Use RFP to Find Best HIPAA Security Assessment Vendor

Like many organizations, your organization may not have the resources to conduct a HIPAA security risk assessment that compares your technical and nontechnical security measures to HIPAA’s requirements. That’s where an outside security assessment vendor can help. It can identify and explain your security weaknesses and the potential threats and vulnerabilities to your electronic protected health information (EPHI). Plus, a security assessment vendor can give you advice on what security measures you should implement to comply with HIPAA’s security regulations and stay in business.

But how do you know which security assessment vendor is the best one for your organization? One good way is to put together a request for proposal (RFP) that you send to prospective HIPAA security assessment vendors. Creating an RFP for prospective vendors will help you focus your security assessment project. And it will give you a chance to review and compare prospective vendors’ written responses to questions tailored to your organization. “Done well, an RFP is an indispensable tool for visualizing a project; and it provides a concrete roadmap for your relationship with the vendor you select,” says information technology attorney Jay Hollander.

We’ll tell you the steps you should take to start the process of choosing the right HIPAA security assessment vendor, including how to set up an RFP. And to help you set up your own, we’ll give you a Model Form of an RFP that you can adapt and distribute to potential vendors (pp. 3–4).

Follow Three Steps to Start Vendor Selection Process

According to Hollander, choosing a vendor to perform a HIPAA security assessment should start with three steps.

1) Assess needs/scope of project. First you must identify what areas your HIPAA security assessment should include. Do you need an assessment of your physical access controls and security policies? Should the vendor conduct a penetration test of your internal and external networks to see how easily they can be breached? “Each organization’s needs will be different,” says information security consultant Earl Crane. For example, smaller organizations that don’t transfer EPHI over extranet connections probably won’t need a security assessment of their extranet, he explains.

Insider Says: For a list of the various areas an organization’s security assessment might need to cover, see p. 5. You can use this list to help you identify your own needs so you can communicate them to prospective vendors.
SECURITY ASSESSMENT VENDOR (continued from p. 1)

2) Narrow list of vendors. Next, you will need to get a list of prospective vendors. To do this, you can search for security assessment vendors on the Internet or ask colleagues for recommendations. Narrow your list by considering the vendors’ experience, general pricing approach, and the services they provide, says Hollander.

Focus on vendors that have the ability to assess both your technical and nontechnical security, recommends Crane. To get a complete picture of your security practices, you will need a technical assessment and a policy assessment, preferably by the same vendor, he explains. “Look for a vendor with a good understanding of HIPAA’s security regulations, and a good technical reputation,” he adds.

3) Prepare RFP. Once you’ve narrowed your list of prospective vendors down to four or five, it’s time to create an RFP. Your RFP, like ours, should include the following provisions:

➤ Purpose and goals. Begin your RFP with a brief explanation of the reason you’re seeking a HIPAA security assessment vendor and your goals for the assessment—that is, to identify and repair security gaps and comply with the HIPAA security regulations [Form, sec. 1].

➤ Proposal contact and method of evaluation. Give prospective vendors the name and contact information of a knowledgeable person in your organization to whom they can go for more information. And tell them who should receive the proposals and any additional information your organization might need [Form, sec. 2(a)]. Also tell them the factors that will affect your decision to accept a proposal. Explain that your consideration of the proposals will be based on more than cost, says Crane. This way, they’ll understand that they may be rejected even if they have the lowest bid [Form, sec. 2(b)].

➤ Schedule. Vendors will also need a schedule that outlines the RFP process from beginning to end, including the date when:
  ■ Responses to the RFP are due;
  ■ Vendor interviews will be held;
  ■ Supplemental information must be received;
  ■ A decision will be made; and
  ■ The project should start and finish [Form, sec. 3].

➤ Organization information. To understand the scope of the project and price it appropriately, prospective vendors will need a basic description of your organization and the information systems it currently uses. Be sure to describe all hardware and software, and let prospective vendors know how many active IP addresses your organization uses [Form, sec. 4].

➤ Scope of project. Based on the needs assessment you conducted before you narrowed down your vendor list, define the scope of the project in your RFP. Be precise, says Crane. Otherwise, your vendors might not bid on the same project, resulting in service and pricing differences that could be hard to identify and compare. And ask your vendors to break down their costs and the amount of time they require for each type of assessment you list in your RFP, Crane adds [Form, sec. 5].

(continued on p. 4)
Distribute RFP for HIPAA Security Assessment to Selected Vendors

Here’s a Model Request for Proposal (RFP) for a HIPAA security assessment. We prepared it with the help of information security consultant Earl Crane and information technology attorney Jay Hollander. You can adapt and use this Model RFP to help you find a vendor who can alert you to your organization’s security weaknesses and recommend ways to solve them. Consult our list of areas typically targeted for security assessments (on p. 5) to help you identify the areas your assessment should include. Then modify this RFP to suit your organization’s needs.

The RFP begins with an explanation of its purpose and goals (sec. 1). It then tells vendors whom to contact and explains what factors will influence acceptance of the proposal (sec. 2). It also gives vendors a schedule of important proposal and project dates (sec. 3). Next, it describes the health care organization (sec. 4) and the scope of the security assessment (sec. 5), and it asks for information about the vendor (sec. 6). The RFP then lists the items the vendor is expected to deliver upon completion of the assessment (sec. 7). Finally, the RFP contains a copyright and confidentiality clause prohibiting further distribution of the RFP (sec. 8) and requires that the RFP and proposal be attached to any contract ultimately signed by the organization with the vendor (sec. 9).

Be sure to have your attorney review your RFP before you submit it to prospective vendors.

REQUEST FOR PROPOSAL

1. PURPOSE AND GOALS

XYZ Health Care Organization (“Organization”) is seeking proposals for a HIPAA security assessment of its information systems and policies and procedures. The assessment will:

a. Identify and allow Organization to better understand potential internal and external threats and vulnerabilities to electronic data;

b. Compare Organization’s existing security measures (both technical and policy/procedure-oriented) against the requirements in HIPAA’s security regulations; and

c. Recommend feasible security measures that will allow Organization to address policy issues, eliminate or mitigate harm resulting from each identified potential threat and vulnerability, and comply with HIPAA’s security regulations.

2. PROPOSAL CONTACT & CONSIDERATION

a. Contact. Vendors must submit all questions, proposals, and supplemental information to:

John Smith, Chief Information Officer
XYZ Organization, 123 Hospital Dr., Anytown, NY
(212) 555-1000; jsmith@XYZOrganization.com.

b. Consideration. Any award made pursuant to this Request for Proposal (“RFP”) shall be based on each proposal with appropriate consideration given to Organization’s operational, technical, and management requirements. Evaluation of offers shall also be based upon each vendor’s responsiveness to the RFP and the total price quoted for all items covered by the RFP.

3. SCHEDULE

All proposals shall follow the schedule below. Any information received by Organization after the date specified shall be considered late and nonresponsive, and shall not be evaluated for the project.

- Sept. 1, 2004: RFP mailed to potential vendors.
- Sept. 15, 2004: Deadline for vendor questions.

4. ORGANIZATION INFORMATION

Organization is a 500-bed hospital with general medical and specialty facilities in three locations across the State of New York, with approximately 700 employees and 200 physicians on-staff.

The following describes Organization’s information systems:

[Insert list of hardware, software, and other system specifications].

5. SCOPE OF PROJECT

Proposals shall provide a one-paragraph description of vendor’s assessment procedures for each of the following:

- Internal/external networks assessment (including penetration tests);
- Internet/intranet vulnerability assessment;
- Web applications assessment;
- Wireless network assessment;
- Host diagnostic assessment;
- Firewall diagnostic assessment;
- VPN assessment; and
- Security policies and procedures assessment.

Proposals shall clearly identify all costs, including travel and expenses, by giving a detailed cost breakdown for each assessment listed above, as well as the number of hours needed to complete each assessment. Prices should include all costs to be charged for the project.

(continued on p. 4)
### 6. REQUIRED VENDOR INFORMATION

All proposals shall attach vendor’s most recent annual report or financial statements and shall include direct responses to each of the following questions in the format provided below:

- **Name & address:**
- **Contact person:**
- **Web site:**
- **# of employees:**
- **Yrs. in existence:**
- **Yrs. of experience conducting security assessments:**
- **Yrs. of experience conducting HIPAA security assessments:**
- **Brief summary of products and/or services:**

Identification and experience of management and information systems teams (including description of all security certifications and accreditations), particularly with respect to HIPAA’s security regulations (attach resumes):

- **List of previous clients for similar type of work with contact information:**
- **List of articles, white papers, and seminars conducted by vendor regarding compliance with HIPAA’s security regulations:**
- **Executive summary of the project proposal, containing synopsis of vendor’s project development approach and pricing structure:**

### 7. DELIVERABLES

Organization requires the following deliverables upon completion of the project:

- **Written documentation of the approach, findings, and recommendations associated with the project,** which shall include:
  - **Matrix of threats and vulnerabilities to Organization’s electronic data, including probability and impact of each threat and vulnerability based on (a) Organization’s current security measures and (b) recommended security measures;**
  - **Supporting detailed exhibits explaining threats and vulnerabilities;**
  - **List of Organization’s technical and nontechnical deficiencies in comparison with the requirements of HIPAA’s security regulations;**
  - **Detailed report of recommended remediation measures for each identified threat, vulnerability, and deficiency.** This report should include itemized costs for each recommendation, broken down by cost for hardware, software, and consulting services; and
  - **Milestone-based work plan with timeline to implement recommended remediation measures.**

- **Executive summary report summarizing the scope, approach, findings, and recommendations in a manner suitable for senior management;** and

- **Formal on-site presentation to Organization’s senior management of findings and recommendations.**

### 8. COPYRIGHT/CONFIDENTIALITY

This RFP is copyrighted by Organization and may not be distributed to third parties, including potential vendor subcontractors, without Organization’s written permission.

### 9. CONTRACT

A form of proposed contract is attached to this RFP. In the event Organization enters into a contract authorizing vendor to perform a security assessment of Organization’s information security systems and security policies and procedures, this RFP and vendor’s responses shall be attached to that contract.

---

**SECURITY ASSESSMENT VENDOR**

(continued from p. 2)

- **Required vendor information.**

  Your RFP should require certain “boilerplate” information about each vendor, says Hollander. He suggests that you structure your RFP to allow for easy and objective comparison between vendor responses. Don’t ask for “essay answers” if you can avoid them, he says. Instead, require potential vendors to answer questions in a specific format, as our Model Form does [Form, sec. 6]. Be sure to ask for:

  - The vendor’s corporate information, including name, contact person, address, phone number, Web site, number of employees, how long in business, and years of experience in security assessments;
  - A brief summary of the vendor’s products and/or services;
  - Identification and experience of the vendor’s management and information systems’ teams, as well as a description of all security certifications (such as a CISSP or CISA) or accreditations;
  - A list of previous clients for similar type of work with contact information.
A list of articles, white papers, and seminars that the vendor has conducted with respect to HIPAA security compliance; and

An executive summary of the project proposal, containing a synopsis of the vendor’s project development approach and pricing structure.

Insider Says: Also ask prospective vendors to attach financial information, such as their most recent annual report, to their project proposals, Hollander suggests. Vendors who are doing well financially are more likely to stay in business longer. So they’ll be around to finish your assessment and answer questions you may have in the future.

➤ Define deliverables. Tell vendors what you expect them to give you after they complete the HIPAA security assessment. That is, make sure you tell them that they must provide written documentation of their approach to the assessment, their findings, and their recommendations, says Hollander. And let the vendor know that you’ll expect a formal on-site presentation to your senior management explaining these findings and recommendations [Form, sec. 7].

➤ Copyright/confidentiality. Include a copyright notice in your RFP and bar the RFP’s distribution without your permission, says Hollander. This should prevent vendors you didn’t contact from responding to your RFP. And it should keep the vendors you contacted from shopping your RFP to subcontractors and competing for a project they aren’t capable of handling by themselves [Form, sec. 7].

➤ Contract. Hollander advises his clients to attach their model form of contract to the RFP. If you do this, vendors know ahead of time what your key requirements will be. It’s also important to let them know that the RFP and their proposal will be attached to whatever contract they sign. This is a good way to hold a vendor to the promises made in its proposal, Hollander notes.

Insider Says: We’ll tell you about what your contract for a HIPAA security assessment should say in a future issue of the Insider.

Insider Sources

Payors Requiring Physician SSNs on HIPAA Transactions

Q We’re a medium-sized, family medical practice with many payors that use clearinghouses to process claims. One of those clearinghouses told us that the HIPAA transactions and code sets (TCS) standards require that we include physician Social Security numbers (SSNs) in all of our transactions. Shouldn’t we be using the practice’s Employer Identifier Number (EIN) in transactions instead?

A Not necessarily, says Karen M. Beard, senior associate with a large medical management and planning firm. “The TCS standards permit payors to use a number of methods, including SSNs, to identify providers for payment or utilization review purposes,” she says. For example, a payor may ask for a provider’s EIN, SSN, or Unique Physician Identification Number (UPIN). So it’s probably okay for your clearinghouse to ask you to provide your physicians’ SSNs in your transactions if they’re what the payor wants.

There are several reasons a payor might need to know a physician’s SSN:

■ For tax reporting purposes, if the medical practice is a sole proprietorship;

■ To identify the referring, billing, and/or supervising physician on a claim form;

■ To verify that the physician is associated with the medical practice submitting the bill; and

■ For credentialing purposes. Many databases that payors use to verify a physician’s education, employment status, and malpractice history require the payor to know the physician’s SSN.

But note that as of May 23, 2007, payors won’t be able to use SSNs to identify physicians on HIPAA transactions. That’s the compliance date for the National Provider Identifier (NPI) rule. For HIPAA transactions on and after that date, payors may ask providers only for their NPI, unless they need the physician’s SSN for tax purposes. For more information about the NPI rule and its effective date, see “CMS Publishes National Provider Identifier Rule,” Insider, March 2004, p. 7.

Insider Source
Karen M. Beard, CPC: Senior Associate, Medical Management Assocs., Inc., 3330 Cumberland Blvd., Ste. 200, Atlanta, GA 30339; (770) 951-8427; kmb@medicalmanagement.com.

Tips for Securing Bar Code Technology

by Paul Korzeniowski

Bar code technology is expected to reduce the many deaths and adverse drug events that occur each year because of human error, misinterpretation of oral communications, misreading of handwritten notes, or administration of the wrong drug. Putting bar codes on medication containers will allow computerization of information about medication orders, dosage, and administration, and help medical personnel closely monitor medication dosages and administration. In fact, bar code technology’s potential benefits are so great that HHS is requiring drug manufacturers to adopt the technology by 2007 for drugs used in hospitals and dispensed under a physician’s order. And it’s expected that most hospitals will have to adopt bar coding by that date to comply with accrediting requirements set by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO).

While bar code technology has the potential to save lives, implementing it in your organization can raise a series of HIPAA security challenges, centering on both the underlying technology and the employees who work with it. If you’re not required to implement it, you’ll still have to decide whether to do so and to what extent. We’ll explain the costs and benefits associated with using bar code technology. And we’ll tell you about the risks the technology may pose for the security of electronic protected health information (EPHI) and give you some tips for dealing with those risks.

Costs and Benefits of Using Bar Code Technology

Should you implement bar code technology, even if it’s not required? Health care providers are besieged with a wide—and ever growing—number of IT investments and face a
difficult economic balancing act. “Small and medium health care providers are under pressure to keep costs down and could have difficulty justifying the investments needed with bar coding,” notes Scott Wallace, president and CEO of a Chicago health care consortium focusing on patient safety. Bar coding represents a significant upfront investment, requiring health care organizations to purchase:

- Bar code readers that collect medication information (priced from $100 to $250 each);
- Software applications that consolidate and interpret information from multiple readers and then tie that information into other applications, such as billing and patient records (priced from $1,000 to $5,000 per application); and
- Security products that maintain confidentiality per reader (adding approximately $50 to $200 to the cost of each reader).

But 7,000 people die in U.S. hospitals every year as a result of 1.25 million adverse drug events, estimates the Institute of Medicine of the National Academies, a nonprofit health care research organization in Washington, D.C. Unlike many other health care investments, bar code technology has benefits that can be measured in actual patient safety statistics—by looking at the reduced number of adverse events associated with patient medications. And those benefits can be quantified in dollar amounts. HHS pegs the cost of each adverse drug event at $5,857 and estimates that these events cost a 700-bed hospital an average of $2.8 million each year.

Use of Bar Code Technology Increasing

Based on the benefits, larger organizations are likely to want to use bar code technology as much as possible. In addition, the expectation that JCAHO will make bar code technology an accreditation requirement is pushing providers toward its implementation. In April 2004, JCAHO released a proposal to require accredited organizations, such as hospitals, to implement bar code technology to help identify patients and match them to their medications or other treatments by January 2007. “The number of health care organizations supporting bar coding is increasing quickly, so by the end of the year we anticipate that 30 percent to 40 percent of all health care providers will be working with the technology,” predicts Wallace.

Three Tips for Securing Bar Coded EPHI

Despite the benefits of using bar code technology, the technology presents a number of HIPAA security risks, including unauthorized access and lax procedures. Here are three risks posed by bar code technology and three tips to help you protect against them.

Risk: Unauthorized interception. Every time EPHI travels from a bar code label—say, on a patient’s medication—to a bar code reader, there’s a risk that an unauthorized person will intercept it. To do this, hackers need to be near the patient or health care employee and eavesdrop on the transmission by means of a protocol analyzer. A protocol analyzer examines information as it travels from the sending device (the bar code scanner) to receiving device (the bar code reader). Typically, bar coding data isn’t encrypted as it passes from the scanner to the reader, so it’s simple for a hacker to read the data.

➤ Tip: Encrypt bar code system transmissions. To prevent this problem, make sure each bar code scanner encrypts the EPHI it collects before sending it to a reader. Many bar code vendors will add scanning capabilities to personal digital assistants (PDAs), which feature add-on security cards that encrypt EPHI as it’s captured. For instance, a nurse could use a PDA to scan medication information, such as the medication’s type or dosage, encrypt it, and then send it to a patient record system for verification. After the system verifies that the medication and dosage are correct, the nurse gives it to the patient.

Risk: Bar codes are easily deciphered. Another security risk stems from the bar codes themselves. Most people think that using bar codes provides instant security because the lines and numbers are impossible to decipher without a scanner and reader. But that’s not true. “Bar codes label information so anyone who looks at it knows what medication a patient is taking,” says Barry Hieb, an industry analyst with Gartner Group. “This could be especially problematic with patients being treated for diseases like AIDS where they may not want to have that information known.”

➤ Tip: Restrict physical access to bar coded information. Your organization will still have to store bar coded medication in safe locations and not in the open. This way, only authorized personnel, such as nurses and doctors, will have access to it.

Risk: Poor user acceptance. According to a survey completed by PricewaterhouseCoopers for the Modern Healthcare Association, the biggest hurdle to new technology is user acceptance: More than half of all physicians and nurses resist new technology deployments.

Nurses, who now find themselves accounting for every second of their day, can represent a significant stumbling block to bar code deployments. “To save time, nurses in a few hospitals scanned medication at the nurse’s station (using copies of bar codes that
BAR CODE TECHNOLOGY
(continued from p. 7)

they kept at their desks) rather than as they were giving it to patients,” says Hieb. In these cases, the nurses weren’t taking the steps required to ensure EPHI integrity. That is, patients could have received one medication, even though the physician ordered—and the patient’s medical record reflects that the patient received—a different medication. This puts patient safety at risk, and it violates the HIPAA security regulations.

➤ Tip: Use trial runs to increase acceptance. To make sure your employees are using bar code technology properly, you’ll need to invest a significant amount of time and money to build their support of bar code programs. Conducting a trial run can help that process. “Like most individuals, health care professionals think only others make mistakes,” says Wallace. “Once a bar code system notifies them of mistakes when they’re giving medication, they become the biggest supporters of the system.”

During a trial run, nurses work with security administrators, who make sure the nurses follow proper procedures to verify and administer medication and protect EPHI integrity.

Insider Sources
Barry Hieb: President and CEO, Gartner Group, Gartner, Inc. 56 Top Gallant Rd., Stamford, CT 06904; barry.hieb@gartner.com; (203) 964-0096.
Scott Wallace: Industry Analyst, The National Alliance for Health Information Technology, One North Franklin, 27th Fl. Chicago, IL 60606; dwallace@na9hit.org; (312) 422-2180.

SECURITY INCIDENT WATCH

The INSIDER has developed this feature to help educate you and your staff about real-life security incidents. Below, we give you an anonymous account of an actual security incident that occurred at a health care organization and describe how the incident was handled. It can alert you to potential problem areas and serve as an effective training tool.

Clerk Accesses Husband’s Medical Record to Dispute Hospital Charges

INCIDENT
The husband of a medical records clerk was treated at a hospital that was part of a large midwestern health care system. The clerk contacted the hospital’s patient accounting department at her husband’s request to dispute charges on his bill. While on the phone with the accounting department, the clerk pulled up her husband’s electronic medical record to discuss the charges. The accounting department’s billing clerk realized that the medical records clerk was reading from the same computer screens that he was looking at on the hospital’s IDX system. Because he didn’t think she was entitled to access those screens, he notified his supervisor.

The billing clerk’s supervisor immediately contacted the medical records clerk’s supervisor and informed her that the medical records clerk was inappropriately accessing her husband’s medical chart. After being questioned by her supervisor, the medical records clerk explained that her husband had given her permission to access his chart, so she didn’t believe that she had violated the hospital’s access policy.

HOW IT WAS HANDLED
The supervisor for the medical records clerk forwarded the matter to the health care system’s chief compliance officer. He determined that the access did violate the hospital’s access policy, as well as the HIPAA privacy and security regulations, because it wasn’t part of the clerk’s regular job responsibilities. “If the clerk had called the accounting department and asked for a copy of the medical record with the husband’s permission, that would have been okay,” explains the compliance officer. “But her job duties didn’t give her the right to access the record herself, even if her husband told her that she could,” he adds.

After receiving the compliance officer’s report, the medical records clerk’s supervisor discussed the matter with the hospital’s HR department, and the clerk was fired within two days. “The clerks in this facility really didn’t take our privacy and security policies too seriously, until they realized we were willing to fire someone who accessed patient information inappropriately,” says the health care system’s compliance officer. “But now, this facility is among the tightest in our system when it comes to following our privacy and security policies,” he says.

SHARE YOUR SECURITY INCIDENT EXAMPLES
Do you have real-life examples of security incidents that you would be willing to share? Be sure to tell us what happened and how you handled it. And give us contact information in case we need more information. If we publish your incident, we’ll keep it anonymous. Not only will you help other organizations learn about security incidents and how to handle them, but you can use your own incident as a training tool without embarrassing anyone at your organization.

➤ Send a letter to: Editor, HIPAA SECURITY COMPLIANCE INSIDER Brownstone Publishers, Inc., 149 5th Ave., NY, NY 10010-6801;
➤ E-Mail awatkins@brownstone.com;
➤ Fax (908) 757-2844; or
➤ Call (908) 757-2843, and speak with the editor.