HIPAA Programs: Design and Implementation

Chris Brown, CISSP, CISA

The degree of success of operating within the rules of Title II of the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) depends upon the ability of the organization to establish a program that ensures thoughtful and consistent execution of the requirements of HIPAA.

PROGRAM

A dictionary definition of program might be “a plan or procedure for dealing with some matter,” or “a series of steps to be carried out to accomplish some goal.” If one expands these definitions to include an explicitly stated ongoing component, then one can establish a working definition for program as it is meant in the context of a HIPAA program. Thus, our definition would be “a plan or procedure for dealing with some matter on an ongoing basis.” It is the “ongoing” characteristic that makes a program distinct from a project.

This article describes a program approach to deal with the security and privacy standards required by HIPAA. It is the significant ongoing requirements of these two standards that set security and privacy apart from the other standards, including transactions and identifiers. The transaction and identifier standards, once in place, require little ongoing oversight except to deal with those issues that organizations already face today, such as coding errors and transmission errors. Transactions and identifiers are a one-time implementation and of a project nature.

Privacy versus Security. The final security rule makes a clear distinction between privacy and security by defining security as covering electronic protected health information (PHI), and privacy as covering all other PHI. These definitions are somewhat different from the common definitions for privacy and security. In the common use, privacy is the state of being free from intrusion into, or disclosure of, personal information or affairs; privacy is almost always considered an attribute of individuals. In the common use, security concerns itself with any information and the conditions that are sought: that is, confidentiality, integrity, and availability.

The program approach. Establishing a program requires that specific supports be in place. First, executive support is a
must. Very few organizations will be able to successfully implement and maintain a program without at least tacit approval from executives. Explicit and active support from executives can help deal with political issues and let the officers concentrate on the program itself. In this regard, HIPAA legislation brings an advantage to information security and privacy program managers and directors in the healthcare industry. The administration is legally compelled to support the privacy and security programs. While this does work to one’s advantage initially, over time one will want to be sure to establish an understanding within the ranks of the executives of the reasons that HIPAA came to be in the first place: that is, why privacy and security are important.

SELECTING AN APPROACH

If it has not already, an organization will need to make a decision regarding the overall approach for HIPAA compliance. Financial constraints, availability of staff, timing, and other issues will be considerations. Because it is unlikely that the Chief Privacy Officer (CPO) or Chief Security Officer (CSO) sits on the board and is fully aware of all issues facing the organization, it is important that these individuals ask directly what their mandates are. The CPO and CSO (the officers) will need to clearly understand the intent of management. The approach can range from “just compliance” to a full information security program based on organizational needs, which would be a “progressive” approach and would include HIPAA compliance. In some institutions, the leadership has chosen, explicitly or tacitly, to wait on HIPAA.

The Traditional Approach

The more common approach is to use HIPAA compliance as the focus and the single driving reason for the information security and privacy programs, and then “adding on” those things that would be considered prudent and that seem to fit as issues are discovered. Most will start with the HIPAA compliance approach. This is often the case because of the difficulty in positioning the information security and privacy programs as important. The traditional approach will also be adopted out of necessity by those organizations that are considerably behind in program implementation.

The advantage to this approach is that HIPAA is the law; and staff will generally understand that if it is required by HIPAA, there is no choice, whether or not workers and management agree with the wisdom of the new rules, and whether or not they understand those rules. The compliance approach is quicker to get going, easier for people to go along with, and requires less work and time initially on the part of the officers and administration.

There are disadvantages to this approach. While HIPAA itself has many of the components of good security and privacy programs, just following HIPAA may not provide a whole security–privacy program. HIPAA merely establishes the minimum requirements across an organizations. Following just the minimum requirements is likely to leave gaps, some that are specific to an organization’s particular environment. In particular, following only the HIPAA required specifications may leave one quite short of a sufficient program. In some way, the risk assessment requirement of HIPAA is meant to ensure that these gaps do not occur, but it should be kept in mind that this measure is only as good as the quality of the risk assessment. Only in extremely small organizations would following only the required specifications be appropriate or prudent.

The Progressive Approach

This approach requires that the organization, through the CPO and CSO, look at what needs to occur throughout the organization to ensure the privacy and confidentiality of patient data and the general security of all other data of importance to the organization and its constituents.
The advantage to using the progressive approach means that the officers can look beyond what is required by HIPAA, to other industries that have experience with information security, at industry-agnostic best practices, and at technologies that solve more than just the HIPAA “problem” at hand. This presents many more opportunities for creative solutions that can fulfill more than one need or want. It is an opportunity for organizations to invest in new technologies that may increase the efficiency of diagnosis and treatment, quality of care, and timeliness of payment. Once commitment has been given, it leads to greater success and a greater likelihood that those involved will understand the reason HIPAA was created in the first place, the purpose it serves today, and how following and acting the intent is more beneficial to the organization than following the minimal letter of the law. It also means that one has a larger group of people helping the officers create novel and often simpler solutions for problems, problems that in a compliance mindset might seem difficult or intractable.

There are disadvantages to this approach. It is more difficult to sell this type of program. It requires that officers be able to articulate organizational reasons for security and privacy beyond mere compliance. This, in turn, requires that the officers understand the business well enough to do this.

**Getting Started**

Once an organization has made an initial decision about where along the traditional progressive continuum it envisions going, the next step is to lay out a plan of how to get there. The plan should explain how the organization will use the adopted approach to achieve HIPAA compliance.

Each organization has unique situations, and there are different levels of risk tolerance and openness to change. Even within a single organization, the risk tolerance and openness to change will vary. Taking these factors into account is important in designing the program. Although it might appear to undermine authority, asking for the opinions and input of relevant departments during the design of the program is one step in ensuring later cooperation and the ultimate success of the program. One very important reason to do this is that it is an opportunity to educate the organization about HIPAA, what it means, and why it is important. Although this is not specifically treated as awareness, it is the first step in the awareness component of the program. This approach makes the often safe assumption that it is the intention of most people to do what is right, if people have the right information and enough time to think about it.

The officers’ role in this process is that of educator and consultant. It is important to give managers and department heads latitude in deciding how to implement those components that do not have required implementations. Working to educate and working in a collaborative manner is more likely to produce solutions that will remain in place when not under the watchful eye of the CPO and CSO. It is also more likely to produce those creative solutions that may be easier, less time consuming, and less costly.

**Policy as the Guide**

After the initial meetings with senior management, the next step is to create high-level policies or statements of intent to use as the foundation and guide for the rest of the program. These policy documents will help clarify and communicate what needs to be done.

**Organization**

It is sometimes said that people are more important in achieving security than are policies and technology. If one considers that all the technology available to the organization and all the policies created by an organization will not be able to overcome a staff that is intent on subverting those controls because they feel those controls interfere with their ability to do their work, then this statement is true. For this reason, one starts with the people during the design and implementation of the plan. Here one talks...
about education, and establishing roles and responsibilities.

**Education**

It cannot be overstated that the position that the officers should take early in the establishment of the program is that of educator and consultant. Every interaction offers the opportunity to explain the requirements of HIPAA, the roles of the officers, the rationale for security and privacy, and how HIPAA is everyone’s responsibility.

**Establish Department Ownership**

The first steps in the education process occur at each meeting between the officers and each individual or group outside the security or privacy offices. At these meetings, HIPAA and the roles of the officers should be explained. It is very important that the officers do not take ownership away from other parts of the organization. Taking responsibility at an inappropriate level would defeat part of the purpose of the meeting, which is to start the process of leading other departments to understand how each department “owns” a piece of the organization’s HIPAA responsibility. That is to say, it is the responsibility of the department head and other administrators to ensure department compliance with HIPAA regulations, and it is their responsibility to also work with other departments to achieve compliance with HIPAA regulations across the organization. Helping them understand this creates a distinct advantage for the officers and, ultimately, the organization. It means that the officers are no longer the “HIPAA police,” but rather the people who will assist the department and the organization in ensuring HIPAA compliance by working with them and providing expertise.

**Assign Roles and Responsibilities.** A key area in the design of the HIPAA program is the assignment of roles and responsibilities. To a large extent, the areas of CPO and CSO oversight are defined by the privacy and security standards. However, how the work is distributed and how it is assigned is a function of the organization’s size, structure, and practices. This should be kept in mind when deciding who does what. Because HIPAA compliance is impacted by nearly every individual in the organization, some level of responsibility should be established for every role — from the part-time volunteer all the way up through the administration, including the president and CEO.

**Developing the Schedule**

Although this article does not discuss project management fundamentals, it is worth mentioning that it is important that milestones and internal deadlines are established for at least getting the program up and running and for achieving compliance, and for one level of sub-tasks that occur underneath these overall goals.

However, it should also be noted that at the time of publication of this article the deadline for privacy will have passed and the deadline for security will be a year away (or less). If the organization is not well on the road to privacy compliance and at least started with security compliance, consider accelerating the program to the greatest degree possible. Noncompliance is likely to be reflected in accreditation reports and scores for healthcare provider organizations. Repercussion of noncompliance will likely manifest itself for plan organizations and for clearinghouses through strained relationships with other covered entities and possibly with reduced business with organizations that contractually require HIPAA compliance. For all organizations, there are established, federally mandated fines for reported violations of privacy. Given the realities of the deadlines and the potential costs associated with noncompliance, an organization that is significantly behind may want to consider bringing in outside resources to help with developing the program. Tight timelines do not lend themselves to the learn-by-trial method. Much of the up-front time can be shortened by bringing in competent assistance from those who
have already done this type of program development work.

**DESIGNING THE PROGRAM**

Once the preceding pieces are in place or in progress, the foundation has been set for the actual steps that implement the program.

**Risk Assessment**

A risk assessment at an early stage of the process of program development will help highlight those areas that create the most risk and those that are most critical to address. A risk assessment is intended to identify and rank assets, identify threats and vulnerabilities, and measure probable impact when vulnerabilities are exploited by or exposed to a threat. While anecdotal and ad hoc assessments are valuable and have their place, the formal process of risk assessment creates a much clearer and more reliable picture for the organization. In addition, the process of involving key groups in a full risk assessment is a good instructive exercise and can lead to “a-ha” moments for everyone involved.

Risks can be dealt with in one of three ways. One choice is to **accept the risk**, which is an acceptable choice if the cost of fixing a situation is more than the potential loss of not fixing the situation. Another choice is to **assign the risk**. A common example of risk assignment is fire insurance. It is difficult to build a fireproof building; because of this, insurance is purchased to assign the cost of the risk to the insurance company. A third choice is to **mitigate the risk**. When dealing with risk, there are often at least some steps to mitigate risk. Referring to the fire insurance example, fire alarms and sprinkler systems can be installed to improve response time and reduce damage.

**Documenting Roles and Responsibilities**

A previous section discussed steps to establish roles and responsibilities. This step focuses on the documenting of these roles and responsibilities. The way in which one documents depends on how responsibilities are already documented in the organization. It should be consistent with the approach used to the extent that it fulfills the program requirement of having the responsibilities documented. This is to say, if one currently does not document roles and responsibilities, then one will have to start. The process of defining roles and responsibilities could arguably be considered part of the policy development process.

**Policies**

A program such as HIPAA should be founded on policy. The CPO and CSO have the responsibility to help develop policies that support the privacy and security of PHI as required by HIPAA, but also to make sure that policy takes into consideration operational, financial, logistical, and human realities.

How an organization structures policies will have an impact on their effectiveness, but only to the degree that makes sense and to the degree that it fits with the existing policy structure. Keep the audience in mind. For example, an organization may decide that it needs policies to cover e-mail and communication systems use, Internet and intranet use, desktop and laptop use, employee monitoring and privacy, user password selection and management, transmission of sensitive data, and physical protection of data. It may also be useful to provide examples of acceptable and unacceptable use. To require staff to read several of these policies can be burdensome and difficult to track. In this situation, consider structuring policies around the reader or the audience, in contrast to structuring policies around a topic, technology, or the policy.
writers. In this case, a single Acceptable and Responsible Use Policy may be easier for readers to consume, even if it comes with the trade-off of slightly more difficulty in policy maintenance on the part of policy writers.

The level of familiarity required for each person with each policy will vary with the role of that person. The ideal situation is to make it as simple as possible for the audience to understand what they need to read and know, and know how to get a hold of it. Ideally, the majority of staff will only need to be familiar with one policy. Management will need to be familiar with a specific set of policies, and IT staff will need to be familiar with a different set of policies.

The list below outlines recommended coverage of one’s body of policies. If using the audience-based approach, structuring policies into the following groups will work. Keep in mind that it is not necessarily the responsibility of the officers to create the following policies, but rather to make sure that they are in place and incorporate information security and privacy issues.

- **Program charter.** This is a document that formally recognizes information security or privacy as an organizational function and requirement, signifies management backing, and designates the officers. (Not required, but helpful in organizations resistant to change.)
- **Risk management.** Risk management provides guidance to assist in assessing, analyzing, reducing, and managing the risks to information systems and telecommunications networks.
- **Staff behavior.** Commonly referred to as an Acceptable Use Policy (or AUP), the purpose of this policy is to outline the guidelines and principles for information system use by all staff. It reviews at a high level all aspects that staff needs to be aware of and understand.
- **Data management (classification, disposal).** The intent of this policy is to guide staff on how to handle the information to which they have access; in particular, what information can be disclosed to non-employees and how to dispose of old paper records. This policy should cover data classification definitions, assignment of data ownership, labeling, access control, third-party interactions, shipping and handling, and destruction and disposal. Note that declassification and downgrading can be included in this list in a non-healthcare environment.
- **Information technology system management.** This policy establishes technical security practices and procedures for information systems that are owned or operated by the organization. Configuration and change management policies should already be established, and processes being followed. Items to consider in this policy include a review of hardware and security features prior to purchase approval; general system requirements; authorization for access to systems, applications, and data; access controls; audit; virus protection; security feature testing; data encryption; network alarms; event reporting; and documentation.
- **Physical security.** This policy has been established to protect sensitive information from accidental, unauthorized, or intentional modification; destruction or disclosure during input; and processing or output operations due to lack of or poor physical controls. Items to include are general facilities security, facility plan outline and content requirements, physical access controls (separation, escort, special areas), workstation placement, portable computers, equipment transfers (loans, repairs, nonorganizational equipment), and media controls.
- **Account and access management.** The Account and Access Management Policy governs the process for requesting access to the organization’s information systems, such as network and software applications. Items to cover include data owner approval, monitoring and suspension of privileges, and unused access. For this policy, it might make sense to include general or high-level procedures...
or requirements for procedures, specifically for the establishment, modification, and termination of accounts.

- **Personnel policies (specifically IT personnel).** The purpose of this policy is to outline the requirements for clearance and authorization of all entities prior to accessing organizational information assets. It should cover agreements and awareness training. Other items to cover include clearances, authorization, supervision, training, and records compliance review.

- **Sanction.** The purpose of this policy is to outline the use of disciplinary sanctions within the organization. Inappropriate behavior and use of confidential information, networks, and systems exposes the organization to risks, including confidentiality breaches, compromise of services, and legal issues. Items to cover include violations (reporting, investigations); progressive discipline; actions (for lesser violations; professional ethics violations, criminal offenses); and in the case of covered entities, HIPAA penalties. These should be Human Resource department promulgated policies. The role of the officers is just to ensure that the proper pieces are included in the Human Resource policies.

- **Disaster recovery (DR) and business continuity (BC).** This policy should provide guidance to assist the organization with identifying its critical business information assets and developing the documentation required to create disaster recovery and contingency/business continuity plans. This document itself is not the DR plan or the BC plan itself, but outlines the minimum requirements for such plans. In addition, this document should assign responsibility for recovery (DR) to IT and operational continuity (BC) to the business units. This policy explicitly requires things such as phone trees and emergency communication procedures.

- **Incident response.** When loosely defined, an incident can be described as an adverse event. It might take the form of a power outage, an infection by a virus or worm, a social engineering attempt, or a natural disaster. When dealing with incidents within the realm of security and privacy, incidents are usually categorized into one of three categories: (1) privacy incidents, (2) security incidents, or (3) disaster events. Privacy incidents involve the accidental or intentional release of protected health information (PHI). Security incidents entail the compromise or attempted compromise of the confidentiality, integrity, or availability of systems or data. Disaster events interrupt the suitability of the environment in which work is being conducted or the availability of resources for conducting work and can be man-made or natural.

  The purpose of this policy is to provide procedures for responding to and handling privacy and computer security incidents. This document is meant to provide all personnel with guidelines on what to do if an incident is discovered or reported; it is meant for those who are responsible for responding to the incident. Portions of this policy will pertain only to incident handlers, and should not be generally available. The policy should cover required use of the incident report form, log books, communication (informing management and other appropriate personnel), release of information, and follow-up analysis. Specific procedures may cover privacy incidents, virus and worm incidents, hacker incidents, active hacker activity, handling hacker incidents, monitoring of hacker activity, and evidence preservation.

- **Compliance and audit.** This policy provides the authority for the officers (and possibly specific roles within the IT department) and designees to conduct security audits on any organizational network or system. Also to be considered for inclusion in this policy are required notifications by these individuals to HR, compliance, and executives; officer requests for access (establishes authority); and requirements for audit logs.
ESTABLISHING CLASSIFICATION
Some in the healthcare field say that there is only one data classification scheme of relevance today. It has two categories: (1) PHI and (2) non-PHI. This is an extreme view; but considering all the data that is formally classified under the regulations as PHI, it is not an unreasonable place to begin a data classification scheme in a healthcare environment. This is especially true for an industry or organization that is underfunded or behind its peers in terms of information technology and information security in general. HIPAA itself does not directly address data classification; but in practice, it creates the PHI and non-PHI classes already mentioned.

The basic recommendation is to not have too many data classification levels. Keep in mind that each additional classification level creates more administration requirements and is likely to create more confusion among staff. Unless there is full-time staff available to manage the data classification process, as in Department of Defense agencies, do not use more than four. In most cases, even four is not required. Consider starting small and work your way up; a simple classification system with some compartmentalization is sufficient for most organizations. It should be noted that classification levels should be collectively exhaustive and mutually exclusive.

Beyond PHI, consider what type of work the organization performs. There is just as much variation in the healthcare industry as there is in any other industry. One will have to consider the particular circumstances. Is it a research institution? Is it for-profit? What are the sources of funding? Do you frequently have visiting physicians; what is the general purpose of their visit? Are your own employees using your services, and are they covered by your plans or services? For each of these questions, there is a type of data to consider in the classification scheme.

In addition, every business — regardless of type — will probably have some concern over general things such as strategic plans, profitability by service or product line, income and donations by source, staff salaries, proprietary techniques, and research being conducted or research results.

Consideration for worker data — when employees and other workers use the services of a healthcare organization, it creates a special requirement that that PHI is not accessible by any but a special set of employees designated to handle employee-related data.

If, for example, an organization determines that it is concerned about just four types of data (e.g., PHI, employee data [PHI, salary, vacation time, benefits], strategic, and financial), then one might map all of the data into three classes: (1) Sensitive (PHI, employee PHI, employee data, strategic, and financial); (2) Internal Use Only (the catchall for internal memos, documentation, administrative output, procedures, etc.); and (3) Public (anything formally approved for release by member relations, public relations, foundation, or legal, depending on the organizational structure).

Technical Architecture
This provides a “roadmap” for technology purchases, design, and implementation. The audience is the IT staff and those making IT purchasing decisions. The design should provide enough information to allow those making decisions to understand how new or newly configured systems should fit into the overall architecture. Considerations should include network design, proxies and reverse proxies, authentication infrastructure, open and closed communication paths, directory systems, management systems, and networks.

IMPLEMENTATION
Integration into Life-Cycle Processes
The easiest way to make HIPAA part of the everyday life of workers is to take existing processes, procedures, documentation, guides, and ways of doing work and incorporating HIPAA into them.
System Acquisition and Retirement Management. Information systems have distinct life-cycle phases. For purchased systems, these phases are selection, implementation, maintenance, and retirement. For built systems, these phases are design, implementation, maintenance, and retirement. Each of these phases requires attention to privacy–security concerns. Consider establishing or supplementing checklists or questionnaires.

System Configuration Management. Systems will generally change due to the application of patches, small changes to configurations to fix various operational problems, the installation of utilities used by system administrators, and for other reasons. In most cases, security will be impacted in some way. It is important that the impact on security be assessed for each change. Periodic system assessments should be conducted to ensure that the cumulative effect of changes did not have unintended consequences. Having good configuration management documentation off-site also assists with disaster recovery efforts.

Change Management. System to confirmation management and changes to applications can impact security. Application changes should be reviewed for potential impact, and put through further scrutiny if it is possible that security will be impacted.

Physical Security. Although the privacy and security rules are distinct in that security covers electronic data and privacy covers nonelectronic data, physical security is important to both. Within the plan, the organization will need to determine where PHI resides, be it in electronic or physical form. Locations to consider on the security side include server rooms and data centers, wiring closets, publicly accessible data ports, servers outside of controlled space, telemetry equipment, any place that PHI can be stored or processed, and every place that networks carrying unencrypted PHI exist or can be accessed. On the privacy side, consider patient (member) record areas, mail rooms, nurses’ stations, patient rooms, call centers, and any other place that PHI is stored or handled. Be careful not to be too quick to discount a particular area. Janitor closets often serve as wiring closets. PHI is almost everywhere in a provider environment, from the pharmacy to the patient charts on the room doors and the nurses’ stations, to the telemetry monitoring screens in various, sometimes highly visible locations. Look for nontraditional media that carry PHI, such as prescription bottles or bags, and sample containers.

For all these areas, establish physical access controls, and ensure proper and complete records of access and appropriate supervision of visitors, vendors, students, temporary employees, and others who are not cleared and regularly authorized for access.

SECURITY AND PRIVACY TOGETHER

The advantages and need for collaboration between security and privacy should be understood. Look at the history of HIPAA as background for this idea. It started with ensuring continued healthcare coverage when employees moved among employers (Title I). This led to the need for administrative simplification (Title II), which then led to the need for standard identifiers and standard transactions. This, in turn, led to concerns over privacy of health-related data. After considering what would be required for making the privacy rule actually work as it was intended, security became a requirement. In healthcare environments in particular, security and privacy can be viewed respectively as a “what” and a “why.” To separate these components is to ignore the history. Separating them also makes it more difficult for security to be seen as a reasonable measure in an environment that is traditionally open, supportive, and sharing.
INTERNAL GROUPS WITH WHICH TO WORK

Building alliances between the HIPAA officers and other departments will help the organization achieve HIPAA compliance. Keep in mind that not all organizations have all these departments. They may go by a different name or be consolidated into one department. For example, Training may be part of Human Resources; Internal Audit may be part of Risk Management, or vice versa. Ask around to find out who is responsible for this work in the organization. Talk to the individuals and management from these departments and see what the common goals are; then start building a list of allies.

Human Resources/Personnel. Human Resources (HR) or Personnel departments are a key entry point for an organization’s new employees. They are often involved in terminations. Hooking your information security and privacy process into HR processes may mean more timely account management when employment status changes. This is also a key place for training. In the process, one can help HR communicate more effectively with IT and Facilities and help them streamline their processes.

Training. The training department can help create an effective training program and can also get one’s issues incorporated into standard training modules. Key modules to ask about are new worker training and any periodic training that is already given to workers. Training may also be able to provide ideas for measures of the effectiveness of the information security and training provided.

Internal Audit and Compliance. These groups are responsible for ensuring that the company is behaving in accordance with generally accepted accounting and financial practices and regulations. In some organizations, their responsibilities extend outside finance and medical compliance, possibly into IT or Operations. Often, they can help identify issues that the officers should be aware of, particularly if Audit interfaces with many other departments. They may also be aware of the issues that external auditors will be reviewing, prior to their arrival. Although they can be cast in a negative light, internal auditors are there to help the organization just as much as any other function. They are held to certain standards and go through regular reviews by external auditors. The officers can help the internal auditors by providing documentation, time for interviews, or other material when requested.

Risk Management. Risk Management takes on different meanings in different organizations. In many HIPAA covered entity environments, risk management refers to either health risk management or legal risk management. Both inside and outside the healthcare industry, risk management may include general business risk, and may fall to the Internal Audit or Legal departments. Depending on the responsibilities of the Risk Management department, there may be common goals between the HIPAA program and Risk Management. The way the officers help Risk Management is by helping to identify and make them aware of the risks that the organization faces.

Quality. Quality is often about processes and improving upon them. To that extent, quality touches all areas of the organization, much like security and, to a lesser extent, privacy.

Executive Management. Believe it or not, executive management is most likely on your side. There are a few things to watch out for in one’s own behavior when dealing with this group. Do not be overzealous about information security issues themselves; speak to the business issues. While executive management leadership styles vary, one will get a lot of mileage out of the approach of being brief and to the point — but be prepared with backup information.
Laws, Behavior, and Culture: Setting the Stage

Laws are enacted to establish behavior with respect to specific subjects, and culture influences behavior in respect to all subjects. Being a change maker requires either a culture that is adaptive to change or modifying the culture for it to accept HIPAA required changes. Playing the “this is required by HIPAA” or “JCAHO will ding us unless we do this” card will work to a degree, but it should be used as a trump card, not as the lead card. Be careful if citing external reasons for taking a certain action; this can lead to doing the minimum required.

Self-Evaluation

Once the program is up and running, how does one evaluate how the organization is doing? The way that requires the least work is to have a third party evaluate the program. If one is inclined to do it oneself, there are a couple of simple ways to conduct a self-evaluation.

The process of staging an incident may be helpful. “Table-top” reviews of plans can identify gaps and be an avenue to improve plans. Be sure to include staff as well as management, as staff is often able to add a lot of creative solutions to encountered problems. Consider running an incident test, a DR test, or a BC test. Ask the people in the hall if they think about security. If one is looking for more quantitative measures, then conduct observations of workers areas, test samplings of system configurations, run network scanning tools, or give staff a formal test.

A Word about HIPAA “Certification”

There is no organization-based certification for HIPAA. A standard or de facto standard for auditing for compliance has not been established. For the privacy rule, the Office of Civil Rights has been assigned the responsibility of ensuring compliance. For the security rule, the entity that will be assigned the responsibility of ensuring compliance has not yet been announced. It is quite likely that the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and other similar accrediting organizations will start including some aspects of HIPAA compliance in their audits.

Getting Outside Help

Some consulting firms in the United States are offering HIPAA assessments. The assessment entails the consulting firm interpreting the HIPAA required and addressable (privacy and security) components and measuring the organization against this interpretation. Because an audit process has not been defined by lawmakers and the rule itself has not been tested in the real world, there are some aspects that may be more open to interpretative variation than others. The quality of the consulting firm and the individuals conducting the assessment will have a bearing on how valuable any particular assessment might be. Be wary of consulting, audit, and law firms offering HIPAA “certification.” Look for organizations that not only know the HIPAA rules, but that can articulate how they use HIPAA in their assessments and how they apply it to various organizations.

Author Note

This article is for informational purposes only. It does not contain legal or other advice. For legal advice on HIPAA compliance, seek competent legal counsel.