Integrating Privacy and Security: Coordination Benefits HIPAA Compliance Efforts

by M. Peter Adler, JD, LLM, CISSP, CIPP

Privacy and security are meant to work in tandem—so why have they grown up apart? An organization that coordinates its compliance efforts can maximize resources and increase effectiveness.

Several years have passed since the compliance deadlines for the HIPAA privacy and security regulations, yet compliance has been elusive for many healthcare providers. By summer 2006, only 39 percent of respondents to an AHIMA survey reported that their facilities were in full compliance with the HIPAA privacy regulations.[1] In fact, there is some indication that the level of compliance is slipping. In the same survey, 85 percent of respondents believed that they were more than 85 percent compliant with the privacy standards, a drop from 91 percent of respondents the previous year.[2]

There are a number of reasons why compliance has been difficult to achieve and maintain, but the most cited reason is a lack of resources.[3] In many organizations there is a problem that diminishes those resources: privacy and security compliance efforts are handled separately, lowering the efficient use of resources.

Privacy and security regulations were intended to work together to effectively protect health information. In most covered entities, that hasn't happened due to a number of historical and organizational reasons. But organizations that can integrate their security and privacy compliance efforts make the most of their resources and boost the effectiveness of their programs. In some instances, this may mean a reorganization of security and privacy roles and reporting structures. In others, it may start with the revitalization of a flagging HIPAA committee.

A Close Relationship, Mutual Dependence

Information security keeps unauthorized persons or systems from gaining access to restricted information. Privacy is the collection of rules and obligations that determine how and when access is to be authorized, in any medium. It follows that good security and privacy practices depend on one another.

Privacy of electronic information would simply not be possible without technology safeguards. Rules and obligations to protect health information cannot be enforced without effective access controls. In the same way, security would not be effective without privacy. It is impossible to ensure that safeguards are implemented appropriately without knowing the rights and obligations defining appropriate access. The growth of health IT will continue to drive a convergence of privacy and security roles and responsibilities.

The failure to have a unified program can clearly impact daily operations. An incident response program that does not involve both security and privacy teams, for example, will lead to disastrous results should a breach occur. The technical security specialist within the organization must identify the breach and notify privacy personnel, who are required to mitigate the breach, and in some states, notify each individual whose information may have been disclosed.

Even fundamental compliance tasks such as compliance monitoring and risk assessment require participation from both security and privacy personnel. These efforts are often thwarted when the two teams fail to jointly set the compliance agenda. The lack of a coordinated approach undermines efforts to obtain the resources to monitor compliance, conduct periodical re-evaluations, and modify the security and privacy compliance program.

The close relationship between privacy and security is identified in the HIPAA regulations. HIPAA defines the term "security or security measures" to "encompass all of the administrative, physical and technical safeguards in an information system."[4]

Each of these terms are defined and given extensive treatment in the regulations on protecting "electronic protected health information" (ePHI):

- **Administrative safeguards** are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's work force in relation to the protection of that information.[5]
- **Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.[6]
- **Technical safeguards** refer to the technology and the policy and procedures for its use that protect ePHI and control access to it.[7]HIPAA does not provide a similar definition for the term "privacy." However, the overall purpose and goals of the HIPAA privacy regulations are to set forth the rights and obligations of individuals and covered entities with respect to the uses—the collection, processing, and retention—and disclosures of protected health information (PHI) in any format.

The privacy provisions also provide that a "covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[8] The safeguards are to protect against intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements included in the privacy regulations.[9]In this way, even though the security regulations are limited to ePHI, the privacy regulations call for security measures for protecting PHI, regardless of its form.

The relationship between security and privacy is exemplified by the development of electronic health records and other emerging technologies. Security experts must work closely with privacy professionals to make certain that new technologies ensure the availability of ePHI to healthcare providers but only when authorized and in a manner that protects the confidentiality and integrity of information.

The Barriers to Coordination

A number of healthcare providers report that their security and privacy departments function well, yet many operate in a semi-autonomous manner, fighting over available resources. Several general factors have led to barriers in coordinating privacy and security compliance activities.

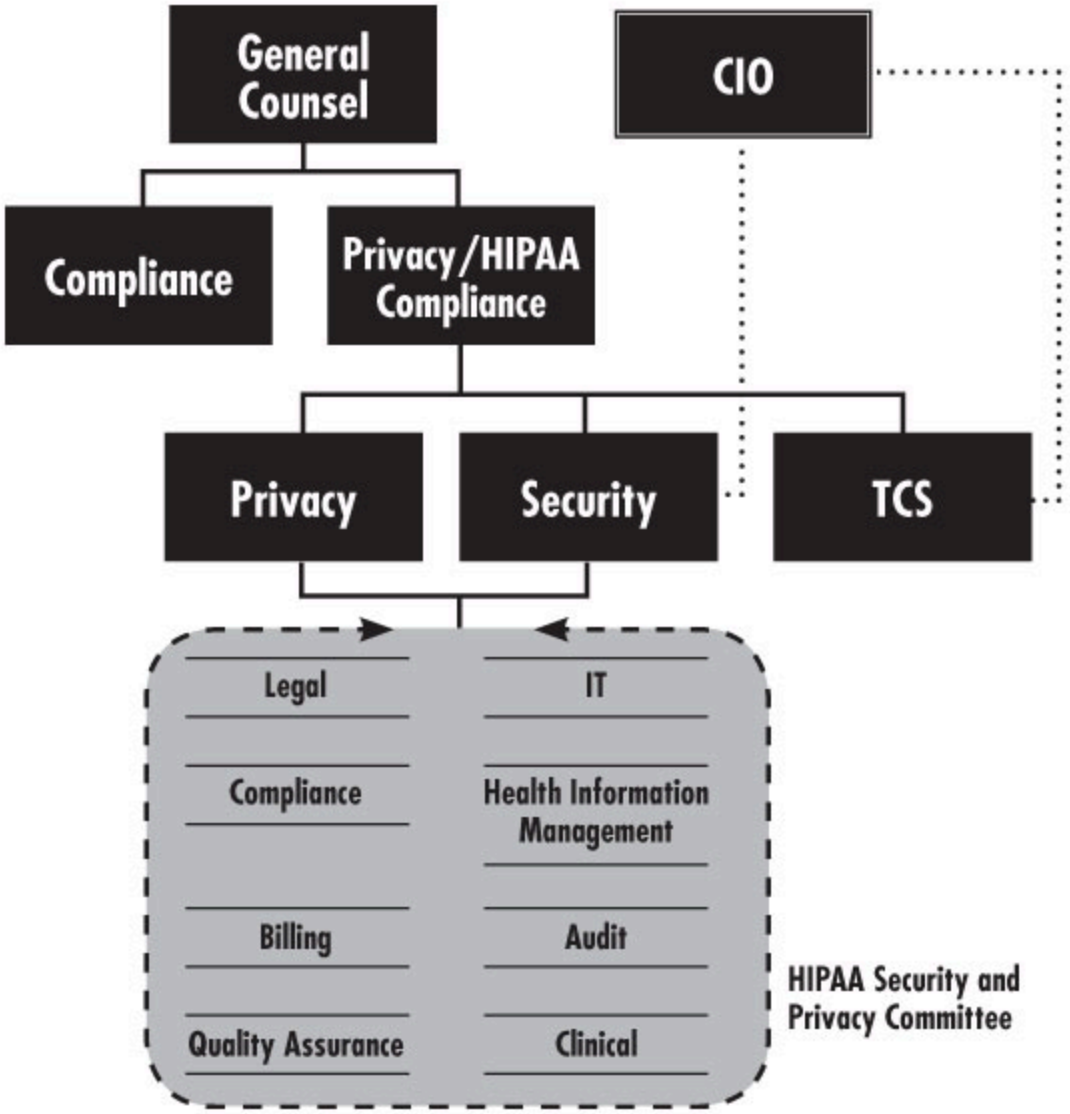
Staggered Release of the HIPAA Regulations

Traditionally, healthcare entities handled privacy and confidentiality separately from security. Often the medical records department had the responsibility to protect the confidentiality of the information contained in health records. As paper-based billing became automated, the IT department both managed and secured the electronic billing systems. From the beginning, and as electronic systems evolved, little coordination occurred between the two departments.

Nor was the need to coordinate security and privacy roles and responsibilities immediately apparent when HIPAA was rolled out. The need was further obscured when the notice of proposed rule making for the security regulations was released more than one year before the notice for the privacy regulations. Gaps between the releases continued through the publication of the final rules, and the compliance deadlines were separated by more than two years.

The security notice was released first, and some healthcare organizations conducted security risk assessments based on the notice. However, most organizations waited until the near-final or final privacy regulations were released before they began to assess their compliance needs. This caused the majority of covered entities to focus on their readiness to comply with the privacy regulations—whose deadline came first—before they looked deeply at the security compliance requirements.

Combining Security and Privacy Compliance Efforts



Organizations can consolidate resources and boost effectiveness by combining privacy and security roles and responsibilities. There are many methods, ranging from a complete reorganization of HIPAA compliance roles to reinvigorating and realigning HIPAA committees or task forces. No single solution will work for all organizations; however, the above illustration is one example.

The foregoing organization combines the privacy and security roles under the privacy and HIPAA compliance office with a person responsible for security, privacy, and transaction and code sets (TCS). A dotted line report is created between security and TCS to the CIO. This ensures that technical support for compliance is provided while separating the delivery of IT from the need to comply with the HIPAA regulations.

The HIPAA security and privacy committee advises the HIPAA compliance office on specific operational needs while working toward consensus on how new technologies can be integrated while complying with HIPAA.

Separate Implementation Efforts

The first efforts to comply with HIPAA faced a daunting challenge, and those with privacy and security responsibility sought participation and advice from other departments within their organizations. This often took the form of a HIPAA committee or task force comprised of individuals who had a stake in one or more areas affected by the rules.

However, many of the HIPAA security and privacy committees operated partially or completely independently of one another. A typical HIPAA privacy committee was led by a member of the compliance or medical records department and included representatives from a wide range of departments including legal, compliance, medical records management, billing, audit, quality assurance, and clinical. The HIPAA security committee was often led by the IT department and included members from many of the same departments, but who also worked with technology.

Communication between the two committees was often compromised when they were staffed by different people from the same departments.

Uneven Administrative Support

Dividing resources between privacy and security compliance has generally provided uneven results. For example, all respondents to the 2006 AHIMA survey reported that their facility had a designated security officer; only 88 percent reported having a privacy officer.[10] More importantly, perhaps, only 27 percent of privacy officers were full-time, compared to 65 percent of the security officers. The higher number of security officers was one reason more healthcare organizations claim full compliance with the security rule (56 percent) than with the privacy rule (39 percent). The discrepancy has occurred even though covered entities had an additional year to prepare for privacy compliance.

Generally speaking, when there is a strong CIO within the covered entity the information security requirements are often given priority. Privacy often takes the front seat when there are strong health record, legal, and compliance departments.

Usually the losers in this tug-and-pull cite the lack of administrative support as the main reason they have difficulty in corralling necessary resources. Respondents to the AHIMA survey complained about a lack of staff and time to focus on key privacy activities such as compliance monitoring and conducting risk assessments.[11] The survey reported:

> Administrative support goes hand in hand with [the lack of resources]. Without significant support, privacy officers or committees have difficulties securing budget or resources to achieve full compliance. Administrative support either from executives or clinical leadership is also directly tied to the attitude employees take toward promoting and incorporating privacy practices in their daily functions. Without this support, reports of slippage in daily practices may grow more prevalent.[12]

Given that support and resources are so closely connected, an organization's best approach is to consolidate and enhance available resources by focusing on a limited number of key security and privacy compliance areas.

Opportunities for Consolidating Resources

Covered entities must take a fresh approach to addressing the lack of resources and the failure to fully attain HIPAA compliance. While every covered entity has its own unique set of circumstances, the following suggestions illustrate how organizations can use resources more effectively to enhance their HIPAA compliance programs.

Revitalize Management's Commitment

HIPAA security and privacy compliance programs languish because many at the leadership level believe that HIPAA compliance has been achieved and minimal resources will be required for future compliance efforts. As a result, once-robust programs have atrophied and are no longer in compliance. Other programs that were not quite complete at the deadline lost momentum and have never reached their goals.[13]

To revitalize compliance efforts, those responsible for HIPAA compliance can identify one to three manageable goals to improve the HIPAA compliance program ("compliance targets") and communicate them to upper management to obtain their support. Each compliance target should include methods to enhance compliance efforts while reducing overall resources required.

Combine Compliance Efforts

Resources can be consolidated by identifying ways to combine HIPAA privacy and security roles and responsibilities within the organization. The historical reasons for establishing separate security and privacy efforts have long passed, and new technologies require a closely collaborative approach to ensure that ePHI is protected, used, and disclosed in accordance with the entity's privacy practices.

There are many methods for combining compliance efforts, ranging from a complete reorganization of privacy and security roles to reinvigorating and realigning HIPAA committees or task forces.

Traditionally, covered entities have used HIPAA committees or task forces as the primary method used to obtain advice from a wide range of departments within the organization. That practice appears to have diminished in recent years. The use of task forces or committees dropped to 64 percent in 2006, down from a high of 89 percent in 2004, according to respondents in the AHIMA survey.[14] Similarly, the use of security task forces fell from a high of 85 percent in 2004 to 59 percent in 2006. This may be because their initial compliance mandate has ended.

Nevertheless, task forces and committees provide an efficient use of resources for complying with the HIPAA rules. Rather than let them die out, healthcare facilities can reassemble one committee to address both security and privacy compliance. Their effectiveness will be enhanced if they are used in a focused manner to address the entity's compliance targets.

No single solution will work for all healthcare organizations. The figure opposite offers one example of how it might be done.

Drastic changes in organizational structure may not be necessary. Any effort by a covered entity to integrate the security and privacy roles and responsibilities will help conserve resources, comply with HIPAA, and better position the organization to respond to upcoming changes in technology and laws pertaining to electronic health information.

Reintroduce Compliance Efforts

The covered entity's announcement of the new HIPAA compliance team will help reintroduce and re-energize the HIPAA compliance efforts. The annual compliance targets that have been agreed to by upper management should become a stated mandate for the HIPAA security and privacy committee.

The combined HIPAA compliance committee can meet regularly to assist the privacy and security personnel attain their current compliance targets. In that way, the HIPAA compliance office will be afforded resources from key personnel from healthcare operations, including those responsible for treatment.

Revitalize Education and Awareness

Privacy and security education and awareness training should be made part of the revitalized HIPAA compliance effort. Training need not become a grueling process if it is kept focused. It can be accomplished through general training sessions augmented by information on the covered entity's selected compliance targets. While efforts to provide general privacy and security training continue, the organization can add training focused on specific compliance targets as each initiative is accomplished.

Notes

1. AHIMA. "The State of HIPAA Privacy and Security Compliance." 2006.
2. Ibid.
3. Ibid.
4. HIPAA, Public Law 104-191, 45 CFR §164.304.
5. HIPAA 45 CFR §164.304. See also 45 CFR §164.308 for the administrative safeguards required by the HIPAA security regulations.
6. Id. See also 45 CFR §164.310 for the physical safeguards required by the HIPAA security regulations
7. Id. See also 45 CFR §164.312 for the technical safeguards required by the HIPAA security regulations
8. HIPAA, 45 CFR §164.530(c)(1).
9. HIPAA, 45 CFR §164.530(c)(2)(i).
10. AHIMA. "The State of HIPAA Privacy and Security Compliance."

11. Ibid.
12. Ibid.
13. Ibid.
14. Ibid.

M. Peter Adler *(adler@adleripg.com) is president of InfoCounsel, LLC, in Alexandria, VA.*

Article citation:
Adler, M. Peter. "Integrating Privacy and Security: Coordination Benefits HIPAA Compliance Efforts" *Journal of AHIMA* 79, no.4 (April 2008): 34-38.