Conduct Walk-Through to Check for HIPAA Security Violations

Security experts agree that employees are often one of an organization’s biggest security weak spots. According to one security professional, “You could have the best security policies in the world, but they aren’t worth their weight in paper if your employees don’t follow them.” For example, like many organizations, you may have a security policy that allows only authorized personnel to use your computers. But if your employees don’t question a stranger who comes in and sits down at an empty computer workstation, your policy isn’t working, and the security of important information—including protected health information (PHI)—is at risk.

The best way to find out if your employees are following your organization’s security policies is to watch the employees in action. One way to do this is to walk through your organization’s facilities and mark off a checklist that compares your security requirements with actual employee practices, says HIPAA Compliance Manager Joan Boyle. By observing security problems first-hand, you get an idea of which areas require attention and which areas are in good shape, she explains.

We’ll tell you how to conduct a security walk-through for your organization. And we’ll give you a Model Checklist, on p. 3, which you can tailor to the requirements in your organization’s security policies and procedures.

How to Conduct a Security Walk-Through

Conducting a security walk-through is as simple as walking around your organization and watching what your employees do or don’t do. Look at whether their actions are in line with your security policies. If they aren’t, you’ll need to talk to your employees and make sure violations are corrected.

Here are some tips for conducting your walkthrough:

**Be anonymous, if possible.** “Conducting a walk-through works best if you’re anonymous,” says Boyle. If people don’t know that you’re the security officer, you’re more likely to see security violations. For example, if your organization is so large that employees might not recognize you, try entering without signing in at the front desk or without wearing an ID badge. “An employee who holds the door open for someone who isn’t wearing an ID badge may think he’s being polite, but he’s really violating your security policies,” says Boyle.

**Conduct walk-throughs both during and after office hours.** Don’t limit your walk-throughs to office hours, says HIPAA Compliance Officer
Chris Apgar. Also check for security violations after employees have left, he recommends. Here’s one reason why: Say your employees use laptop computers that they regularly take out of the office for patient or customer visits. Although those laptops may seem secure during the day because the employees are using them, an after-hours walk-through might reveal that employees aren’t locking up laptops properly before they leave.

Avoid a regular schedule. Conduct your walk-throughs regularly, says Apgar, to be sure your employees continue to implement your security policies and procedures. But don’t set up a regular schedule that employees can guess. If your employees know that you regularly check for security violations on the first Monday of every month right before a director’s meeting, they’ll be more security conscious on that day, and you won’t get a true picture of possible security violations.

Insider Says: You may notice some security problems that aren’t violations of your security policies but that require fixing, says Boyle. For example, one compliance manager we talked to noticed that for scrap paper, his employees were using discarded reports containing PHI. “There was no specific policy against this in our organization,” he explains, “but we quickly put a policy in place that required all documents with PHI to be shredded. That way, no one could use them as scrap paper anymore.”

What Your Checklist Should Include

Like our Model Checklist, your checklist should assess:

**Employee conduct.** Look at the conduct of your employees objectively. For example, if your organization requires that all employees and visitors wear ID badges, check that everyone is wearing a badge. If you see a person walking around the building without an ID badge, note whether an employee challenges him and contacts a security officer if the person can’t produce an ID badge.

**Workstation use.** The potential for a security violation is enormous at employee workstations. “You would be surprised at the amount of confidential information that could be lying around,” says Apgar. Also, check that computer screens are positioned so that electronic protected health information (E PHI) isn’t easily viewed by unauthorized persons. And see whether portable equipment is secured, says Boyle—preferably locked down, with the key tucked safely away.

**Insider Says:** Check your organization’s printers, copiers, and fax machines, too, says Apgar. Make sure they’re in secure areas and that PHI isn’t left unattended after it’s printed, copied, or faxed.

**Access controls.** Check for compliance with your organization’s access control policies. Most people know that they shouldn’t write their password on a note and post it on their computer. But they may hide a note with the password under some papers in their desk drawer. Anyone with a little time could open the drawer and find it, says Boyle. So when you’re conducting a security walk-through, ask employees if they have their passwords written down somewhere...
Compare Employee Behavior with Your Organization’s Security Requirements

Security experts agree that conducting a walk-through of your organization’s facilities is a good way to make sure your employees are following the requirements set out in your organization’s security policies and procedures. Here’s a checklist you can adapt and use to make sure you know what to look for during a security walk-through at your organization.

Our checklist requires you to assess employee conduct, workstation use, access controls, and environmental controls. Be sure to customize this checklist to your organization’s needs by including specific requirements from your own security policies and procedures.

<table>
<thead>
<tr>
<th>SECURITY WALK-THROUGH CHECKLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EMPLOYEE CONDUCT</strong></td>
</tr>
<tr>
<td>Employees and visitors wear ID badges.</td>
</tr>
<tr>
<td>Employees challenge persons who are not wearing badges.</td>
</tr>
<tr>
<td>Employees protect security of PHI by speaking softly and, when appropriate, using nonpublic areas.</td>
</tr>
<tr>
<td><strong>WORKSTATION USE</strong></td>
</tr>
<tr>
<td>Workstations and computer monitors are positioned to prevent unauthorized persons from viewing EPHI.</td>
</tr>
<tr>
<td>Employees protect user IDs and passwords, and don’t share them.</td>
</tr>
<tr>
<td>Employees don’t share workstations while logged in.</td>
</tr>
<tr>
<td>User IDs and passwords are not posted on or near workstations.</td>
</tr>
<tr>
<td>Documents with PHI are face down or concealed, especially in public areas and when employees leave their workstations.</td>
</tr>
<tr>
<td>When documents with PHI are not in use, they are stored or filed so as to avoid observation or access by unauthorized persons.</td>
</tr>
<tr>
<td>Unattended computers are returned to the logon screen (automatically or by user) or have password-enabled screen savers when not in use.</td>
</tr>
<tr>
<td>All computers are shut down after hours.</td>
</tr>
<tr>
<td>Laptops, PDAs and other portable equipment are physically secured with lock that does not have key present or nearby.</td>
</tr>
<tr>
<td>PHI on printers, photocopiers, or fax machines is always attended by employees.</td>
</tr>
<tr>
<td>Backups of EPHI are secured in safe area (e.g., off-site and not in or near workstation).</td>
</tr>
<tr>
<td>PHI is shredded or discarded in secure container.</td>
</tr>
<tr>
<td><strong>ACCESS CONTROLS</strong></td>
</tr>
<tr>
<td>Doors with access-control mechanisms, such as locks or swipe-card systems, are closed.</td>
</tr>
<tr>
<td>Access to computer room is restricted to authorized personnel.</td>
</tr>
<tr>
<td>Access to fax machines and printers is limited to authorized staff.</td>
</tr>
<tr>
<td>Office doors, filing cabinets, and desks are closed and locked when unoccupied.</td>
</tr>
<tr>
<td>If after hours, office doors, filing cabinets, and desks are locked and/or building is alarmed properly.</td>
</tr>
<tr>
<td>Telephone closets are locked so unauthorized persons cannot gain access to telephone wires.</td>
</tr>
<tr>
<td><strong>ENVIRONMENTAL CONTROLS</strong></td>
</tr>
<tr>
<td>Smoke detectors and fire extinguishers are accessible and operational.</td>
</tr>
<tr>
<td>Computer equipment is plugged into surge protectors and, where appropriate, uninterruptible power supplies.</td>
</tr>
</tbody>
</table>
CONDUCT WALK-THROUGH
(continued from p. 2)

close by. And make sure that desk
drawers and filing cabinets are closed
and locked when an employee is away
from his desk or when it’s after hours.

Another common security viola-
tion is a door left open that should
have been closed and locked. One
health care provider told us that em-
ployees in his organization typically
prop open locked doors so they can
leave for a smoking break or to use
the restrooms. That’s a security prob-
lem, even if the door is left open for
only five minutes.

Environmental controls. Many
organizations overlook environmental
controls such as smoke and fire detec-
tors. You should check these each
time you conduct a walk-through,
says Boyle. Also check that computer
equipment is plugged into a surge
protector or an uninterruptible power
supply, adds Apgar. Otherwise, the
integrity and availability of your
EPHI could be at risk.

Environmental controls. Many
organizations overlook environmental
controls such as smoke and fire detec-
tors. You should check these each
time you conduct a walk-through,
says Boyle. Also check that computer
equipment is plugged into a surge
protector or an uninterruptible power
supply, adds Apgar. Otherwise, the
integrity and availability of your
EPHI could be at risk.

‘HIPAA-Compliant’ Products

Q Many IT vendors have advertisements claiming that
their products are “HIPAA-compliant” or meet
HIPAA’s authentication, encryption, and password man-
agement specifications. What does that mean?

A There’s no such thing as a HIPAA-compliant prod-
uct, says HIPAA security expert and Searchsecurity.com columnist Kevin Beaver. “Vendors have tried to
capitalize on the publication of HIPAA’s final security reg-
ulations and the general lack of understanding of HIPAA’s
security requirements by offering canned security solu-
tions,” he explains. He has seen vendors tout HIPAA com-
pliance to sell practice management systems, firewalls,
data encryption products, electronic transaction clearing-
house services, and more. But he warns that buying into
their promises could be a critical mistake.

“You can’t buy HIPAA compliance,” says Beaver.
It’s not just about technical solutions or IT in general, he
explains. Your organization’s security policies and proce-
dures are as important as the products you use to help you
achieve compliance. Although it’s true that health care
organizations will have to buy products and services to
help them comply with HIPAA’s security regulations, that’s
just one part of compliance.

Here’s an example of why a HIPAA-compliant product
alone won’t make you HIPAA-compliant. We saw one
software product that contained many of the safeguards
required by HIPAA’s security regulations—access controls,
user IDs, passwords, and a time-out feature that logs users
out of the system after a set period of inactivity. But sup-
pose your system administrator uses these security features
to create a generic account for temporary or new employ-
ees with the ID “Newuser” and password “Welcome.”
You’ll be in violation of the security regulations’ technical
safeguard that requires each user to have a unique user
name and/or number and prohibits generic logons. So even
though the software’s password feature can help you be-
come HIPAA compliant, you won’t be compliant without
good policies and procedures—in this case, a policy pro-
hibiting generic logons.

Filing Claims that Don’t Comply
with HIPAA’s TCS Standards

Q We know that Oct. 16, 2003, was the deadline for us
to start filing our claims electronically, in compli-
ance with HIPAA’s electronic transaction and code sets
(TCS) standards. But we’re still not ready to submit our
claims using the new electronic formats, and we probably
won’t be for months. Does this mean that plans will reject
all of our claims until we’re compliant?

A Not necessarily. If a plan is already in compliance
with the TCS standards, it can reject all noncompliant
claims after Oct 16. But the Centers for Medicare and
Medicaid Services (CMS) has said it won’t automatically
reject providers’ noncompliant claims after Oct. 16. And most plans are also unlikely to automatically reject such claims, according to San Francisco attorney Reece Hirsch.

CMS announced on Sept. 23, 2003, that it would implement a “contingency plan” to accept noncompliant electronic transactions after the Oct. 16 deadline. In its announcement, CMS also encouraged “other plans” to implement their own contingency plans to accept noncompliant claims from providers. “CMS recognized that most providers aren’t yet ready to submit compliant claims and wanted to make sure that providers’ cash flows and operations weren’t disrupted while they worked to become compliant,” Reece explains. “It also gave other plans some welcome flexibility to accept nonstandard claims and not alienate their providers,” he added. (To see CMS’s announcement, go to www.cms.gov. Click on “Public Affairs,” then on “Press Releases,” and scroll down to the press release issued Sept. 23, 2003.)

CMS didn’t go into detail about its own contingency plan, nor did it suggest what plans should include in theirs. So if a plan hasn’t notified you that it has a contingency plan and said what’s in it, you’ll need to contact the plan and find out what contingency measures, if any, it has put in place. For instance, the Blue Cross Blue Shield Association announced on Sept. 29 that each of the 42 Blue Cross Blue Shield (BCBS) companies would institute a contingency plan. But that means there will be 42 contingency plans just from BCBS, and they most likely won’t all be the same.

You’ll also need to ask each plan how long its contingency plan will remain in effect. “There’s no set time period for these plans. Even CMS hasn’t said how long its contingency plan will last. But at some point all providers will need to be in compliance,” says Hirsch. If a plan hasn’t yet set a time limit on its contingency plan, you’ll need to carefully monitor the situation so you’ll know your deadline for being compliant, he recommends.

Insider Sources
Kevin Beaver, CISSP: President, Principle Logic, LLC, 4430 Wade Green Rd., Ste. 180, Kennesaw, GA 30144; kbeaver@principlelogic.com.
Reece Hirsch, Esq.: Sonnenschein Nath & Rosenthal, 685 Market St., 6th Fl., San Francisco, CA 94105; (415) 882-5000; rhirsch@sonnenschein.com.

IN THE NEWS

► NIST Recommends Minimum Security Controls for Information Systems

The National Institute of Standards and Technology (NIST) recently released an initial public draft of its much anticipated publication, Recommended Security Controls for Federal Information Systems (NIST SP 800-53). The 238-page draft recommends minimum security controls for federal information systems that NIST has categorized as having low or moderate protection needs.

How does this draft affect you? HIPAA refers to NIST publications as “guidelines” for implementing the HIPAA security regulations’ requirements. In the preamble to HIPAA’s security regulations, HHS encourages health care organizations to monitor NIST activities and to provide comments and suggestions when NIST requests them. Experts in the security industry predict that this draft will greatly influence the security controls used by private organizations, including health care organizations.

The draft provides a catalog of management, operational, and technical controls for securing information systems, and could be used as a “best practices” standard for security compliance efforts. For example, the draft recommends a number of security measures to prevent unauthorized physical access, including:

■ Prominently marking restricted areas and separating them from nonrestricted areas by physical barriers;
■ Controlling/manning main entrances to restricted areas;
■ Using cameras and/or electronic detection devices, such as card keys, to control access to secondary entrances;
■ Investigating apparent security violations and resolving them, if necessary;
■ Requiring staff and visitors to wear identification badges; and
■ Ensuring that emergency exits and reentry procedures allow only authorized personnel to reenter restricted areas after an emergency or drill.

Comments on the draft are due by Jan. 31, 2004, and can be e-mailed to sec-cert@nist.gov.

Avoid Five HIPAA Security Problems Caused by Web Services

Paul Korzeniowski is a freelance writer in Sudbury, Mass., who specializes in security issues. His e-mail address is paulkorzen@aol.com.

You’ve probably been hearing a lot about Web services lately—and justifiably so. Web services are ways to build enterprise applications that enable computers to communicate more efficiently and use data from multiple sources. Their advent promises to allow health care organizations to easily exchange information within their own systems and with their partners, patients, and customers.

But the security infrastructure supporting Web services is still in the early stages of development and can expose your electronic protected health information (EPHI) to significant security breaches—including intrusions from outsiders. Your organization could face liability for violating HIPAA’s security regulations, as well as lawsuits by individuals whose privacy has been violated.

Because Web services’ benefits are so great, many health care organizations are evaluating them and, in some cases, getting ready to deploy them. Before you too move ahead with Web services, make sure you understand not just the potential benefits but the potential security problems. We’ll tell you about both the benefits and problems—and about what you can do to defuse the problems.

Benefits of Web Services

Web services have a different design foundation from existing—or legacy—applications. Legacy applications were built to operate in a controlled manner with information flowing in set patterns from central computers to other systems. But Web services can pull information from many computers instead of a central one. They allow any computer to communicate with any other computer, which takes advantage of the Internet infrastructure.

You can add Web services’ capabilities to any application, including human resource systems, office supply applications, and patient billing applications. Doing so offers the following potential benefits:

Faster application delivery. For example, with Web services, your patient billing system could connect automatically to an accounts receivable application, without a programmer having to make the connection. This automatic connection could shrink application development time considerably—say, from one month to two weeks—which means you’ll get the applications sooner.

Simpler service enhancements. You can rapidly add a new user interface to any system within your organization, such as to a product ordering system. So Web services could make older programs more functional.

Lower maintenance costs. You can develop Web services to provide certain functions (say, formatting a document for printing). So a programmer wouldn’t have to spend as much time making minor enhancements to a business application like an imaging system, which would save your organization money.

More flexible applications. Web services are easier to manage, and provide users with more options than legacy applications. For example, Web services would enable a user to insert an image into a database in an instant. Previously that step would have required a programming change.

Avoid Five HIPAA Security Problems Caused by Web Services

Five Potential Problems

Web service suppliers like Microsoft and Sun have moved quickly to deliver the application development tools needed to support Web services. As with most new products, these tools were completed before the necessary security infrastructure was perfected. Here are five potential security problems, and ways you can avoid them.

1) Lack of control points.

Because of the way Web services work, there’s no central point or points to place security checks. With legacy applications, software sitting on a central computer controls the flow of information and is the logical place to put security checks in place. But with Web services, virtually any computer on a network (including a desktop PC or PDA) can initiate an information flow. “Most security products were designed to operate with simple point-to-point connections and cannot handle the one-to-many links possible with Web services,” explains market researcher Susan Eustis.

What to do. Don’t assume that your existing security policies or the security methods and products you use to implement them will continue to work. A move to Web services requires that you reexamine and consider rewriting your existing security policies. With legacy applications, you could control different security checks such as password control, encryption, and access monitoring through one system. If you deploy Web services, you’ll need to reexamine those checks and make sure they are adequate for the many systems used by Web services.

2) Bypassed firewalls.

Firewalls act as a line of defense in securing EPHI transaction integrity. They are
designed to monitor incoming traffic and block unknown and sometimes unwelcome guests from accessing your network. With Web services, you may want to let unknown users in, so Web services vendors have developed ways for them to bypass the firewall and get into your network. While this simplifies application development, it creates a huge hole in your security perimeter.

**What to do.** Firewalls operate at the lower layers of the network. You can better secure your connections by adding more security functions on top of your firewall. For example, Secure Sockets Layer—an industry protocol that manages the security of information as it moves from an application to a user’s browser—operates at the network layer so the two ends of a connection are secure.

3) **Ineffective or incomplete security.** Security vendors are trying to put checks in place for Web services, but what works in the lab may not function on a real network. “One company had a 100M byte file that it wanted to secure, but that file was bigger than anything its security vendor had anticipated,” said computer security expert Pete Lindstrom. As a result, the security application aborted and the customer had to reevaluate its Web services deployment until the vendor came up with a way to fix it.

**What to do.** Grill your security vendors on how their products handle Web service transactions. In some cases, you’ll discover that their products have holes you may have to fill yourself.

4) **Greater application exposure.** Web services allow more computers to initiate transactions, such as examining information in a database, sending a shipment receipt to a customer, or moving a file from system to system. The downside of this flexibility is that it’s available not only to your employees, customers, and partners, but also outsiders, who can use it to wreak havoc on your computers.

**What to do.** Move slowly. Currently, Web services security is not robust enough to adequately protect sensitive items, such as EPHI. Your best bet is to limit your use of Web services to less sensitive applications, such as ordering new supplies or company internal information delivery systems. And you should separate these applications from the more sensitive ones.

5) **Lack of clear-cut standards.** Web services rely heavily on the Extensible Markup Language (XML) programming language to provide needed application fluidity. Vendors in a number of standards groups are developing standards to secure XML transactions—more than a dozen standards are now under development, and more may emerge. But the work is complex and difficult. The standards are also at different stages of maturity, with some finished but others still on the drawing board. Web services standards for basic security measures like message integrity and access control are still being developed, so vendors might not be delivering the security measures you need.

**What to do.** If authentication, key management, and encryption are sufficient to secure your transactions, you should be able to find XML products to meet your needs. But if you have information for which you need tighter security, such as EPHI, you should buy additional protective products your vendors have available or hold off on deploying Web services until the standards are finalized.

**Insider Says:** Consider bringing in an outside expert to help with the design and deployment of Web services. It’s difficult to get different products to work together and support your security functions in a new applications environment, especially if you’re doing this for the first time. The smallest misstep, such as overlooking a password reset routine, can open a hole in your corporate network. So you’ll probably want assistance—first with identifying potential problem spots and then with fixing them. Turning to a systems integrator, especially those experienced in health care, could help to skirt some of the problems. We’ll tell you how to find a good systems integrator in a future issue.

**Insider Sources**

**Pete Lindstrom:** Research Director, Spire Security, LLC, PO Box 152, Malvern, PA 19355; (610) 644-9064; petelind@spiresecurity.com.

**Susan Eustis:** President, Wintergreen Research, Inc., 6 Raymond St., Lexington, MA 02421; (781) 863-5078; susan@wintergreenresearch.com.

© 2004 by Brownstone Publishers, Inc. Any reproduction is strictly prohibited. For more information call 1-800-643-8095 or visit www.brownstone.com
'This index lists all articles published in the INSIDER from April through December 2003.'