Applying Your Corporate Compliance Skills to the HIPAA Security Standard

Patricia I. Carter, JD

ABSTRACT

Compliance programs are an increasingly hot topic among healthcare providers. These programs establish policies and procedures covering billing, referrals, gifts, confidentiality of patient records, and many other areas. The purpose is to help providers prevent and detect violations of the law. These programs are voluntary, but are also simply good business practice.

Any compliance program should now incorporate the Health Insurance Portability and Accountability Act (HIPAA) security standard. Several sets of guidelines for development of compliance programs have been issued by the federal government, and each is directed toward a different type of healthcare provider. These guidelines share certain key features with the HIPAA security standard. This article examines the common areas between compliance programs and the HIPAA security standard to help you do two very important things: (1) Leverage your resources by combining compliance with the security standard with other legal and regulatory compliance efforts, and (2) apply the lessons learned in developing your corporate compliance program to developing strategies for compliance with the HIPAA security standard.

KEYWORDS

• HIPAA
• Security
• Privacy
• Compliance
• Legal
• Standard
• Regulation
• Health information
• Risk assessment
• Risk analysis
• Gap analysis
To meet the requirements of the HIPAA security standard\(^1\) you will need to create an organizational framework, which includes risk assessment, internal processes, documentation, and training. This approach is very similar to organizational efforts to develop a corporate legal compliance program. If your organization has already undertaken to develop a voluntary corporate compliance program, it will already have many of the skills, organizational processes, and infrastructure that will be required to successfully implement the HIPAA security standard. If your organization has yet to develop a compliance program, now is a good time to start. The overlapping areas between corporate compliance programs and compliance with the security standard mean that your organization can gain efficiencies by undertaking these two projects concurrently, or by integrating the HIPAA security standard into an existing compliance program.

This article (1) provides an overview of corporate legal compliance programs, (2) summarizes the types of requirements found in the security standard, (3) reviews the risk assessment and gap analysis processes used for both the compliance programs and the security standard, and (4) reviews the seven core elements of a compliance program and the counterparts to those elements under the security standard.

Note: This article is based on the proposed security regulations (45 CFR Part 142), published on August 12, 1998. The final security standard is currently scheduled to be published in late 2000. Few substantive changes are expected; however, your should refer to the final regulations as you develop your implementation plans.

**Compliance Programs**

Healthcare providers implement legal compliance programs to establish internal controls to prevent, detect, and correct unwanted conduct. Compliance programs have become necessary due to increased enforcement and sanctions under the fraud and abuse provisions of HIPAA and the Balanced Budget Act of 1997. Compliance programs are not required by law, but they are fast becoming the standard of care in the healthcare community. The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) strongly encourages development of effective compliance programs, to address improper conduct under federal and state law, and Medicare and other payor programs. Furthermore, having an effective compliance program is a mitigating factor under the Federal Sentencing Guidelines. The Sentencing Guidelines' criteria for what constitutes an effective legal compliance program have shaped the development of these programs in the healthcare industry.

To support these self-policing compliance efforts, the OIG has issued compliance guidance for several segments of the healthcare industry, including hospitals, clinical laboratories, home health agencies, third-party medical billing companies, nursing facilities, and others.\(^2\) Healthcare providers, large and small, are developing and implementing compliance programs in an effort
to ensure legal and ethical business practices in accordance with guidance from
the OIG. Some do it to mitigate risks and penalties in anticipation of govern-
ment investigations or audits. Some do it because it just makes good business
sense.

A compliance program helps the provider avoid financial loss, legal lia-
ability, and reputational harm. A legally effective compliance program (meeting
the standards set forth by the OIG) will help providers reduce their risk of
criminal and civil litigation. While this is sufficient incentive for some
providers, others have recognized that a compliance program can be effective
in practical as well as legal terms. A compliance program can bring posi-
tive practical results—it can improve internal processes and patient service,
and increase employee efficiency and morale by clarifying appropriate prac-
tices and expectations.

A compliance program should effectively articulate and demonstrate the
organization’s commitment to legal and ethical conduct. To do so, it must fit
the culture, business operations, and risk management strategy of the organi-
zation. An “off the shelf” program is unlikely to become integrated into the
day-to-day operations of the organization and is, therefore, unlikely to succeed.

HIPAA Security Standard

The proposed security regulations, released by HHS in August 1998, will apply
to all healthcare providers, health plans, and clearinghouses that electronically
transmit or maintain individual health information. These standards gener-
ally represent good information practices that you may be following already.
In broad terms, the goals of the proposed standard is to ensure that electronic
healthcare information is accurate and available, but accessible only to appro-
priate individuals. To comply with these standards, you will need to develop
a security plan, provide security training for employees, and document your
security policies and procedures. Other administrative procedures, physical
safeguards, and technical measures will also be required and will vary by orga-
nization. The requirements in the proposed regulation have been divided into
the four categories shown in Table 1.

The final security regulations will be effective sixty days after they are
published, and you will have twenty-four months after that date to be in full
compliance. The final security regulations are expected to be issued late in
2000, which means being in compliance before the end of 2002.

The security standard is not meant to impose “one size fits all” require-
ments but is intended to be scalable and flexible. No specific technologies are
mandated, and the standard focuses primarily on policy and process issues,
rather than technology issues. HHS recognizes that, depending on size and
complexity, healthcare entities will have different security risks, needs
and resources. This makes it easier for you to match your compliance strategy
to your own risk assessment, but also makes it more difficult to determine
whether the security plan you design is sufficient to meet the regulatory
standards. Therefore, it will be important for you to document your risk assessment and risk strategy—that is, the reasons for the compliance choices you make in addressing these standards. Consider preparing a strategy document that outlines your decision making, including your risk assessment, resource issues, cost-benefit analyses, and the business and technological strategies leading to your ultimate approach.

Risk Assessment and Gap Analysis

Risk assessment, or risk analysis, is the process by which you identify vulnerabilities and threats to your organization, identify the resulting risks, evaluate the level of each such risk, and select cost-effective measures to address them. Risk assessment requires you to balance the cost of these measures against the losses that would be expected without these measures. As a result, no “off the shelf” compliance program or “one size fits all” approach to risk assessment will meet your compliance needs. Every organization’s vulnerabilities and risks are, at least to some degree, unique.

To assist healthcare providers in developing compliance programs, the OIG has issued guidance and identified risk areas for several industry segments. This guidance is extremely helpful in developing your own risk analysis, but is not a replacement for it. Simply adopting the OIG guidance without integrating it into your own organization will not be effective, legally or practically. There is no single “correct” compliance program for all providers.

Similarly, no two providers will implement the security standard in exactly the same way. The security standard is designed to be flexible and scalable and does not require any specific technologies. In fact, the security standard specifically requires each covered entity to assess its own security needs and risks, and to devise, implement, and maintain a security program to address those risks. Whether for a corporate compliance program or the

<table>
<thead>
<tr>
<th>Administrative Procedures</th>
<th>Physical Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>A broad range of internal policies and procedures, regarding matters such as passwords; “chain of trust” partner agreements; backup and disaster recovery plans; internal audits, personnel procedures; virus protections; training, and more</td>
<td>Controls over media going in and out of the organization (such as disposing) of old equipment; the physical placement of and protection of the computer system; policies for workstation use; and security awareness training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Data Security Services</th>
<th>Technical Security Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access privileges, audit controls, and data integrity measures</td>
<td>Prevention of unauthorized access to data over a communication network</td>
</tr>
</tbody>
</table>
HIPAA security standard, your risk assessment must be customized to your organization.

**The Risk Assessment Team.** Identify the appropriate people to participate in the risk assessment process, whether for a corporate compliance program or in the context of the security standard. For your organization’s compliance program, the compliance officer will spearhead this process—but he or she usually cannot do this alone. A compliance committee should be considered, at least at the developmental stage, and particularly in larger organizations. The committee generally consists of managers, officers, clinical staff, administrative staff, and others representing multiple disciplines within the organization. A cross-disciplinary team will provide insight and expertise in identifying risk areas and appropriate risk management strategies. For example, health information professionals should be able to identify problem areas that others might not be aware of, based on their knowledge of the organization’s uses and disclosures of information.

To successfully complete a risk analysis with regard to the requirements under the HIPAA security standard, the support and collective wisdom of a multidisciplinary task force will also be needed. This may be the same group that serves as the compliance committee. Certainly health information management staff should be included, and perhaps other staff or consultants with technical expertise. This security task force, or committee, can also provide valuable assistance in the implementation of the security standard.

**Matters of Privilege.** You should consider having an attorney as part of the compliance and security risk assessment committees. Your attorney can provide helpful expertise with regard to legal risks. Moreover, as with any internal investigation that may uncover problems, establishing attorney-client privilege for these discussions and findings may be very beneficial. Having your attorney closely involved in the identification of risk areas and discussions of risk management issues should help maximize the application of attorney-client privilege and work-product privilege to any facts you uncover in this process.

**Risk Assessment.** Once the team is in place, the task of risk assessment begins. The first step is to identify the vulnerabilities and threats to your organization. Although the OIG has identified some risk areas, your compliance program, as a voluntary program, does not mandate specific issues to be addressed. Your risk analysis must look at your own organization’s lines of business, sources of revenue, and organizational structure; and the framework of statutes, regulations, and accreditation in which it operates. A compliance program need not address every possible compliance issue, but it should strive to identify and eliminate significant risks.

In contrast, the security standard not only requires that you complete a formal risk assessment, but also that you provide a framework specifying the issues that must be addressed. However, as with the OIG compliance guidance, the security standard does not mandate specific solutions. The precise manner
in which the security requirements are met are adaptable to each organization's risk assessment.

The risk assessment process should help prevent your compliance program or security program from being too unfocused or unrealistic in scope and help you target your priority issues. It can also help you avoid another common mistake—putting too many resources into a single area. Do not be more ambitious than is dictated by the needs of the organization. The security standard is intended to be scalable and flexible, which allows you to match the legal requirements to the risks and resources of your organization. The downside of this flexibility is that there is no “safe harbor” under the security standard. As a result, it is critical that as you do your risk analysis and develop your implementation strategy, you document the process of developing your security policies and procedures. Explain why the policies and procedures selected are reasonable and appropriate choices for your organization. You may be called upon at some future date to justify the security approaches that were taken. In most cases, there will likely be no “wrong” rationale for the approach you chose other than having no rationale at all.

**Gap Analysis.** The second stage of the risk assessment process is to perform a gap analysis. Whether for the compliance program or the security standard, all existing policies and procedures should be reviewed. This includes both reviewing existing written policies and interviewing personnel to determine actual practices. These interviews will provide a “reality check” on your written procedures and will bring to light common practices that have never been reduced to writing. These interviews, ideally, should be conducted by a neutral third party (that is, not the individual’s supervisor) in order to get the most candid and accurate results.

Once you have determined the current operation of the organization, you can compare it with the legal and ethical requirements, as identified by your risk analysis. This gap analysis should identify any deficiencies. A second level of risk analysis is then performed—to quantify the risks associated with these deficiencies and the costs of mitigating those risks. Do your current processes and procedures adequately mitigate the risks you have identified? Quantifying the risks can be the most difficult part of this process, and it may not be possible to be precise. You should consider not only the likelihood that a problem will occur, but what harm would result if it does. Using a chart such as the one in Figure 1 may help you to think about the magnitude of risk for a given issue.

For example, the security standard requires that you have some type of backup system for critical information. What are the potential risks of having no backup system? For one, information vital to patient care could be lost. What is the likelihood of this happening? Perhaps a low or moderate risk of occurrence. What would be the resulting harm? Potentially lower-quality care, loss of business, or reputational harm to your organization. This would likely be considered high harm. You will want to address this issue in your security program.
Everyone’s resources are limited. Therefore, you should put the most resources in the high risk of occurrence/high harm areas. The fewest resources will be allocated to the low risk of occurrence/low harm areas. For example, if you transmit billing data over a private network, rather than over an open system such as the Internet, the likelihood of that information being intercepted is likely very low, based on your current process. The potential harm that might ensue if the information were accessed by an unauthorized person might be no more than moderate. As a result, you might choose not to encrypt that data.

For the risks that are to be addressed in your compliance or security program, create a checklist of policies, procedures, and standards to be developed, and where necessary, technological solutions to implement. Assign these tasks to appropriate individuals, and be sure all the resulting procedures and standards are documented, as well as documenting the risk analysis process itself.

The Seven Core Elements of an Effective Compliance Program

The compliance guidance provided by the OIG tells us that to attain the maximum legal benefits, a compliance program must contain the following seven core elements. These provide the framework for your compliance program, regardless of the specific risk areas to be addressed. Each of these elements has a parallel in the security standards, as explained below. Note: Table 2 provides a summary of these seven elements and includes a comparison to the proposed health information privacy regulations published by DHHS in 1999. For ease of reference, citations are given in Table 1 to the applicable sections of each regulation.

Implementing Written Standards and Procedures. As part of your compliance program, your organization should develop and distribute written
Table 2. Quick Reference Comparison of the Seven Core Elements of an Effective Compliance Program and the Security and Privacy Regulations under HIPAA

<table>
<thead>
<tr>
<th>Seven Elements of a Compliance Program</th>
<th>HIPAA Security Standards</th>
<th>HIPAA Privacy Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and distribute written policies, procedures, and standards of conduct that promote the organization's commitment to compliance and address areas of potential fund.</td>
<td>High-level security policy to provide framework for program. 45 CFR 142.308(a)(10)(iv). Written security plans, rules, procedures, and instructions regarding all components of an entity's security. 45 CFR 142.308(a)(8)(i).</td>
<td>A covered entity must adequately document its policies and procedures demonstrating compliance with the applicable privacy requirements. 45 CFR 164.520.</td>
</tr>
<tr>
<td>Designate a compliance office and other appropriate bodies, who report directly to the CEO and governing body.</td>
<td>Assigned security responsibility—practices established by management to manage and supervise the execution and use of security measures to protect data, and related personnel conduct. 45 CFR 142.308(b)(1). Includes risk analysis and risk management. 45 CFR 142.309(a)(10).</td>
<td>Designated privacy official, responsible for the development and implementation of the entity's privacy policies and procedures. 45 CFR 164.518(a)(1).</td>
</tr>
<tr>
<td>Conduct regular, effective training and education for all affected employees.</td>
<td>Personnel security system, which ensures appropriate supervision, records of access authorization, and personnel clearance procedures. Ensure all appropriate personnel receive security awareness training. 45 CFR 142.308(a)(7); (a)(12); (b)(6).</td>
<td>Conduct training for all member's of the workforce likely to obtain access to protected health information. Training must include the entity's privacy policies and procedures relevant to the individual's job function. 45 CFR 164.518(b).</td>
</tr>
</tbody>
</table>
Develop effective lines of communication to receive complaints, protect anonymity, and prevent retaliation against whistle-blowers.

Develop security incident procedures (formal documented instructions for reporting security breaches) that include report procedures and response procedures. 45 CFR 142.308(a)(9).

Designate a contact person to receive complaints, and develop a process whereby individuals may make complaints. 54 CFR 164.518(a)(2) and(d).

Conduct internal audits and other evaluation techniques to monitor compliance and identify problem areas.

Conduct internal audits, which are in-house reviews of the records of system activity to identify potential security violations. 45 CFR 142.308(a)(6); (a)(7); (a)(8).

No specific monitoring or auditing requirement specified, but must be able to account for individuals’ uses/disclosures under 45 CFR 164.515.

Enforce standards through well-publicized, appropriate disciplinary measures. Perform background checks, as appropriate.

Sanction policies and procedures regarding disciplinary actions, communicated to all employees, agents, and contractors. 45 CFR 142.308(a)(10)(iii). Personnel clearance procedures. 45 CFR 142.308(a)(7).

Develop and apply appropriate sanctions against workers for noncompliance. 45 CFR 164.519(e).

Respond promptly to detected offenses and initiate corrective action and preventive measures.

Security incident procedures (formal documented procedures) that include reporting security breaches and response procedures. 45 CFR 142.308(a)(9).

Procedures to mitigate, to the extent practicable, any harm from an improper use or disclosure. 45 CFR 164.519(f).
standards of conduct to employees. This code of conduct should set forth the fundamental principles and values of your organization and serve as the framework for your compliance program. Your organization should then develop and distribute more detailed written procedures to address the key risk areas. Appropriate managers and staff should develop these procedures under the direction of the compliance officer and distribute them to the appropriate individuals.

The security standard requires the development of a high-level security policy, setting forth the organization's fundamental principles in relation to protecting the confidentiality, integrity, and availability of information. Like the code of conduct, the security policy provides the framework within which more detailed security procedures and standards are established. The policy may be incorporated into the code of conduct to provide a single, integrated source of guidance for your employees. The security standard further requires comprehensive documentation of all policies and procedures you develop to satisfy each of the specified requirements. This documentation must then be made available to those individuals responsible for implementing the safeguards and must be reviewed and updated periodically. This is the same approach you should follow for compliance program materials.

**Designating an Officer to Provide High-Level Oversight.** A compliance program should be authorized and supervised at the highest levels of the organization. To ensure high-level oversight, the board of directors, partners, owners, or CEO should appoint a compliance officer to serve as the focal point of the compliance activities. The compliance officer should be outside the normal chain of command and have a direct reporting relationship to the board, CEO, or other high-level officer within the organization. The compliance officer should be someone in a position to influence individual and organizational behavior and needs to have the authority to exercise his or her independent judgment in developing the compliance program, auditing, and responding to incidents.

The compliance officer may be a full-time position or may represent additional duties for a current employee. Compliance activities should, however, be a material part of the person's job and part of the basis of his or her performance evaluation. The compliance officer should lead the risk assessment and risk management process, ensure that appropriate staff training is provided, oversee audits, maintain a hotline or other reporting mechanism, respond to complaints, and document compliance efforts. Coordination and communication are the key functions of the compliance officer. Fundamental to developing and maintaining effective compliance programs include knowledge of the organization's structure and operations; the ability to accurately interpret and implement regulatory requirements; the ability to interpret legal requirements; an established rapport with physicians and other practitioners; strong managerial, leadership, and interpersonal skills; and strong analytical skills. 7
Under the security standard, security responsibilities must be assigned to a specific individual (called a chief security officer). This chief security officer’s (CSO) responsibilities include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data. This CSO position is important in providing an organizational focus for security issues, emphasizing the importance of security, and pinpointing responsibility. The CSO will be responsible for developing, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. Security management also includes risk analysis and risk management.

As with the compliance officer position, the CSO may be either a full-time employee or additional responsibilities for a current employee. The CSO should likely not be the same individual as the compliance officer. The compliance officer may not be able to take on this additional workload; moreover, the CSO position requires technical skills and knowledge of information management, which may be outside the expertise of the compliance officer. The CSO may report to the compliance officer. At a minimum, the CSO should have direct access to and work closely with the compliance officer. Oversight of your organization’s security management should form an integral part of your organization’s overall compliance program.

**Conduct Effective Training and Education.** Training and education of all levels of the organization—including board members, management, staff, contractors, and volunteers—are critical to the success of any compliance program. These groups should receive general training on the compliance program, plus focused training on key policies necessary for each of them to fully understand their job functions. Compliance training encompasses a wide range of topics relating to applicable laws (such as anti-kickback, Stark/self-referral, Medicare/Medicaid coding and billing practices, quality of care, confidentiality, and conflicts of interest) and what employees need to do to comply. The security standards also require training, both for security awareness (regarding the vulnerabilities of the health information) which is applicable to everyone, and for the specific policies, procedures, and standards applicable to each individual’s job functions, including training in password management and virus protection. These security training requirements should become part of your overall compliance training curriculum. They may be combined with other topics in a particular training session or addressed separately.

Training should be provided to all new employees, and to all employees at least annually. As part of the initial training, the code of conduct and security policy should be distributed. Your compliance program should set a minimum number of hours of annual training for each employee. Generally, this should be at least one hour. (Mandatory corporate integrity agreements imposed by the OIG typically require a one- to three-hour minimum.) More time will be necessary for some groups of individuals. For example, as
technology or your operations change, employees responsible for receiving or transmitting electronic data may need additional security training. Similarly, training regarding changes in billing and coding procedures and regulations should be provided to appropriate staff at least annually. Periodic mini-training sessions and other reminders about information security and other compliance issues are also advisable. These can be as simple as posters, screen-savers, or spending a few minutes highlighting a compliance or security issue during regularly scheduled staff meetings.

Training should include information on sanctions for violating the organization’s policies and procedures, and the means of reporting suspected non-compliance. Some employees may feel threatened or troubled by this information, and morale and effectiveness may suffer as a result. Therefore, it is important to present this material in the proper context—that is, by recognizing and reinforcing what you believe to be the honest and ethical nature of healthcare employees. All training should be coordinated with your human resources department.

Following initial and annual training, all participants should sign an agreement that indicates their awareness of and willingness to abide by the organization’s code of conduct, security code, and all related policies and procedures. This agreement should identify actions that violate policies and penalties for noncompliance. For agents and independent contractors, attendance at training sessions could be part of their contractual obligations. These signed agreements should be kept on file. Finally, all training should be documented and each individual’s attendance recorded. If your organization should have to react to a legal compliance or security incident, documented training will provide evidence of your prevention efforts.

**Develop Effective Lines of Communication.** Effective compliance programs must establish and communicate to employees their right and obligation to report suspected violations of the law. Employees should be provided with an anonymous reporting mechanism through which they can voice compliance concerns, without fear of retaliation. Hotlines are such a mechanism endorsed by OIG; however, this specific method is not required, and a simple drop box for written complaints may be sufficient for some organizations. You should keep records of these reports and their resolution. The compliance officer should work closely with legal counsel in addressing reported problems.

The security standards require formal, documented instructions for reporting security breaches and other inappropriate use of the computer system to management, to assure these matters are handled promptly. Unlike the compliance program guidance, which specifically recommends a mechanism for anonymous reporting, the security standards do not address the reporting method. Nevertheless, to leverage your efforts, security incidents may be reported using the same mechanism you have developed for reporting other types of compliance issues. As with problems reported under the compliance program, you should keep a record of reported security problems and their
resolution. Depending on the nature of the reported security problem, it may be appropriate to involve legal counsel.

**Conduct Appropriate Internal Monitoring and Auditing.** An effective compliance program must include an ongoing monitoring and auditing system reasonably designed to detect inappropriate conduct. Monitoring and auditing can detect and correct inappropriate conduct before serious problems arise. Audits and monitoring should focus on the risk areas identified for your organization. Your selection of audit targets should also be guided by specific problems that have arisen in the past. These same principles apply to auditing under the security standards. In addition, the security standard specifically requires an in-house review of the records of system activity (such as logins, file accesses, uses of “override” capabilities, and security incidents).

Compliance audits should be conducted on a random, periodic basis, using a process designed to uncover both intentional and unintentional instances of noncompliance. They should be frequent enough to catch patterns of activity. Educate employees about your compliance auditing and monitoring process, to encourage staff to ask questions when in doubt and to help deter unwanted conduct. With regard to security, simply tracking all system activity may not be effective; you may need tools to identify improper access to information and to analyze patterns of system activity. As with compliance auditing, publicize the fact that all access to records will be documented; this will help you deter unauthorized users and improper use.

Your compliance auditing system may include having legal counsel review certain types of transactions which could raise compliance issues under the anti-kickback or Stark law. Your security auditing may include a review of your organization’s sharing of health information with business partners. You may want to have legal counsel prepare the necessary “chain of trust” agreements with those business partners. Whether under the compliance program or security standard, any audits that become necessary in the context of potential civil or criminal liability should be conducted under the direction of legal counsel. This improves the organization’s chances of protecting the privileged nature of the investigation, should it conclude that it should rely on such protection.

**Enforce Standards through Clear Disciplinary Guidelines.** If an organization cannot demonstrate that it consistently and appropriately disciplines individuals for compliance violations, the effectiveness of the program may be called into question. The OIG believes a compliance program should set forth a progressive disciplinary policy for failing to comply with the organization’s standards and policies and applicable statutes and regulations. Sanctions could range from oral warnings to suspension, termination, loss of clinical privileges, or financial penalties, as appropriate. Compliance policies must be consistently enforced, including, as appropriate, discipline of supervisors or managers for negligent failure to detect or correct an offense. Knowledge of and adherence to confidentiality and security policies, and other
compliance issues, should be a factor in employee evaluations. By linking performance reviews to compliance, employees will have an ongoing incentive to adhere to the organization's policies, thereby helping to reduce the risks to the organization.

The security standard also calls for disciplinary policies and procedures that are to be communicated to all employees, agents, and contractors. As noted above, these sanctions could include progressive disciplinary policies, up to and including termination of employment or contract termination. Those affected must also be advised of the potential civil and criminal penalties for misuse or misappropriation of health information, and that such actions may be reported to law enforcement, regulatory, accreditation, and licensure organizations.

Information as to the disciplinary policies of the organization should be included in the employee manual, made a part of training, or otherwise clearly communicated to all employees. This information should the potential for reporting noncompliance to outside agencies, as appropriate. Also include sanctions related to the security policy and any other compliance policies. For agents and contractors, sanctions for failure to comply with the organization's policies and federal and state laws and regulations should be part of the contract for services.

A corporate compliance program should also include appropriate background checks for new employees who have discretionary authority to make decisions that may involve compliance with the law. A reasonable and prudent background investigation, including a reference check, should be part of every such employment application. Your compliance program should also include protocols for handling the information collected. The security standard also requires appropriate personnel clearance procedures for those individuals with access to health information. Under the security standard, this requirement may be satisfied in a small organization by standard personal and professional reference checks. In a large organization, more formal, rigorous background investigations may be more appropriate.

Respond Promptly to Detected Offenses and Take Corrective Action. Despite your implementation of an effective compliance program, inappropriate conduct still may occur. When a problem is reported, it must be promptly investigated, and appropriate corrective and additional preventive actions are required. An effective compliance program must include defined processes for conducting compliance investigations and for ensuring and documenting that appropriate corrective action is taken. Part of your response to a compliance issue must be to demonstrate that steps are being taken to prevent recurrences of the same or similar problems. If your organization fails to respond to the complaint, the employee has the option of reporting the problem to the government or filing a qui tam action. An effective reporting process is more likely to keep complaints within the organization, because employees will trust the organization's resolution of the problem.
Under the security standard, you will be required to implement security incident procedures, along the same lines as the compliance incident procedures described above. These are formal, documented instructions for reporting security breaches, and procedures for responding promptly and appropriately to such reports. The response procedures should include implementing corrective measures to deal with compromised data.

Conclusion

While legal compliance programs are voluntary, HIPAA compliance will not be. Although there is a technical component to the requirements under the security standard, the majority of the requirements relate to policies, processes, and procedures. As a result, the security standard should fit easily within the compliance framework you have created. If you have not yet begun to develop a compliance program, the HIPAA security standard will provide additional incentive to do so now. To comply with the security standard, you will have to develop a risk analysis team and a risk management strategy. Once you have mastered this process and created the organizational framework for this function, you can move on from security to other compliance risk areas. Similarly, once you have established formal, documented procedures for the security standard, developed and scheduled a regular training program, and designed reporting and incident response mechanisms, these can be extended to other risk areas. The work that you put into meeting the HIPAA regulations can thereby be leveraged into more efficiently establishing a fully developed, effective compliance program for your organization.

References

   http://www.access.gpo.gov/su_docs/aces/aces140.html.
2. Department of Health and Human Services, Office of the Inspector General, Compliance Program Guidance,
6. Federal Register, 64, 599918–60064 (3 November 1999).

About the Author

Patricia I. Carter, JD, is a health law attorney at Gray, Plant, Mooty in Minneapolis, Minnesota, with a prior fourteen-year career in health insurance, including eight years as an information systems manager.