Finding Quality HIPAA Security Resources (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, CHPS, FHIM

Many of us struggled to understand the HIPAA privacy rule and initially had few resources to turn to for help. As your organization begins planning for security rule compliance, however, many of you may be finding that you're overwhelmed with the volume of potential resources available.

Virtually every vendor that sells anything related to information security is attempting to sell products or provide giveaways that can help your organization comply with HIPAA security requirements. While many vendors offer valuable information and certainly many good products, it may be helpful to cast your net a bit wider when looking for security resources. This article offers suggestions on how to find quality resources to help your organization prepare for security rule compliance.

Sorting through Freebies

There are many free resources available on the Web, at trade shows, in trade journals, or presented as advertisements in the mail. Do not discard these resources, as many of them can be valuable. You just need to know how they can be of value to you.

Web Resources

If you want to understand a security concept, the Internet can be an excellent source of information. But be careful—you will need to filter your surfing. Look for "white papers," "models," or actual documents in the descriptions of resources. Also look at the source—generally if a resource is from a university, professional or trade association, or from a covered entity directly, it can be reliable. However, be sure to review the document's date—you'll be surprised how many documents are several years old.

You will want to review several documents on the same topic, as you will also be surprised at the variability of interpretations, even from reputable sources. Vendors will also offer white papers, and many can be enlightening, but you may have to register with the site to view the document (which means you may get a marketing e-mail or call from the vendor). When you review white papers you will also need to mentally filter out what is related to the vendor's product versus what is just generic information. You may be tempted by various freeware or shareware, but you should never download anything that is executable without checking with your organization's IT department first.

Professional and Trade Association Offerings

Though you may obtain free material from professional and trade associations on the Web, these resources are somewhat different than those obtained through idle Internet surfing. Typically, these sponsors can provide best practices by benchmarking their members or subscribers, offering product comparisons, and providing an interpretation of security concepts applicable to their target audience.

To find associations and publications applicable to security, search the Web using the HIPAA security standards as key words. For example, if you look for "disaster recovery" you will find *Disaster Recovery Journal*, a quarterly publication for contingency planners. Several association Web sites include excellent glossaries and references to textbooks.

To Spend or Not to Spend

Not surprisingly, there are plenty of sources that come at a cost. Some of the Web sites you visit sell policy and procedure templates, document generators, and other products. Unless you have exhausted all other resources, however, you may want to hold off on spending.

Some security resources are standards or guidelines from standards development organizations for which a small fee is charged. As long as the organization is reputable, preferably accredited by the American National Standards Institute (ANSI), you may want to consider paying for these resources, as they typically go to support the work of the organization.

Help from the Government

NIST Resources

The National Institute of Standards and Technology (NIST) is part of the US Department of Commerce. It is responsible for developing standards and guidelines in support of government computing systems. Its security documents are many, varied, and generally easy to read. In addition to their narrative content, these documents include illustrations, glossaries of terms, references to additional resources, and model documents.

Three NIST documents are specifically referenced in the preamble to the HIPAA security rule, so you should feel comfortable using NIST’s documents as resources. However, you should also be aware that the documents are written for government agencies, not HIPAA covered entities. You will need to adapt them to the healthcare environment in which you work.

Most of the NIST documents applicable to HIPAA security come from its Computer Security Resource Center Special Publications 800 series. To view a full list, visit http://csrc.nist.gov/publica tions/nistpubs. The following are some resources that may be especially helpful for your HIPAA compliance activities:

SP 800-64 “Security Considerations in the Information System Development Life Cycle” (October 2003) describes how to incorporate security into all phases of systems acquisition, through use to disposal.

SP 800-50 “Building an Information Technology Security Awareness and Training Program” (October 2003) is an excellent resource to help you comply with section 164.308(a)(5). Note that the earlier SP 800-16, “Information Technology Security Training Requirements” (April 1998), is referenced in the HIPAA security rule preamble. SP 800-50 complements and expands on the earlier work.

SP 800-34 “Contingency Planning Guide for Information Technology Systems” (June 2002) will help you understand disaster recovery and emergency mode operations plans for compliance with section 164.308(a)(7).

SP 800-33 “Underlying Technical Models for Information Technology Security” (December 2001) was referenced in the HIPAA security rule and is useful for understanding various technical controls, especially audit controls.

SP 800-30 “Risk Management Guide for Information Technology Systems” (January 2002) will help you conduct your risk analysis in compliance with section 164.308(a)(1).

SP 800-26 “Security Self-Assessment Guide for Information Technology” (November 2001) provides a tool to use in identifying vulnerabilities as part of your risk analysis.

SP 800-14 “Generally Accepted Principles and Practices for Securing Information Technology Systems” (September 1996) is a fairly old reference, but it is also referenced in the HIPAA security rule preamble and is considered a classic for understanding an overall framework for information security.

In addition to these references, the SP 800 series also provides standards and guidelines on specific technical topics such as wireless networks, telecommuting, e-mail, network security testing, firewalls, handling security patches, PKI, intrusion detection systems, and more.

CMS Resources

Although they are not referenced in HIPAA, the Centers for Medicare and Medicaid Services (CMS) provides a number of very useful documents on its IT Web page at http://cms.hhs.gov/it/ security/References/ps.asp. These documents are primarily policies for CMS's Automated Information Systems Security Program or for its business partners and contractors, but, with some adaptation, they are very relevant to HIPAA security. Because CMS is responsible for security rule enforcement, its interpretation of the security rule may be influenced by its own documents. Of particular interest are the following:

- "CMS Internet Security Policy"
- "CMS Threat Identification Resource"
- "CMS Information Security Risk Assessment Methodology"
- "CMS System Security Plans Methodology"

International Standards and Open Source Materials

Another resource that might be helpful for benchmarking specific controls is the International Standard ISO/IEC 17799, "Information Technology—Code of Practice for Information Security Management" 2000. The International Organization for Standardization and the International Electrotechnical Commission develop international standards, and the ISO/IEC 17799 provides recommendations for controls associated with most of the HIPAA security rule standards. In the US, the document is available from ANSI (www.ansi.org) for a processing fee.

While you are looking for security resources, you may also find what are called "open-source" software or methodologies. An example is the "Open-Source Security Testing Methodology Manual," copyrighted by Peter Vincent Herzog and available for free dissemination under the GNU General Public License (visit www.isecom.org/projects/osstmm.htm for more information).

While open source may be most closely associated with the Linux operating system, it has come to mean any software or methodology that is licensed for free distribution. The purpose of the license is to protect the integrity of the original work. Open-source material may be developed through a group consensus, individual, or other process.

If you find a resource you like online, bookmark the URL and consider saving the document (and catalog it). Many of the materials available on the Web disappear or are updated rapidly—make sure you're not missing any valuable information.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Finding Quality HIPAA Security Resources." *Journal of AHIMA* 75, no.1 (January 2004): 58-59.