Implementing HIPAA One Step at a Time

Save to myBoK

by Jim Bettendorf

Many in the healthcare industry are facing the difficulty of incorporating HIPAA into their organizations. As a newly appointed privacy officer for a healthcare clearinghouse, I, too, was presented with the challenge of assimilating HIPAA into our organization.

Always Ask Questions

Little printed information or "best practices" exists on HIPAA from a clearinghouse perspective. The real obstacle was determining what applied to our organization, especially under the privacy and security standards.

A valuable lesson I learned early in this process was to ask three questions on everything from selecting resources to implementing policies and procedures. The questions are:

- What is the return on investment?
- What is the scalability to the organization?
- What is the most reasonable approach?

Using these, I more effectively prioritized organizational needs and gave perspective to the steps required to reach the projected outcome.

A "Living" Process

I am incorporating HIPAA into our organization as a "living" process. The "living" documents become a blueprint for compliant behavior throughout the healthcare organization.[1]

Already familiar with a corporate integrity agreement, I realized the tool to implement our HIPAA compliance effort existed with the federal sentencing guidelines for a voluntary compliance program. Creating a compliance program would provide the framework for compliant behavior within and throughout the organization.

An effective, proactive compliance program:

- can identify areas of noncompliance or risk within the organization
- can reduce the risk of violating regulatory statutes within the organization by implementing internal controls
- may offer some protection by demonstrating a formal structure to identify and correct any misconduct
- should significantly reduce the risk of unlawful or improper conduct by all employees
- will help the organization uncover inefficiencies and possibly items or procedures that could be considered in violation of the privacy, and eventually the security, standards by the government

Acquiring HIPAA-specific knowledge is a continual process of obtaining information from a number of sources. To start, I completed a week-long course and earned a Certified Healthcare Compliance Officer (CHCO) designation, which set me on the correct path to build and implement an effective HIPAA compliance program. Other ways to gain helpful information include:

- reading the HIPAA statute itself (http://aspe.hhs.gov/admnsimp) and updates (www.aspe.hhs.gov/admnsimp/lsnotify.htm)
- following the efforts of groups named in the rules or active in the process such as the Workgroup for Electronic Data Interchange (www.wedi.org) and the Association for Electronic Health Care Transactions (www.afehct.org)

- networking with colleagues
- participation in regional efforts such as the Strategic National Implementation Process
- workshops and conferences
- e-mail list services
- HIPAA-specific articles
- subscriptions to HIPAA-focused periodicals

Constructing a HIPAA Compliance Program

Once I possessed the skill set to develop a compliance program and pertinent reference resources, I was ready to begin building our organization's HIPAA compliance program. Through the seven basic components of a voluntary compliance program provided by the federal sentencing guidelines, the protocol for moving the organization forward is established. These guidelines are:

- establish practice standards and procedures
- designate a compliance officer or contact(s)
- conduct appropriate training and education
- audit and monitor
- develop open lines of communication
- enforce disciplinary standards through well-publicized guidelines
- respond to detected offenses and develop corrective action initiatives

Using these guidelines, I established the HIPAA compliance standards the organization will follow to ensure a safe, law-abiding, ethical, and productive business.

A baseline audit was also conducted to identify areas with risk potential that have been identified by the HIPAA regulations. The audit was based on information outlined in the three HIPAA rules (transactions and code sets, privacy, and security). Security was included, even though the rule is not finalized, because many of the provisions are fundamental to our organization's HIPAA compliance program.

Continuous Evaluation

Continuous evaluation of the HIPAA compliance program will allow it to be effective. The extent and frequency of audits are determined by the size of the organization, the results of the baseline audit, the frequency of reports of suspected non-compliance, and the number or complexities of new or revised laws and regulations.

All areas of our organization are audited for compliance at least annually. Staff with the appropriate expertise in each of the specific audit areas will perform those audits. In addition to internal auditors, external auditors are used. Regardless, all auditors must be objective and possess knowledge of federal and state laws and regulations. Complete documentation of audit results is important, especially all attempts, either written or oral, that have been used to comply with the applicable standards.

Open communication between the privacy officer and those associated with the organization is continually stressed. It is helpful to maintain written confidentiality and non-retaliation policies to encourage communication. Methods that should be made available for individuals to ask questions, obtain clarification of policies and procedures, and to report all incidents of potential misconduct include:

- discussion at staff meetings
- community bulletin boards
- locked suggestion boxes

Handling Violations

Disciplinary action is also clearly defined, as is outlined action for inappropriate conduct or non-compliance with the organization's standards and policies and non-compliance with any applicable laws and regulations. Our HIPAA policies

include what constitutes non-compliance and indicate who is responsible for taking appropriate action. Levels of HIPAA non-compliance outlined in our organization are stated clearly:

- intentional or reckless disregard for policies and regulations
- failure to detect a violation
- failure to report a violation

All allegations or suspicions of HIPAA non-compliance must be investigated and documented completely. If a violation occurs, the privacy officer must develop or coordinate a corrective action plan that includes:

- a description of the discrepancy
- a description of the specific remedy that was instituted
- any disciplinary actions that resulted from the violation
- copies of any reports generated to any applicable government or business associate
- timeline for solutions to be implemented, including any amendments and/or additions to the compliance program resulting from the violation
- training or re-training of all affected personnel
- regular monitoring of the progress and/or effectiveness of any correction action that has been instituted

By constructing HIPAA compliance as a living process within our organization, it is our intention that it becomes a part of our day-to-day operations. Through the use of tools available in the healthcare industry and the proliferation of resources, I am able to generate and implement the policies and procedures that are necessary to achieve my stated goal—HIPAA compliance.

Notes

1. “Healthcare Compliance Resources,” LLC Medical Office Compliance Program Guide, June 2001.

Jim Bettendorf *(jbettendorf@gatewayedi.com) is the director of compliance and business development for Gateway EDI, Inc.*

Article citation:
Bettendorf, Jim. "Implementing HIPAA One Step at a Time." *Journal of AHIMA* 73, no.3 (2002): 59-61.