



Managing Information Security in Healthcare

What Healthcare Executives Should Know and Do About Information Security

By Jeff Collmann, PhD and Stephen Grimes, FACCE, SHIMSS

From the perspective of an organization's executive leaders, all opportunities for gain necessarily risk loss. Even successful projects as judged with reference to their stated objectives require foregoing the pursuit of other opportunities for gain as well as incurring real costs. For example, when healthcare executives consider deploying information technology to support clinical, personnel, inventory, or financial functions, they incur risks for the organization even as they potentially enhance its strategic capabilities. A successful IT deployment may postpone investment in clinical equipment, force business process reforms, eliminate jobs, and subject the healthcare organization to novel regulatory requirements. Beneficiaries of the successful deployment may herald its achievement while those who perceive they have been adversely affected may denounce its implementation. Many will resist changes in their work patterns that the new technology inaugurates. Launching any new project requires managing the consequences of these threatening conditions for everyone in the organization. Organizational leaders thus function as risk managers in the course of every day business because they must choose among diverse opportunities for gain, loss, cooperation and conflict.

The role of organizational leaders as risk managers also establishes the proper context for interpreting the benefits and costs of compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996's privacy and security regulations. HIPAA's federally mandated regulatory standards are designed to limit the risks of loss due to breaches of privacy and security and, thereby, help create a safer environment for investments in advanced health information technology. HIPAA provides strategic benefits even as it incurs operational costs, particularly in an industry with little experience with the perils of networked computing infrastructures.

Compliance with HIPAA helps protect healthcare organizations from a range of adverse consequences, including:

- **Damaging the reputation of an organization and its leaders:**

Officers in the military health system refer to the "*Washington Post* test." Situations that could potentially generate a critical story on the front page of the *Washington Post* newspaper warrant close scrutiny. Significant breaches of privacy or security by a military treatment facility fail the *Washington Post* test as

would major HIPAA breaches. Disclosure of such mistakes could lead to reassignment and jeopardize careers.

- **Compromising patient care (e.g., misdiagnosis, delays in treatment, patient injury or death):**

Avoiding medical errors represents a major challenge for healthcare organizations as evidenced by the Institute of Medicine's report *To Err is Human* (IOM 2000). Unauthorized and incorrect changes to a patient's medical record or data in medical equipment (breaches of integrity) yield medical errors with potentially disastrous consequences for health or life. The IOM also emphasizes the role of unavailable information in producing medical errors.

- **Re-assigning staff to damage repair and control:**

Managing a major breach of confidentiality, integrity or availability requires diverting staff at all levels of a healthcare organization from their normal routines to crisis management activities for what can be extended time periods. In addition to forensic activities, staff must repair or recover the relevant information assets, take measures to prevent further compromises, and implement a public relations campaign with apologies to patients, consulting physicians, or partners as well as explanations to the press. If a patient sustains injury as a result of the breach, providers must attend to the patient's complications as well as be prepared for any possible litigation.

- **Incurring financial penalties or costs:**

Although HIPAA does not explicitly grant an individual the right to sue for breaches of privacy or security, affected individuals may potentially sue on other grounds, including but not limited to injury. HIPAA does provide for criminal and civil penalties in the event of significant privacy or security breaches, particularly after extended warnings from the US Department of Health and Human Services.

- **Undermining the organization's mission:**

Depending on its scope and management, a privacy or security breach may disrupt a healthcare provider's ability to deliver care. An organization may delay or terminate programs that depend on secure information management, such as an online patient support service, in the event of a breach.

- **Sustaining multiple, interacting harms:**

A major breach of privacy or security rarely entails only one type of damage. If a breach of data integrity causes harm to a patient, the healthcare organization will probably suffer damage to its reputation; spend much time and resources on clinical and administrative crisis management; pay penalties or settlements, court costs and legal fees; retrain, discipline or terminate employees; and restructure programs.

Key Steps to Take

What steps should healthcare executives take to integrate information privacy and security processes into their organization's risk management activities?

- **Aggressively and visibly sponsor information privacy and security campaigns:**

HIPAA offers healthcare executives the opportunity to demonstrate strong and unambiguous support for the value of protecting patient privacy and security. In addition to leading the mobilization of HIPAA compliance efforts, healthcare executives should remain engaged to sustain and transform HIPAA activities as standard operating procedures after the compliance dates. The chief executive officer should become

the privacy and security “poster child” to demonstrate to everyone in the organization the importance of effective privacy and security management.

- **Appoint influential, effective leaders from the organization’s staff and physicians to plan, implement, and sustain the privacy and security campaign:**

Commonly known as “champions,” staff and physician leaders carry the message to their colleagues as well as execute the work. Choosing low ranking or ineffective staff to organize the HIPAA campaign communicates its insignificance and hobbles the work effort. These people should represent the range of major organizational constituencies, including different disciplines and levels of the hierarchy. The organizational leadership should recognize work on privacy and security as an assigned component of regular job responsibilities, not an “extra duty as required.”

- **Educate and train the privacy and security team:**

Although all staff and consulting physicians will bring essential knowledge of the organization’s clinical and administrative processes to their information security work, the privacy and security team members will need training in specific topics such as the HIPAA regulations, good information security practices, and information security risk assessment. The organization should fund the training from its central budget and provide local relief for missing staff.

- **Hold privacy and security team members accountable for their work:**

The HIPAA regulations established compliance deadlines for all covered entities. Although skepticism exists in the healthcare community about the sanction process, organizational leadership should aggressively work maintenance of HIPAA into routine, long-term performance expectations. The annual evaluations of all staff should include performance on individual privacy and security requirements such as training. Reporting on maintenance of HIPAA compliance should also become a means for incorporating privacy and security issues into administrative accountability processes, including regular reports to senior leadership and the board of directors. The organization’s board should specifically hold the chief executive officer accountable for success in the privacy and security program.

- **Provide adequate resources for privacy and security initiatives:**

Privacy and security initiatives must compete for resources with other organizational priorities, many of which potentially yield tangible benefits such as increased clinical productivity. Healthcare executives should evaluate investment in privacy and security like any other strategic initiative, however, as necessary for establishing the organization’s long-term success and avoiding short-term harm such as compliance penalties. Supporting the time and effort of the privacy and security program members will require special attention because of their loss to clinical and administrative operations.

Activities

What specific activities should healthcare executives sponsor in their organizations in the domain of information security risk management? Because the HIPAA Security Rule grounds its compliance approach in ongoing information security risk management, its requirements represent a set of baseline controls for planning, implementing, and evaluating an organization’s information security program, particularly its emphasis on administrative, physical, and technical controls. HIPAA’s focus on protected health information limits its scope to a single if nonetheless critical asset. In mobilizing for HIPAA, the organization should establish the basic framework to comprehensively address its total information security needs. HIPAA

requires several key risk management activities that can help accomplish broader organizational risk management aims, including:

- **Establish a security management program:** HIPAA clearly intends for healthcare organizations to incorporate information security management into their routine administrative processes. By including administrative, physical, and technical controls, HIPAA articulates a vision of health information security as an enterprise responsibility—not just a technical operation. Appointing and empowering privacy and security “champions” initiates this process.
- **Conduct a comprehensive information security risk assessment:** HIPAA lists risk assessment first among its implementation specifications suggesting its relative importance. No healthcare organization can make any progress in information security without identifying and mitigating threats to protected health information as well as vulnerabilities in organizational security policies, procedures, and practices. The privacy and security team should tackle this as the first step in building its program using a comprehensive method that meets the NIST guidelines such as OCTAVESM.
- **Sponsor an information security risk management process:** As the privacy and security team conducts its risk assessment, it will identify specific strengths and weaknesses in the existing health information security program. In order to overcome weaknesses and sustain strengths, the team must design, implement, and evaluate a health information security risk management plan. Initially, HIPAA requires that a healthcare organization focus its risk management plan on protecting patient health information and related assets. Given its core importance in the healthcare mission, instituting administrative, physical, and technical controls to protect health information will inevitably enhance protection of other information assets. For example, privacy training for all hospital staff instills a general awareness about the need to protect the confidentiality of all types of sensitive information in addition to patient information. A technical as well as physical perimeter defense helps protect financial and clinical information. As the program achieves its initial goals of compliance with HIPAA, however, it should explicitly address the specific security requirements of other types of information and their related information assets. Breaches of the confidentiality, integrity, or availability of personnel, financial, or operational performance information jeopardize a healthcare organization’s mission in different but highly significant ways. Information security risk management begins—not ends—with protecting patient health information.

Conclusion

HIPAA offers healthcare executives an opportunity to incorporate information security into their portfolio of risk management strategies. Although an imposed regulatory activity, HIPAA compliance potentially protects investments in information technology by aligning a healthcare organization’s policies, procedures, and practices with an identifiable standard of practice. Building the information security risk management team also strengthens the organization by institutionalizing privacy and security processes and providing a mechanism for dispute mediation among stakeholders in a contentious, potentially divisive issue. Thus HIPAA’s Privacy and Security Rule requirements, while entailing operational costs, build an organizational information security program that yields major strategic benefits.

Appendix 1

Guidance

How should healthcare executives envision the specific risks of information privacy and security? HIPAA focuses on protecting the privacy and security of individually identifiable patient health information.

Nonetheless, healthcare organizations manage many other types of sensitive, mission-critical information that require protection, including personnel, financial, credentialing, clinical research, de-identified, and proprietary business information. Healthcare organizations must also manage other types of information assets such as their information acquisition, archiving, and distribution systems as well as biomedical and information technology support personnel. A comprehensive information security management program entails protecting all these types of information and information assets from harm. Several organizations produce guidelines, tools, and processes to assist healthcare organizations in understanding and accomplishing this task, including:

- **Healthcare Information and Management Systems Society (HIMSS):**

HIMSS has aggressively developed many resources to assist healthcare executives in understanding health information privacy and security. The Privacy and Security Steering Committee meets monthly to sponsor and execute specific initiatives, including support for the security requirements of the National Health Information Infrastructure (NHII). The Steering Committee also establishes individual taskforces to address issues of special concern such as the Medical Device Security Taskforce. HIMSS makes *The CPRI Toolkit: Managing Information Privacy and Security in Healthcare*, a primary reference tool for managing healthcare information security, and many other privacy and security resources available at no charge on its Web site (<http://www.himss.org>).

- **American Health Information Management Association (AHIMA):**

AHIMA has a wide range of resources on privacy and security available on their Web site at www.ahima.org. Their Professional Development section provides ongoing meetings, seminars, and teleconferences on current privacy and security topics. Archived versions of teleconferences are available on CD or download on the Internet. AHIMA's Bookstore has a variety of books on privacy and security as well as health information technology (HIT) and the electronic health record (EHR). Their Practice Brief series provides industry best practices on topics ranging from Basic HIPAA Security Overview, Securing Wireless Technology in Healthcare, to discussing the comparison of the Homeland Security Act, the Patriot Act, and HIPAA. Their resources are written mostly for the user side of the computer screen and frequently present technical concepts in language understandable to the technically challenged. Many resources are free to download.

- **National Institute of Standards and Technology (NIST) Publications:**

In the course of developing computer security guidelines and standards for agencies of the Federal government, NIST has produced a wealth of information from which commercial healthcare organizations can draw important lessons, including its recent publication on HIPAA security (see attached executive summary) and guidelines for an adequate information security risk assessment (see attached executive summary). NIST publications are available for download at no charge on its computer security Web site (<http://csrc.nist.gov>). For a list of known vulnerabilities in software and operating systems, see <http://icat.nist.gov>.

- **CERT Coordination Center (CERT/CC) at the Software Engineering Institute (SEI), Carnegie Mellon University:**

CERT/CC is a center of Internet security expertise focused on improving the state of Internet security. Healthcare executives will best know CERT/CC through its forensic work on computer viruses. CERT/CC issues vulnerability alerts as well as public advisories about new viruses or other major threats to the Internet, including such important cases as the *Melissa* and *Lovebug* threats. CERT/CC publishes many booklets on critical topics in health information security aimed primarily at the commercial market. As a

Federally-funded Research and Development Center, SEI often receives funds for major computer security projects. Under such a project, the CERT/CC developed the Operationally Critical Threat, Asset and Vulnerability EvaluationSM (OCTAVE SM), a self-directed information security risk assessment method for use by hospitals and other organizations that do not necessarily command extensive information security expertise. For information, see <http://www.cert.org>.