By the Rules: Making Security Policies Stick

compiled by Anne Zender, MA

Considerable attention has been paid to the development of organizationwide information security policies—especially what they should contain and how they should be put in place. But enforcing these policies isn't always easy. We asked four information security experts to give us their views on how to make policy enforcement fair, equitable, and—ideally—simple.

Our panelists are:

- *Joel Henenberg*, information resources security officer, University of Texas MD Anderson Cancer Center, Houston, TX
- *Jayne Lawson*, RRA, information security manager, Hartford Hospital, Hartford, CT
- *Katherine Lindsey*, clinical systems manager, Virginia Mason Medical Center, Seattle, WA
- *Carole Okamoto*, RRA, principal, CO Concepts, Seattle, WA

Q: Since the department of Health and Human Services issued its proposed rules for security and electronic signature standards in August 1998, many facilities have been busy developing and implementing information security policies and training their staff to comply. Now the question of actually enforcing the policies is coming into play. In your experience, how difficult are these policies to enforce? What factors affect a facility's ability to enforce them?

Henenberg: Enforcement of policies can either be extremely difficult or extremely easy. I believe policies that are written to be flexible are easier to enforce than those that are rigid. This is not to say that we do not need rigid policies. In the case of HIPAA, there will be several areas, such as electronic signature on medical records, where rigid policies will be needed.

Lawson: One of the biggest factors in enforcing policies is dealing with accountability. Information security is everybody's job, but there are times when you may apply policies and everyone may think you are being obstructive or impeding the processes of the organization. That's part of the learning curve.

Okamoto: I agree about the importance of accountability—I believe that security policies and procedures must be supported at the highest level of the organization to be effectively implemented and sustained. This includes ensuring that the board of directors understands the regulations and the legal ramifications of non-enforcement to the institution as a whole.

Lindsey: There are a number of important factors in enforcement. For one, the leadership should understand, mandate, and support policies and resources—human and technical. You need to make sure resources are in place to prevent staff from finding it necessary or "easier" to share passwords. You need to make security part of the organizational ethics—as important as safety in providing patient care. And you should work toward not having a double standard—so that all patients, whether they are employees of the hospital, VIPs, or regular people—are entitled to the same level of security.

Q: What are some of the key characteristics of an effective plan to enforce a security program?

Lawson: One thing we are doing is approaching enforcement from a team effort. You need to get the right players to address these issues and make the process more effective. Our team includes representatives from information systems, risk management, physicians, and human resources. This ensures that, as issues are addressed, the right players are at the table.

Henenberg: To effectively enforce any security program, an institution needs to understand the role of information security and the personnel in the department. Risk needs to be understood as well. I can't enforce policies or procedures that are not communicated to employees, so education also becomes an important part of enforcement.

Okamoto: Education—particularly understanding new regulations and the organizational implications and penalties for lack of compliance—is critical. If people don't understand what the regulations are, they can't or won't comply. Also, achieving a

balance between access management and legitimate business needs is a factor. Technology has made patient information much more accessible. In the paper-based model, there was a one-to-one relationship between the record and the end user. In an EMR environment, this shifts to a one-to-many relationship, and access control becomes a significant challenge. HIM departments need to achieve a careful balance between access management and legitimate provision of access for patient care and other business needs.

Lindsey: Another key is gaining administrative support. Our confidentiality task force tries to get visibility at high levels within the organization. We also promote accountability at the managerial level—making managers accountable for staff education and for auditing and tracking staff in their departments. For security policies to work, employees need to hear the message from the people who evaluate them. We also work closely with the human resources department to guarantee equitable disciplinary responses and consistency among managers. And we consistently log and track patient complaints.

Q: Ideally, who makes the final decision regarding enforcement of a security policy (including disciplinary and/or termination decisions)?

Okamoto: In my view, administration should make the final call, in conjunction with human resources. The security manager should provide the supporting documentation necessary to defend the actions taken. It's also important that all levels of administration understand the ramifications of information security—even the board of directors. This is where HIM professionals have to educate administrators about HIPAA. The key is to educate at all levels—and once you have support at the top, it will necessarily trickle down.

Lawson: At our organization, if the problem is from a system perspective, the decision may go to the CIO. Some issues have been decided by the management council. If it is an employee problem, it may need to go to human resources. The security manager acts as a coordinator. For day-to-day issues, we look to our information security team to recommend what to do.

Lindsey: Hopefully, a facility's policy also provides clarity in determining when security policies have been breached. This should go a long way in identifying the need for action. Ultimately, though, the decision may lie with human resources, in conjunction with the employee's supervisor. Human resources provides guidance and consistency to avoid a situation in which one manager fires someone while another who thinks the same problem is "not a big deal."

Henenberg: In an ideal world, all policies should be enforced. However, the investigation of a policy breach should provide enough information that the recommendation to management fits the breach. Then it is up to management to take disciplinary action or not.

Q: How can a facility make enforcement policies equitable, warranted, and fair for all staff?

Henenberg: For a start, as I said before, all policies should be enforced. If a policy is unrealistic, then it should be changed so that people can't ignore it (and, therefore, not enforce it).

Lindsey: Make sure that staff have the training and resources to follow the policies. And make it known that all (management and physicians as well) are accountable for following the policies.

Lawson: I agree that you should make sure the users know what the ramifications are if they use information inappropriately. This also needs to apply to users who are not part of your staff. For instance, there may be people who have remote access in an off-site physician's office who use our information. How can a hospital discipline a physician office staff member? What mechanics are in place to ensure compliance? These questions need to be answered.

Okamoto: In terms of dealing with violations, physicians themselves are not always treated as employees—sometimes they are treated more like partners. So administrators may have a different enforcement procedure for physicians. If there is flagrant violation, termination or suspension is a political and individual choice for the organization. One thing HIM professionals can do is to raise awareness and get better support for security issues. Then step up your policies and procedures—there should be similar policies for both employees and physicians. You can sell this if people are properly educated.

Q: Have you (or someone at your facility) ever had to confront a security policy enforcement issue? How did you handle it?

Lawson: There have been issues and situations that have been discussed—the need to audit and monitor, for instance, or in some cases limit access. One important point is that people need to be made aware of what the risks are. If there is an issue with a new initiative, for example, we will do a risk assessment before we make a determination to move forward. That's a major goal—to minimize risk.

Lindsey: The most common issue we face is when managers are reluctant to follow through with the disciplinary process, either due to philosophical differences or lack of time. Usually, a meeting with the manager to reinforce the importance of the issue and provide examples to them of other incidents within the organization is sufficient action to generate a response. Issues related to staff accessing records of their family members are also challenging; it takes a lot of time to make both managers and staff understand why such policies are necessary. It's helpful to give people examples of unanticipated breaches. Once they understand the rationale, it's easy from there.

Q: One of the keys to a successful security program is securing commitment from the highest levels of administration. What are some ways to secure—and demonstrate—this kind of commitment?

Henenberg: I think what makes a good security program successful is that everyone, from the CEO down, adheres to good information security practices. If people see that a senior manager gives his password out to his secretary, then the secretary thinks it's OK to give someone her password. With this kind of example setting, you can see how the problem propagates. My advice: be a role model and remember that information security is everyone's job.

Okamoto: And this begins when you educate, educate, educate at the highest levels of the organization. Ensure that people understand the "ownership" of security rests with them, not with the security manager. Lindsey: In our organization, the process of getting administrative support began with creation of the confidentiality task force. We made an effort to increase this group's visibility at high levels. We also use organizational manager meetings to provide information and education and to generate discussion about the issues.

Lawson: Our administration has endorsed our policies. We keep them informed about issues related to security. It's also important to include your administrators, when you can, in things that are going on. Our COO says that the information security team "is our conscience." That's a good perspective. Information security managers and teams don't make final decisions, but we can be the conscience, telling people what the issues are and what they need to consider to make decisions. That's where we need to go—being the conscience.

Tools of the Trade—a Confidentiality Tool Kit

When Katherine Lindsey began to work with a confidentiality task force at her organization, the group realized that as far as enforcement was concerned, it was important to give guidance to individual managers. "Do you set standards according to who the guilty party is?" she asks. "We realized that enforcement could not be contingent upon 'who did it.' But a lot of managers don't know what to do to get the message about security across, and what's more, they would enforce policies inconsistently."

The group's solution was to design a "confidentiality tool kit" that included a statement of organizational policy, philosophy of confidentiality, and summaries of the information employees have received, including confidentiality agreements. It also includes examples of types of breaches that can occur. "The reality is, depending on the type of breach, people don't have a formula of responses," Lindsey says. "By putting a tool kit together and making managers accountable, we put a process in place that made it more likely word would spread." It also is a more effective training tool than "bringing in an outsider" to talk about confidentiality, she says.

The tool kit also includes recommendations for measures such as "meeting summaries" when inconsequential breaches occur. "Many breaches are fairly 'innocent'—but rather than dismiss them, you should take the opportunity to make them a learning experience," Lindsey says. Following a minor breach, the committee recommends that a manager meet with an employee and discuss the incident. The manager would also write a follow-up memo stating that it was discussed. "These situations can intimidate managers—they don't want to harm their employees," Lindsey says. "This is a nonpunitive way of making the point and demonstrating a facility's commitment to confidentiality."

A similar system also works for clinicians through physician liaisons who work in cooperation with the confidentiality task force.

Toeing the Line—Tips for Enforcing Policies

How can you successfully enforce information security policies in your organization? Our experts offer some tips:

Create Policies

- Design your policies wisely. Use a team approach to identify areas where policies need to be developed. Keep the language in the policy simple, so there is no room for misinterpretation
- Get input from everyone who will be affected by your policies. Joel Henenberg advises: "Make sure those most affected by the policies participate in writing them. Ask people in departments that will be affected by the policy to review it and give their comments."

Educate and Educate Again

- Make sure all staff members sign confidentiality agreements—when they are hired and when they receive any additional access to patient information
- Make sure employees have a clear understanding of password protection. Teach password management and provide discipline when passwords are abused
- Get buy-in from management and users through education. Help managers understand that they have an important role in making sure that issues (and potential breaches) are dealt with
- Educate people when they are hired—and keep educating them. Give an annual safety update. Educate at computer classes. When incidents do occur, discuss them with staff
- One effective training method is to present to smaller groups or one-on-one sessions. "It's more labor intensive and expensive, but well worth it," says Carole Okamoto

Make Your System Work for You

- Design your information access structure based on job responsibilities. Make sure people have access on a "need to know" basis
- Design your system to include the ability to routinely audit and run special reports when needed. "We have automatic access logs printed that are reviewed for potential breaches," Katherine Lindsey says. "We also generate quarterly summaries of the types of potential breaches for use by the confidentiality task force."

Involve Your Vendors, Too

- Keep in touch with your vendors as you build a policy. Communicate that you will immediately cut off their access if they are responsible for a breach of security. Make sure this is included in your contract with them (you may also need to seek the advice of legal counsel). Make sure that any information used in accordance with an agreement with a vendor is returned to you when the contract is up. Also, ask vendors to advise you when one of their employees is terminated or leaves the company, so that you can disable their user IDs
- Put policies in place for reciprocal access agreements (e.g., business partners and other organizations that might have access to your data). Ask them to "meet or beat our standards" and ensure that they can demonstrate a strong business case for gaining access in the first place

When Things Go Wrong...

- Address all breaches somehow; don't ignore them. Even a documented discussion of an "innocent" breach makes an impact on an employee
- When a breach occurs, offer to meet with the manager and employee together for education. Don't let managers pawn the job off on someone else; the staff needs to know the manager supports the policy

No Double Standards, Please

It may seem difficult to fairly enforce policies for employees of varying levels. Our experts agree, however, that when it comes to security and confidentiality, there shouldn't be a double standard in enforcing policies. Here are some ways to make sure enforcement is fair:

- Ask a physician to participate on your organizationwide confidentiality committee. He or she can address confidentiality issues with peers
- Make sure that employees understand that knowing a patient personally, even if he or she is a family member, does not give a staff member license to look at their information unless they have a legitimate, work-related need to know
- Be aware of "teaching moments," e.g., when a celebrity is a patient at your facility. Perform an audit of that period and see if anyone inappropriately looked at the celebrity's records. Use this as an occasion to educate people about security

Gaining Visibility

One of the most important keys to building a successful information security program is to make sure the program is highly visible throughout the organization. Here are some ways to get your message out:

- Become an expert. You may not know everything there is to know about information security, but you can learn. Determine what you don't know, then do some homework. Know what has to be done to bring your organization into compliance
- Make sure every member of your department is an advocate of the security program
- Bring your boss up to speed. This may involve doing presentations on HIPAA, information security, and other issues to upper management and/or your organization's board of directors. If you are uncomfortable speaking in public, partner with other HIM professionals or enlist the help of your local or state association
- Understand that some of your colleagues may perceive having to constantly think about security as a barrier to progress—when they want to upgrade systems or implement new processes, for instance. Make sure they understand the risks involved in not complying with security measures. When issues arise, perform a risk assessment and make a determination together

Anne Zender *is editor of the Journal of AHIMA. She can be reached at annez@ahima.org.*

Article Citation:
Zender, Anne. "By the Rules: Making Security Policies Stick." *Journal of AHIMA* 70, no. 9 (1999): 62-65.