AICPA CITP Credential Examination Series

Topic: HIPAA Compliance

Presenter: Brian Thomas

Brian Thomas: Hello, and welcome to the AICPA CITP Credential Examination series. This podcast will assist you in preparing for the examination specific to the topic of HIPAA compliance. This is Brian Thomas. I'm a partner with Weaver, an accounting firm in Texas with offices on both coasts. My role is I'm the partner in charge of the firm's IT advisory services practice which includes IT audit and security services. I'm also a member of the IMTA executive committee.

Today we're going to be talking about HIPAA. HIPAA is actually an old law that was passed in 1996. It stands for the Healthcare Insurance Portability and Accountability Act. It got a boost though in terms of its enforcement through the HITECH Act, which was actually passed in 2009, which has generated a lot more current interest in the subject.

While HIPAA addresses many things, when people refer to HIPAA compliance, they're typically referring to the rules relating to the privacy and security of protected health information. What is protected health information? It's any information about health status, provision of health care, or payment thereof and this is the context we'll be discussing HIPAA in today.

Real quickly we'll be covering four main subject areas. First, how does HIPAA affect organizations. Two, what are the general requirements of HIPAA. Three, what is the plan of attack for compliance with HIPAA and four, what are some the common pitfalls that we see in compliance with HIPAA through some of our clients.

First let's talk about how HIPAA may affect your organization. First off it affects two main parties, covered entities and business associates. Covered entities are described as health plans, clearing houses, and health care providers. Obviously that affects parties such as hospitals, health care organizations, clinics, doctors, and medical practices but it also affects health plans which would include both insurance carriers, as well as those that are self-insured. If you think about your organization's own health care plan, to the plans you're providing to your employees, these would be considered covered entities.

Business associates are those who do business with or on behalf of a covered entity involved in the use and disclosure of protected health information, "PHI" as we're referring to it. Common examples would include, third-party administrators, perhaps data hosting providers, IT outsourcing firms, accounts receivable processing billing and collection firms, mail processors and yes, accounting firms. Specifically those accounting firms that may have access to protected health information through the services they're providing to their clients. This could be audit or tax services being provided to medical institutions, doctor's practices, doctors themselves, all of the billing records and other types of records that are processed through those organizations are going to contain protected health information.

Then let's talk about the requirements. When we talk about the requirements for HIPAA, while there are many requirements involved with HIPAA compliance overall, typically the ones that we're most concerned with from a compliance perspective are going to be those that are involved with the privacy and security rule.

Underneath the privacy and security rule, there are several safeguards that need to be considered. They're typically referred to as the administrative, technical and physical safeguards, as well as various organizational and policy and procedure documentation requirements.

All in all, there are about 50 total requirements that have to be considered and implemented, and many detailed sub-requirements. Those requirements are as broad as policies and procedures and requirements for training, and they can be as specific as password requirements or encryption requirements necessary for the transmission of protected health information. Many of the requirements are actually relating to processes, including risk assessment, incident handling and management, and breach notification.

Now then let's talk about the plan of attack. First off, we would recommend that you start with classifying and inventorying your data. This entails considering everywhere throughout your network and throughout your systems where you may store, process, and transmit protected health information. This endeavor would include perhaps searching throughout the network looking for repositories of information that include protected health information, as well as interviewing various parties throughout the organization to understand how they're handling and processing and storing information.

Next then we would recommend that you do a broad risk assessment. Things that you should consider with respect to a risk assessment for HIPAA would include, were there ways in which this PHI could be exposed, who has access, how well-controlled is that access, has that access ever been audited, how much has the organization invested in security tools and processes to stop common threats like malware, ransomware, phishing? Are third parties involved in the handling, transmission or storage of protected health information? Next, we would recommend that you implement policies and controls to address the higher risk potential exposures. A good reference point to consider when trying to determine which policies and controls to implement would be the information that you can reference on the Department of Health and Human Services website, to reference the technical and administrative safeguards for securing protected health information. Those risk areas that are considered to be higher should be prioritized in terms of the implementation of controls and processes.

Next, we would recommend that you perform a HIPAA gap assessment, similar to implementing policies and controls we would recommend that you download the information available on the Health and Human Services website to understand the technical, administrative and physical safeguards that are necessary to be implemented for HIPAA. Utilizing these requirements and the sub-requirements underneath those, you can go through and essentially evaluate which policies and procedures you already have in place, and those that you do not. Some may be partially covered through existing policies and procedures.

By going through that process and considering the risk assessment that had been previously conducted, you can come up with a prioritized approached as to which gaps are most significant and need to be addressed immediately, versus those that can be addressed over a period of time.

The last step you need to perform is to operationalize the HIPAA compliance program. What does this mean? It means pulling it all together, creating a single document that allows you to understand how the concepts and requirements of HIPAA are addressed by the various policies and procedures that exist within your organization, periodically re-assessing the risk by performing annual or more frequent risk assessments and training your employees.

Now, let's talk about some of the common pitfalls. What are some of the common pitfalls that we see with HIPAA compliance in various organizations? Well, typically what we often see when we first go into an organization is that while they may have many of the requirements addressed, they're addressed through informal and loose documentation, disparate policies and procedures that are not pulled together into a single compliance program addressing the HIPAA requirements.

What we also see is that there's a lack of regular risk assessment. The risk assessment component is one of the first requirements that you have to address through HIPAA compliance, and so not having a regular risk assessment process in place will, by default, make you non-compliant with HIPAA.

Weak incident identification procedures and response procedures are also a common pitfall.

While the organization maybe have documented a policy to respond appropriately when they identify an incident, what we often identify is that when you get into the actual procedures that the organization is performing, they do not have adequate procedures in place to actually detect an incident, so being able to detect the incident in order to trigger the actual response process is a common pitfall we see within organizations.

Lastly, we also see that a common pitfall is not thinking broadly enough about where PHI might be stored, processed, and transmitted throughout the organization, including third parties. Where third parties are involved, a business associate agreement should be implemented, and that business associate agreement should be transferring the requirements of HIPAA from the covered entity to the other business associate who is performing some sort of activity on behalf of the covered entity that relates to PHI.

Business associates can also have additional business associates themselves. These would be subcontractors; good examples of that would include IT service providers, and data handling and data storage providers that we mentioned as well, so those organizations would also potentially need to have business associate agreements in place that would transfer the requirements of HIPAA to those sub-service providers that are participating in the services necessary to the covered entity.

I hope you found this information to be useful. In summary, we've covered one, how does HIPAA affect your organization? Two, what are the requirements? Three, what is the plan of attack that you can use for HIPAA compliance? Four, what are some of the common pitfalls?

On behalf of the AICPA Information Management and Technology Assurance Division, this is Brian Thomas. I'd like to thank you for tuning into this CITP Exam series podcast on the topic of HIPAA compliance. This is just one in a series of podcasts that the AICPA's IMTA Division is pleased to offer around a variety of topics of importance for the CITP exam. Be sure to check out other podcasts in this series on topics that include, Data Analysis and Reporting Infrastructures, Data Backup and Recovery, Information Lifecycle Management, the COSO Model Framework, Service Organization Controls, PCI Compliance, and Internal Audit. Thanks for listening!

Disclaimer

This podcast is designed to provide illustrative information with respect to the subject matter covered, and does not represent an official opinion or position of the AICPA or AICPA.Org. It is provided with the understanding that the AICPA and AICPA.Org are not engaged in offering legal, accounting or other professional service. If such advice or expert assistance is required, the services of a competent, professional person should be sought. The AICPA and AICPA.Org make no representations, warranties or guarantees as to, and assume no responsibility for, the content or application of the material contained herein, and especially disclaim all liability for any damages arising out of the use of, reference to, or reliance on such material.