
Entity 4	$ 124,057	85%	95%	5,002	100%
Entity 5	$ 395,000	90%	95%	1,300	100%
Entity 6	$ 690,000	65%	85%	1,979	100%
Entity 7	$ 750,000	80%	95%	4,218	66%
Entity 8	$ 896,000	80%	90%	13,000	100%
Entity 9	$ 1,722,987	50%	90%	13,050	100%
Entity 10	$ 2,419,000	75%	90%	14,000	100%

Privacy Regulations Have Already Had an Impact on Entities

Nineteen entities (63.3 percent) reported that they have already experienced an increase in inquiries as a result of HIPAA privacy regulations (see Figure 5). In addition to receiving more inquiries, eight entities (26.7 percent) reported an increase in the number of requests individuals made to inspect and copy their protected health information. Those entities reported an average increase of 362 such requests. As

Figure 5



Note: These averages were calculated from the 19 entities that reported increases in inquiries.

specified above, some entities also reported that they have already received notice of suspected and confirmed violations of privacy.

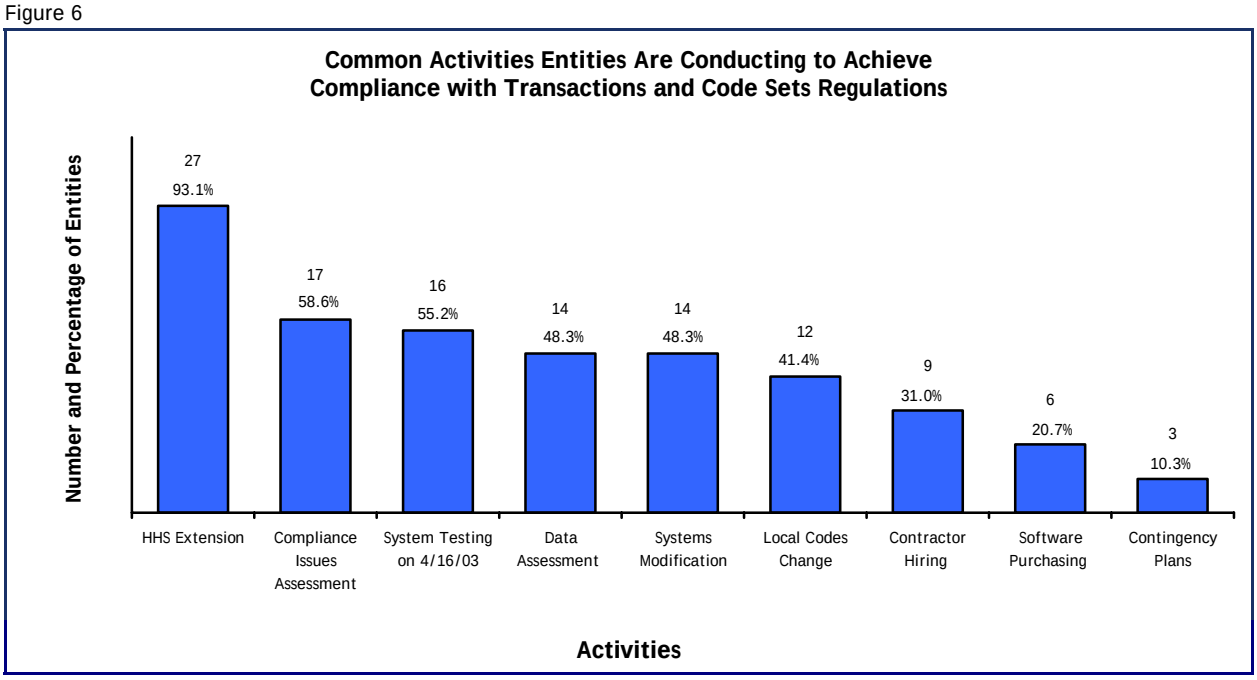
Chapter 2-B

Activities to Achieve 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, as discussed in more detail below, 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. Most entities reported that they do not have well-established contingency plans in case they do not achieve compliance by the deadline.

The activities that entities reported conducting to comply with transactions and code sets regulations varied depending on the nature of each entity's work. Figure 6 summarizes the most common activities entities are conducting.[4]

Figure 6



The original deadline for compliance with the transactions and code sets regulations was October 2002. However, most entities filed requests with the U.S. Department of Health and Human Services to extend the deadline to October 16, 2003. In those

[4] Percentages in Chapter 2-B were calculated based on responses from 29 entities because one entity reported that it is relying on another entity for compliance with transactions and code sets regulations.

requests, entities were required to specify their overall plans for meeting the new deadline. One entity reported that it did not file an extension because it was already in compliance with regulations.

Areas in Which Entities May Need to Intensify Their Efforts

Some entities have not assessed their systems that process electronic transactions to identify potential compliance issues. Depending on the volume of their transactions, it is possible that these entities will have more difficulty meeting the deadline.

The Purpose of Transactions and Code Sets Regulations

Transactions and code sets regulations require entities to adopt standards for electronic transactions and code sets to be used when transmitting transactions via electronic data interchange (EDI). The use of standard transactions simplifies administration and enables the efficient electronic transmission of certain health information. Transactions and code sets regulations apply only to electronic transactions.

The U.S. Centers for Medicare and Medicaid Services (CMS) estimates that administrative costs represent more than 15 percent of the more than $1.3 trillion in annual health care expenditures. High administrative costs are caused both by paperwork and the existence of more than 400 different data transmission formats. CMS asserts that transactions and code sets regulations related to EDI can increase efficiency in transaction processing, lead to fewer errors, reduce postage and other paper-related expenses, and accelerate reimbursements.

The cost of complying with transactions and code sets regulations varies from entity to entity, depending on the nature and volume of transactions. Most of the associated costs are considered one-time expenses.

In addition, some 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. Such testing is critical because it can identify areas that do not meet all regulations or are not functioning properly.

Some entities also are relying heavily on vendors to conduct key activities such as assessment, testing, and creation of contingency plans. In several cases, however, entities could not provide us with assurance that their vendors were actually performing these activities.

Most entities reported that they do not have well-established contingency plans in case they do not achieve compliance by the deadline. Many entities stated that they would work on those plans closer to the deadline; several stated they would switch to using hard copy transactions. Not having these plans may lead to the disruption of payments to providers and overall business operations.

In general, entities whose primary function is related to health care submitted adequate supporting documentation to substantiate their activities to achieve compliance with transactions and code sets regulations. On the other hand, hybrid entities, only a portion of whose operations is related to health care, submitted less substantial supporting documentation. Hybrid entities were more likely to report that they were relying on software vendors or contractors to achieve compliance with transactions and code sets regulations. The vendors they reported relying on generally appeared well established and capable of achieving compliance.

The majority of entities reported that they are not planning to obtain certification that their systems comply with transactions and code sets regulations. The U.S. Centers for Medicare and Medicaid Services (CMS) will certify an entity's systems if the entity has received federal funding to change its Medicaid management information systems. In addition, CMS asserts that certification would increase any entity's chances of successfully transmitting transactions through electronic data interchange.

Complying with Transactions and Code Sets Regulations Can Involve Significant Analysis, System Changes, and Expense

The goal of transactions and code sets regulations is to standardize transactions and code sets; therefore, entities have to review the format of their transactions and the codes they use in these transactions. Industry experts state that some organizations, mostly health care providers, will have to (1) adjust or add different data elements to their transactions and (2) delete some local codes they use in their transactions.

Approximately half of the entities reported that they had assessed the data they collect for their transactions to ensure that they collect appropriate information and use it appropriately in their transactions. Some entities reported that they are relying on vendors to do this assessment. However, industry experts have noted that entities that are relying on vendors still must conduct a significant amount of work to ensure that they are collecting all the information HIPAA requires and that their staff are properly educated about that information. Even errors on a small part of a transaction can make the transaction invalid.

On average, entities that have assessed their systems to identify potential compliance issues reported that they will need to modify from one to six systems. Twelve entities (41.4 percent) reported that they would have to delete or adjust local codes that they assign to items such as specific providers, clients, and diseases. On average, they reported that they would have to delete 351 codes and adjust 77 codes. Entities reported that their business associates have to delete an average of 79 codes and adjust an average of 33 codes. Nine entities (31.0 percent) reported that the deletion or adjustment of codes had an effect on their operations. For example, some entities reported that they had to adjust their policies and rate methodologies and provide employees with additional training.

Five entities (17.2 percent) reported that they had established a separate budget for implementation of transactions and code sets regulations. Table 3 summarizes the budgets they reported. The federal government is paying up to 90 percent of the costs associated with the changes that entities have to make to Medicaid management information systems.

Table 3

Entity-Reported Budgets for Implementation of Transactions and Code Set Regulations

Entity	Budget Amount	Estimated Percent of Budget Spent	Estimated Percent of Implementation Plan Achieved	Number of Systems Affected by Transactions and Code Sets Regulations
Entity 1	$ 114,000	0%	0%	0
Entity 2	$ 401,732	72%	65%	3
Entity 3	$ 1,100,000	60%	55%	3
Entity 4	$ 7,832,751	10%	50%	6
Entity 5	$ 30,212,768	35%	60%	4

Chapter 2-C

Activities to Achieve Compliance with Security Regulations

Although the majority of entities anticipate achieving full compliance with security regulations by the April 21, 2005, deadline, only six entities (20 percent) reported they had established an overall plan to comply by that deadline. 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 specifications. While entities reported that they had started to implement many of these specifications, they frequently did not provide supporting documentation for that assertion.

Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202 (effective June 17, 2002), 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.

HIPAA Security Regulations Include Required and Addressable Specifications

HIPAA security regulations include two categories of specifications:

- Required specifications that entities must implement.
- Addressable specifications that entities must implement if they are applicable to their operations. Entities can substitute alternative measures for addressable specifications; if they determine that certain addressable specifications do not apply to them, they must document this determination.

Appendix 2 contains detailed information on entities' reported status in implementing required and addressable specifications. A summary of that status is as follows:

- Sixteen entities (55 percent), primarily universities and medical institutions, reported that they have either addressed or are addressing more than 50 percent of the required specifications. (Universities are generally hybrid entities, which means that only a portion of their operations are subject to HIPAA. Therefore, it is possible that it is relatively less difficult for universities to achieve compliance with these

HIPAA Security Regulations

HIPAA security regulations define processing and technology standards for electronic protected health information. The regulations' purpose is to ensure the integrity, confidentiality, and availability of electronic protected health information, as well as to protect this information against reasonably anticipated threats and improper use or disclosure.

The U.S. Centers for Medicare and Medicaid Services (CMS) is responsible for overseeing compliance with security regulations. CMS has described the security regulations as follows:

- Flexible and scalable. CMS has pointed out that covered entities should take into account their size, complexity, capabilities, costs, and the potential risks to their electronic protected health information.
- Technology neutral. Security regulations do not require the use of any particular technology.
- Comprehensive. Security regulations are designed to protect electronic data through administrative, physical, and technical safeguards.

specifications.) However, entities that reported they are in the process of addressing required specifications generally did not submit adequate supporting documentation for their assertions.

- Eighteen entities (62 percent), primarily universities and medical institutions, reported that they have addressed or are addressing more than 50 percent of the addressable specifications. As with required specifications, however, entities that reported they are in the process of implementing addressable specifications generally did not submit adequate supporting documentation for their assertions.

- One entity reported that it would not implement security specifications because it relies on a contractor for security.

Entities Have Conducted Other Activities to Comply with Security Regulations

With regard to other activities to achieve compliance with security regulations, entities reported the following:

- Twenty-four entities (82.8 percent) have designated an official who is responsible for HIPAA security standards implementation. Other entities will make this designation in the future.

- In addition to appointing a security officer, the majority of entities have started assigning personnel to work on security requirements.

- Eleven entities (38 percent) reported that they have not begun developing written polices and procedures for security, and 17 (58 percent) are developing or have developed these polices and procedures. One entity is relying on a contractor to comply with security regulations.

- Entities are required to implement a security awareness and training program for all employees (including management). Five entities (17 percent) reported that they have provided this training. Most of these entities provided 1 to 2 hours of training to each employee.

- Security regulations require entities to require their business associates to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the electronic protected health information. Twenty-five entities (86 percent) have contracts with business associates. Approximately half of those entities reported that they have established security requirements in their contracts with business associates. While some entities reported that they have addressed security regulations through contract provisions regarding privacy, it is important to note that privacy and security regulations are quite different. Entities should not assume that addressing privacy regulations ensures compliance with security regulations.

- Five entities (17.2 percent) reported that they have established a separate budget for the implementation of security regulations. Table 4 summarizes the budgets they reported. Other entities reported that they are developing these budgets or stated that they would absorb the cost of implementing security regulations. One entity reported that no funding was available to establish a separate budget.

Table 4

Entity-Reported Budgets for Implementation of Security Regulations				
Entity	Budget Amount		Estimated Percent of Budget Spent	Estimated Percent of Implementation Plan Achieved
Entity 1	$	210,000	60%	100%
Entity 2	$	300,500	79%	75%
Entity 3	$	324,800	0%	0%
Entity 4	$	3,577,804	40%	60%
Entity 5	$	4,463,000	0%	0%

Challenges in Determining Whether Entities Must Comply with HIPAA

Entities reported that they encountered difficulty in determining whether they are required to comply with HIPAA regulations. Seventeen entities (56.7 percent) that are subject to HIPAA regulations needed assistance in making this determination.

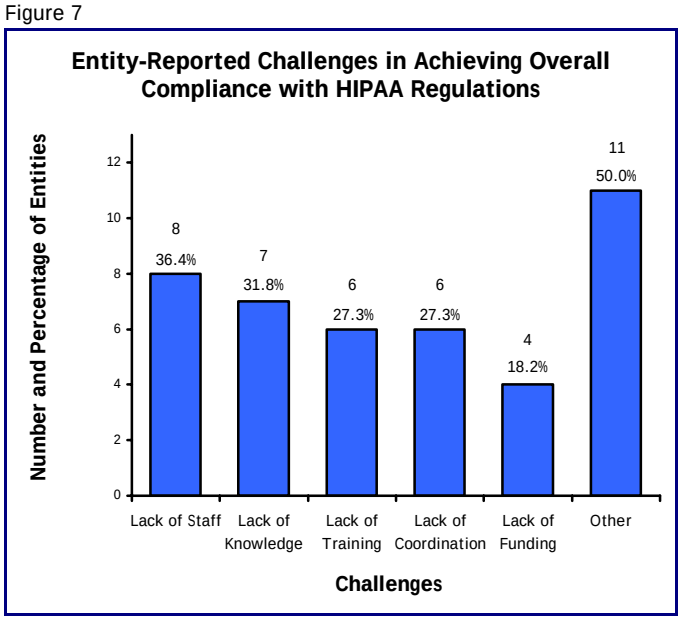
Entities that were exempt from HIPAA regulations also reported that they had to go through extensive analysis and legal research to make this determination. State schools and higher education institutions also reported that confusion involving two overlapping federal laws—the Federal Education Records Privacy Act (FERPA) and HIPAA—makes it difficult for them to determine whether they are covered entities.

The supporting documentation two entities submitted did not adequately support their assertions about whether they were or were not covered entities. For example, one of the entities reported that it was a hybrid entity and, because of that, did not consider itself to be a covered entity. However, HIPAA regulations specify that a hybrid entity is a form of covered entity.

Overall Challenges to HIPAA Implementation

Overall, 20 entities (66.7 percent) stated that they received some form of assistance from other state entities and federal agencies, while 22 (73.3 percent) reported that they attended workgroups for specific HIPAA issue areas. However, six entities stated that they were not aware of the workgroups.

Figure 7



Twenty-two entities that are subject to HIPAA (73.3 percent) reported that they experienced challenges to overall HIPAA implementation (see Figure 7). Eight of them cited lack of staff as an overall challenge. As one entity noted, a great deal of time and effort is required to learn HIPAA regulations, develop required policies and procedures, and train staff.

Individually, entities reported a variety of other specific challenges to overall HIPAA implementation, including:

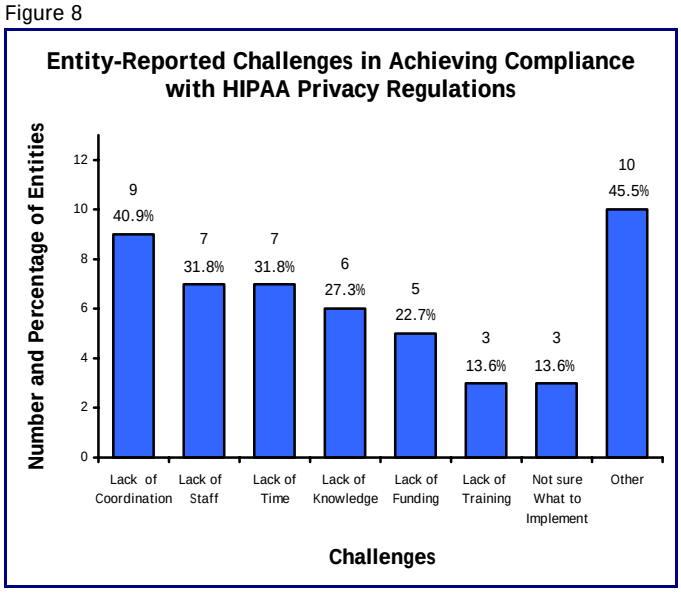
- Insufficient guidance from the U.S. Office of Civil Rights, which oversees and enforces HIPAA privacy regulations.
- Conflicting priorities, time and budget constraints, and the complexity of required remediation.

- Difficulties in adjusting HIPAA regulations to an academic institution.
- Lack of support from a software vendor.

Challenges to Implementing Privacy Regulations

Twenty-two entities (73.3 percent) reported that they experienced challenges in implementing privacy regulations (see Figure 8). The reported challenges varied from entity to entity, depending on an entity's size and its involvement in providing direct health care. However, the challenge entities cited most frequently was lack of coordination.

Figure 8



It is important to note that the 77th Legislature required the Health and Human Services Commission's (Commission) National Data Interchange Standards (NDIS) Task Force to work with several other state entities to develop a plan for selected state entities' integration of HIPAA provisions. This task force recommended that agencies pursue their own implementation of HIPAA, with coordination and integration activities to be provided by the Commission's Program Management Office in conjunction with the task force. (The NDIS Task Force focuses only on electronic data interchange related to transactions and code sets regulations and does not coordinate the implementation of privacy and security regulations.) Other states have taken a variety of approaches to enhancing coordination. For example:

- The State of California established an Office of HIPAA Implementation within its Health and Human Services Agency. That office provides leadership and oversight for HIPAA implementation across state government, develops policies and procedures, provides information and technical advice, and offers HIPAA education and training.
- The New York State Office for Technology established a Central HIPAA Coordination Project, which offers information on HIPAA regulations and a variety of tools and reference guides to assist state agencies in complying with HIPAA.
- The State of Ohio established a HIPAA Statewide Project to help coordinate state agencies' implementation of HIPAA.

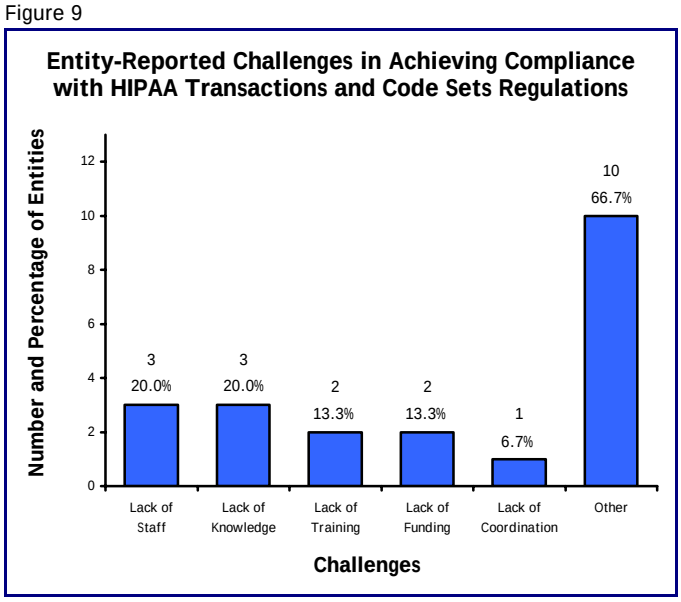
Individually, entities reported a variety of other specific challenges to implementation of HIPAA privacy regulations, such as:

- Lack of authoritative interpretive guidelines.
- Conflicting priorities.
- The fact that the privacy regulations kept changing.

Challenges to Implementing Transactions and Code Sets Regulations

Fifteen entities (51.7 percent) reported that they experienced challenges in implementing transactions and code sets regulations; however, none of the challenges cited was predominate (see Figure 9). Three entities reported that lack of staff was a challenge to implementing transactions and code sets regulations. Those entities estimated that they needed to devote 1 to 2 employees to work on issues related to this implementation.

Figure 9

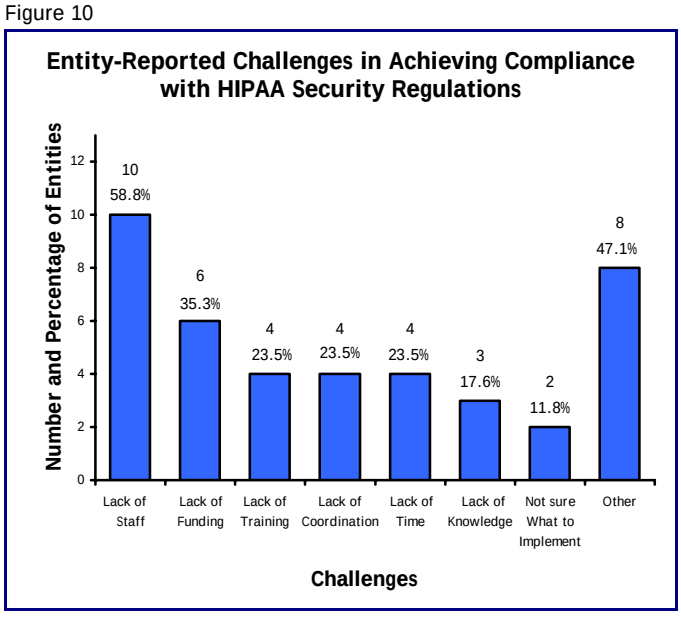


Individually, entities reported a variety of specific challenges to the implementation of HIPAA transactions and code sets regulations, such as:

- Determining the overall impact on the entity's operations.
- Third-party processors not being prepared to accept the new transactions and code sets.
- Difficulty working with payers.
- Lack of published, consistent standards for all trading partners.
- Conflicting priorities.

Challenges to Implementing Security Regulations

Figure 10



Seventeen entities (58.6 percent) reported that they experienced challenges in implementing security regulations, with 10 noting that lack of staff presented a challenge (see Figure 10). Overall, entities estimated that they needed 1 to 5 additional employees to comply with security regulations. Entities that reported lack of funding as a challenge reported that they required anywhere from $100,500 to $1,000,000 in additional funding.

The entities also stated that security regulations are complex, and analysis and evaluation of the corresponding regulations are time-consuming. Many entities reported that they have not experienced challenges in implementing HIPAA security regulations, primarily because they have not progressed far enough in addressing those regulations.

Appendices

Appendix 1

Objectives, Scope, and Methodology

Objectives

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.

Scope

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.

Methodology

We developed our survey based on an analysis of HIPAA administrative simplification regulations for privacy, transactions and code sets, and security. We judgmentally selected entities to participate in our survey if at least a portion of their operations might involve health information in some form. Those entities generally included health and human services agencies, medical institutions, and universities.

Entities provided answers to the survey via the Internet. Their answers were submitted directly into a database that we then used to perform detailed analysis. 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.

Other Information

The information in this report has not been subjected to the tests and confirmations that would be performed in an audit. The following members of the State Auditor's staff conducted this review:

- Natalia Boston, MPAff, Project Manager
- Rodney Almaraz, CPA, MBA
- Margaret Nicklas, MPAff
- Jaime Contreras, CISA, MBA
- Juan Sanchez, MPA
- Leslie Ashton, CPA, Quality Control Reviewer
- Joanna B. Peavy, CPA, Audit Manager
- Frank Vito, CPA, Audit Director

Appendix 2

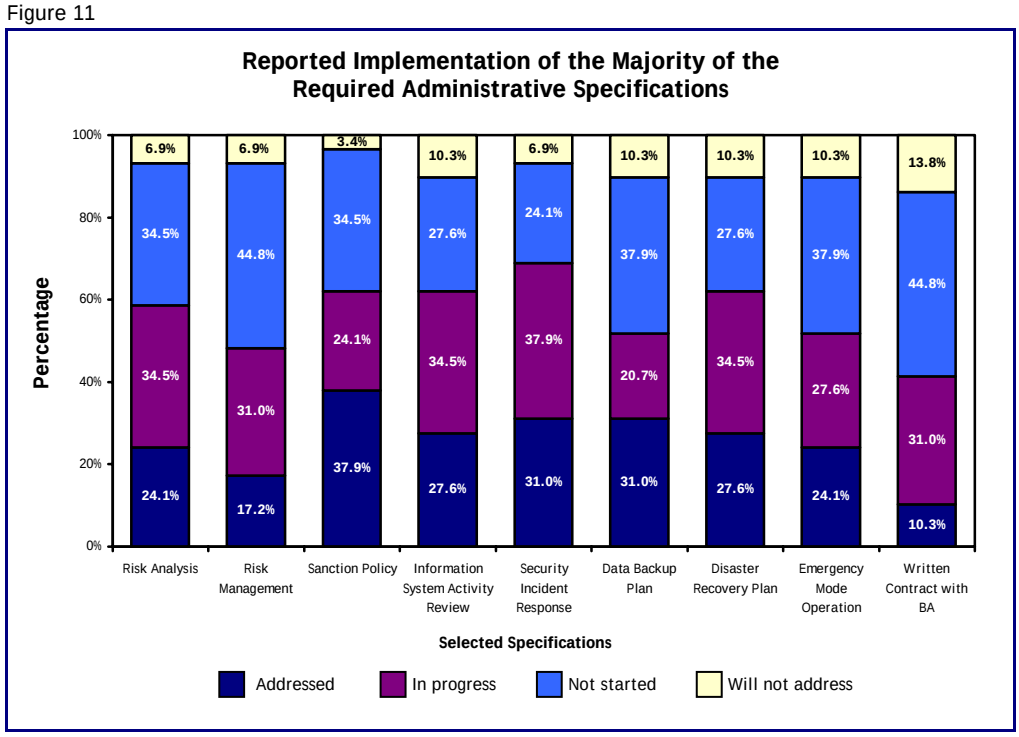
Activities Entities Are Conducting to Achieve Compliance with HIPAA Security Regulations

The following information is regarding entities' reported status in complying with required and addressable HIPAA security specifications. The information summarizes what entities reported. However, our limited review of the supporting documentation entities submitted found that (1) in many cases, entities did not submit supporting documentation to support their assertions or (2) the documentation they did submit did not adequately support their assertions.

Activities to Implement Required Administrative Specifications

The purposes of required administrative specifications are to (1) establish procedures for selection, development, and use of the security controls; (2) determine how employees must handle protected health information; and (3) establish proper data back up and data recovery plans. Figure 11 summarizes entities' reported status in implementing selected required administrative specifications.

Figure 11



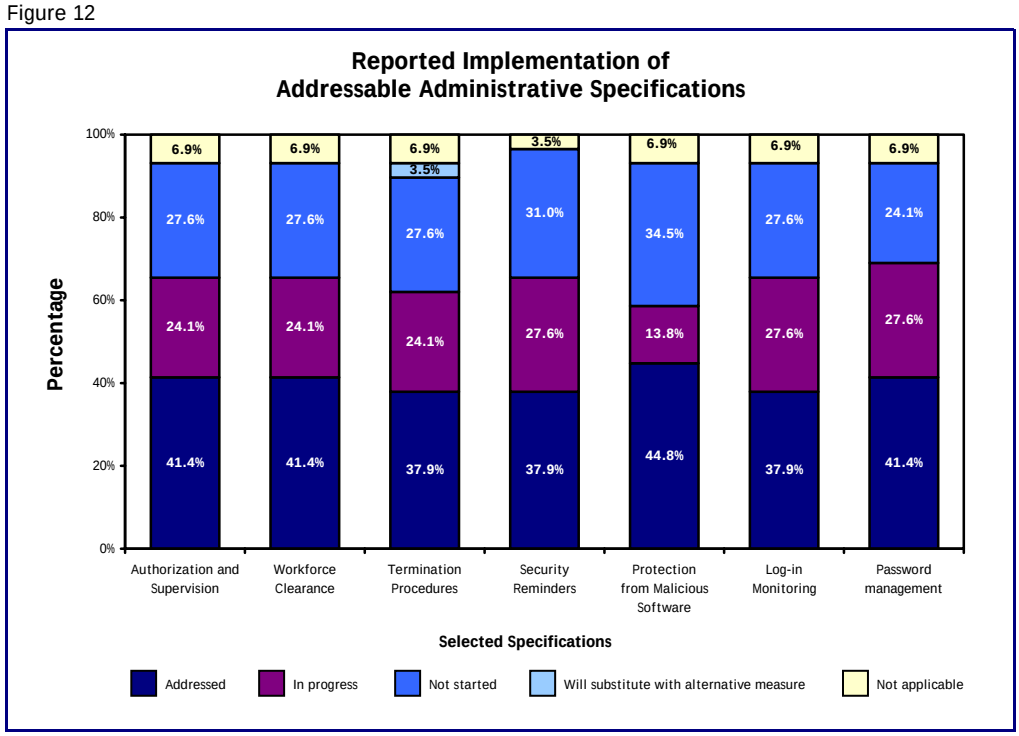
Overall, entities have not made significant progress in implementing required administrative simplifications. Few entities reported they had completed the required risk analysis to assess potential risks to the confidentiality, integrity, and availability of electronic protected health information. This analysis is essential for identifying threats to information security, assigning associated dollar values, and determining how to proceed. Even fewer entities have taken the next step to manage the risks identified in the risk analysis.

Many entities reported they intended to start working on implementing security regulations after they implement transactions and code sets regulations. These entities reported that they plan to establish security committees in November 2003 or begin implementing security regulations after completing the required risk analysis.

Activities to Implement Addressable Administrative Specifications

In general, the purposes of addressable administrative specifications are to oversee employees' access to and use of protected health information and to establish certain policies that protect health information from unauthorized access. Figure 12 summarizes entities' reported status in implementing selected addressable administrative specifications.

Figure 12

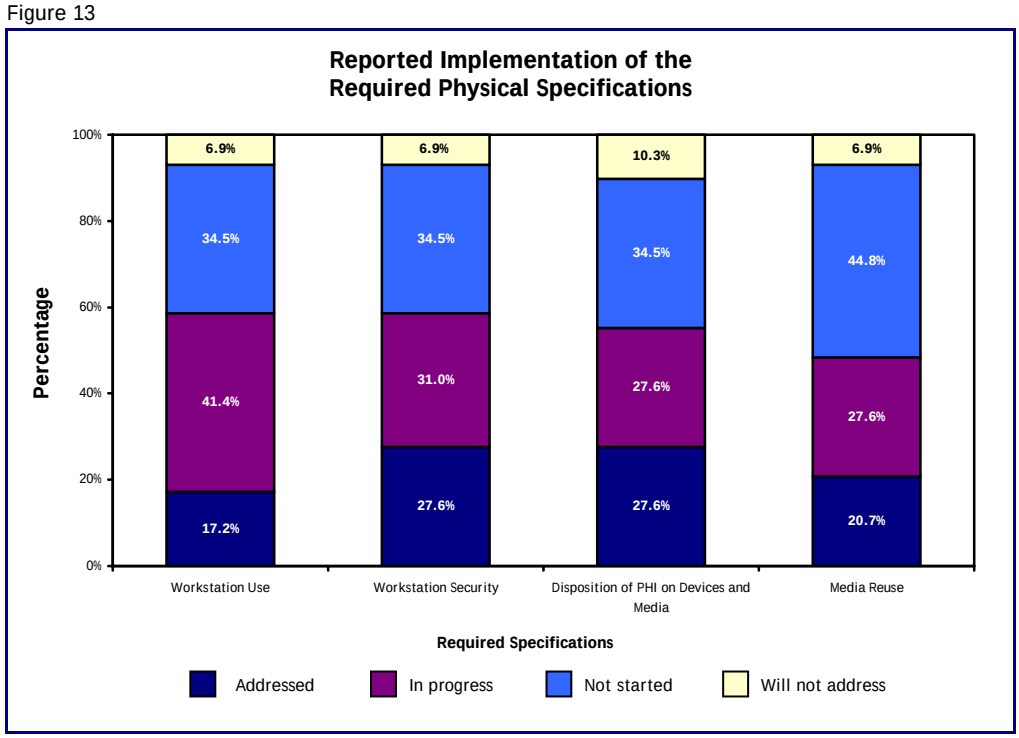


Although almost one-third of the entities have not started implementing addressable administrative specifications, entities appear to making the most progress in this area when compared with other specifications. Addressable administrative specifications are generally specifications that entities implement without regard to the type of information involved and as part of their normal business operations.

Activities to Implement Required Physical Specifications

The purpose of required physical specifications is to ensure that (1) entities have policies and procedures specifying proper functions to be performed on workstations that have access to the protected health information and (2) only authorized users can access protected health information. Physical specifications also require entities to have processes to address disposition and removal of protected health information from hardware and media devices. Figure 13 summarizes entities' reported status in implementing required physical specifications.

Figure 13



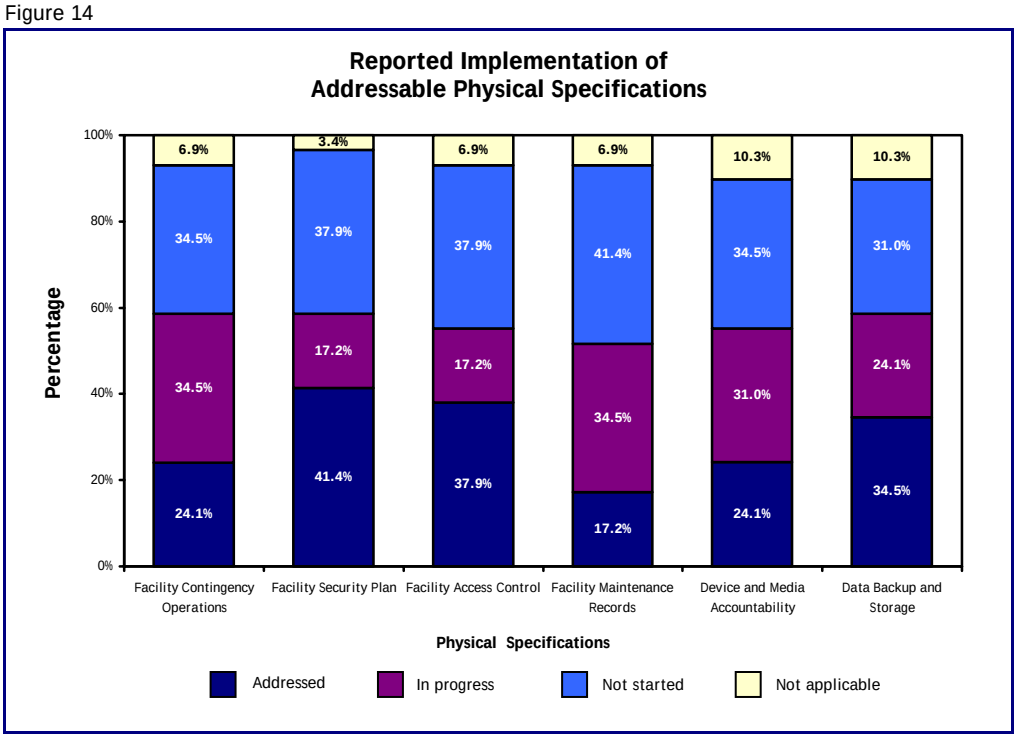
Although entities reported making some progress in implementing required physical specifications, one-third of them have not started implementing physical safeguards for the workstations that access protected health information. One-third also have not implemented policies and procedures for the proper use of these workstations. In addition, almost half have not started working on procedures to remove protected health information from hardware and media devices such as disks and diskettes before making those devices available for reuse.

Activities to Implement Addressable Physical Specifications

The purpose of addressable physical specifications is to ensure that entities establish (1) measures to safeguard facilities and equipment and (2) procedures for accessing facilities. Entities also must track the movement of hardware and electronic media through proper maintenance of records and establish procedures for creating copies of protected health information.

Figure 14 summarizes entities' reported status in implementing addressable physical specifications.

Figure 14

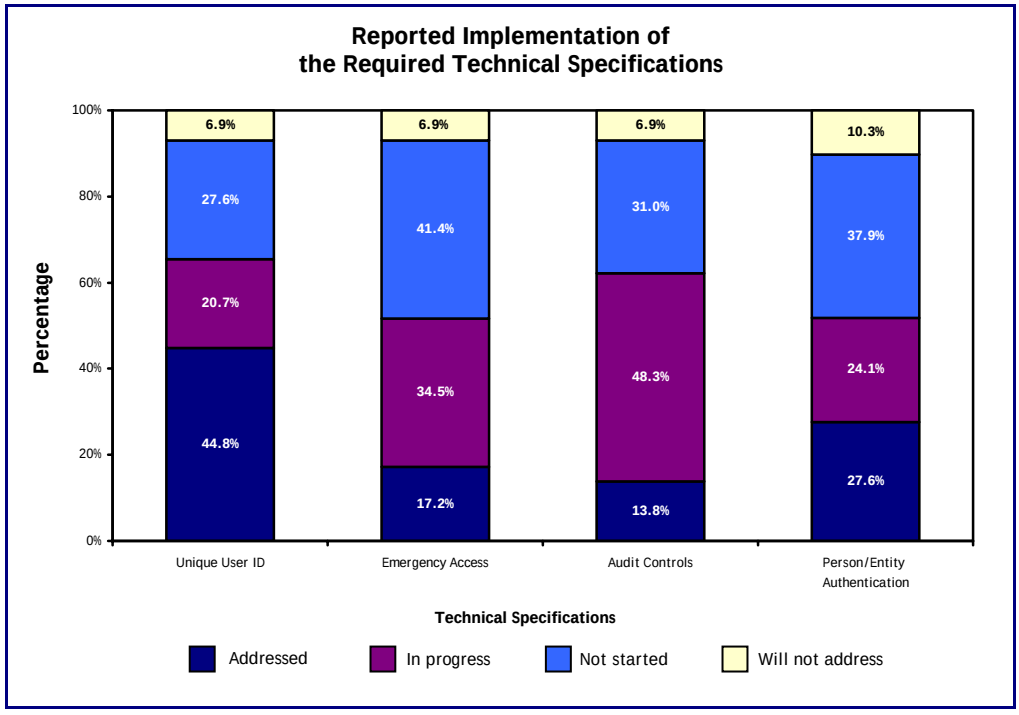


Facility security and access control are the most commonly implemented specifications. Several entities provided internal audit reports or assessments showing that they recognize the seriousness of physical security. However, specifications regarding facility maintenance records are the category of specifications that have been addressed the least. Many entities also have not started addressing data back up and storage, which are crucial to any organization.

Activities to Implement Required Technical Specifications

The purpose of required technical specifications is to require entities to establish procedures for identifying and tracking user identity, verifying users' identities, obtaining protected health information during emergencies, and examining information system activities. Figure 15 summarizes entities' reported status in implementing required technical specifications.

Figure 15



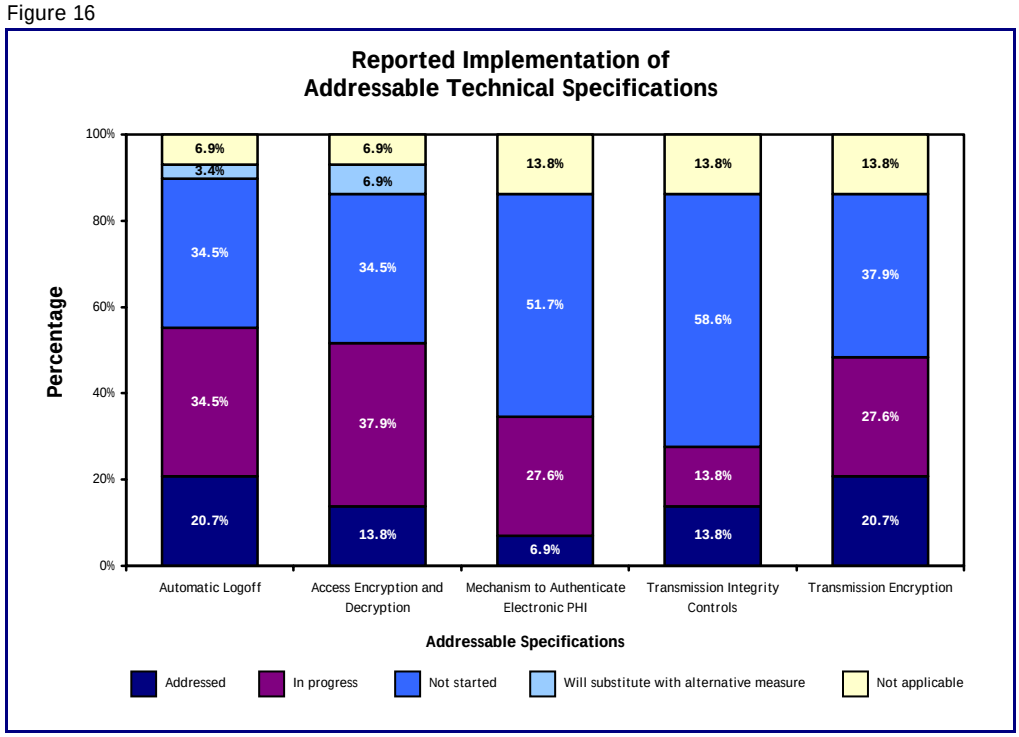
The majority of entities have not established mechanisms to record and examine information system activity and have not established procedures for obtaining electronic heath information during an emergency. However, many reported that they have already established a process to identify and track user identity.

Activities to Implement Addressable Technical Specifications

The purpose of addressable technical specifications is to ensure that entities (1) establish procedures for automatic system logoff and (2) implement mechanisms to protect electronic health information during transmission.

Figure 16 summarizes entities' reported status in implementing addressable technical specifications.

Figure 16



It appears that entities have not worked on implementing addressable technical specifications to the same extent that they have addressed other security regulations. Many entities reported that they have not started establishing transmission integrity controls, encryption processes, or procedures to authenticate electronic health information.

This page intentionally left blank.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Tom Craddick, Speaker of the House, Chair
The Honorable David Dewhurst, Lieutenant Governor, Vice Chair
The Honorable Teel Bivins, Senate Finance Committee
The Honorable Bill Ratliff, Senate State Affairs Committee
The Honorable Talmadge Heflin, House Appropriations Committee
The Honorable Ron Wilson, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Entities Covered by this Review