HIPPA NOTES
Radiology Responds
By Dan Harvey

In a presentation he helped deliver at the last meeting of the Radiological Society of North America (RSNA), Eliot Siegel, MD, who has written extensively on security issues in radiology departments, pointed out that the Health Insurance Portability and Accountability Act (HIPAA) has been called "the most confusing and anxiety-provoking nightmare to affect radiology in the United States in the past 100 years."

Indeed, HIPAA lately has been responsible for spreading Richter-scale heart palpitations throughout the healthcare field. Particularly, its security and privacy aspects are matters of great concern among radiologists and radiology departments. In a way, because computer technology is integrally involved, the situation feels similar to the Y2K anxiety of two years ago. The only difference is that HIPAA is real and it's inevitable. In fact, it's as inexorable as an asteroid on a collision course with the Earth. The impact will be just as profound, especially for the unprepared. Right now, some are just starting to take what amounts to belated steps. Others remain blithely unaware.

"In general, information technology departments in most hospitals are beginning to make preparations," says Siegel, director of the department of diagnostic imaging at Baltimore VA Medical Center/University of Maryland. "Hospital CEOs are aware of the issues but, in talking informally with colleagues, I think the majority of radiologists haven't even heard the term HIPAA or are only aware that it has something to do with security. They really don't know the background, the specific regulations, or the timetable for enforcement."

"Unfortunately, awareness levels are still pretty low," agrees Patricia Kroken, FACMPE, of Healthcare Providers, LLC, Albuquerque, N.M., and immediate past president of the Radiology Business Management Association, a nonprofit organization that assists radiology business management professionals. "People are just starting to realize that this is real and that this is going to happen. On the vendor side, they're aware but, in many cases, no one really knows what it means in every iteration of using equipment."

True, PACS and radiology information systems (RIS) vendors have engaged in proactive planning. Many have studied HIPAA requirements to determine what products or upgrades they must develop to help clients become compliant. Some customers even have started examining what services vendors can provide. Still, the consensus is that much remains to be done.

"I expect most people will be in panic mode a year from now," says Herman Oosterwijk, president of OTech Inc., a healthcare technology training and consulting company in Aubrey, Tex. Andy Forsyth, vice president of development at RIS Logic, a Solon, Ohio-based company that provides comprehensive RIS products, agrees with Siegel's assessment. "Looking around the industry, I'd say a lot of people have not progressed much in trying to make themselves compliant until recently," he says.

What's most important for now, Siegel believes, is that customers meet with vendors to identify needs and strategies to ensure patient confidentiality and security. Essentially, customers and vendors must now enter into a collaborative relationship in developing new software. "That's been happening to some extent, but it needs to happen more," says Siegel.

HIPAA Overview

Before taking a closer look at what has been done—and what still needs to be done—it's best to review

the elements of HIPAA most relevant to radiology. HIPAA was signed into law by former President Bill Clinton on August 21, 1996. The intent of the act is to simplify the exchange of information between healthcare plans, providers, and clearinghouses and to ensure the privacy and security of an individual's health information. **HIPAA's Administrative Simplification provisions are divided into four sections that cover informatics standards including the following:**

A. Standard Code Sets and Electronic Transaction involving standards governing the electronic transmission of specified administrative and financial transactions

B. Unique Identifiers referring to standards for national unique identifiers of health plans, healthcare providers, employers, payors, and individuals

C. Security and Electronic Signature Standards ensuring the confidentiality, integrity, and availability of electronically transmitted and maintained healthcare information

D. Privacy Standards ensuring the confidentiality of healthcare information through rules governing how that information can be used and disclosed

Security and privacy are the elements most relevant to radiology-specifically, security and privacy protections in the use of computer-based patient records, the electronic delivery of information, and the remote sharing of health information. Radiology departments now must concern themselves with the technical means to protect healthcare information and the patients' right to protect the disclosure of their information.

"HIPAA will have a critical impact on the RIS and PACS environments," says Oosterwijk. "These systems deal with patient information, so, security and privacy are a critical component. One can say that HIPAA requires a totally new approach to providing the information."

Consequences of noncompliance are potentially severe. Violation of standards can result in civil monetary and criminal penalties. For instance, an intentional misuse of patient information can incur fines of up to $250,000 and/or a maximum imprisonment of 10 years.

Privacy regulations are slated to start on April 14, 2003. Security regulations have yet to be finalized. "Some people speculate that it will happen fairly soon," says Siegel. "Once security regulations are finalized, it will be approximately two years after that date before they are enforced."

Path to Compliance

Many say that HIPAA compliance is 80% administrative and 20% technical. Thus, the greater part of compliance involves site configuration rather than equipment technology. On the technical side, each institution must assess systems for vulnerabilities. Vendors are focused on that 20%, as HIPAA technical security requirements are designed to create what some have called secure enclaves or trusted computing environments built on confidentiality, integrity, and availability.

Fortunately, HIPAA-based products are being created to meet these technical challenges. RIS and PACS program upgrades have been developed to address essential elements including the following:

A. Entity Authentification involving log-in security on information systems

B. Authorization and Access Control involving access security and limiting the access of patient information to the appropriate person

C. Transaction Reporting and Logging involving audit security and system logs designed to track who accessed information and when

D. Data Encryption promoting network security

To Michael Cannavo, president of Image Management Consultants of Winter Springs, Fla., the vendors appear to have taken the lead in developing HIPAA compliance strategies.

The vendors are doing it themselves," he says. "They see HIPAA as a major concern, and they're taking responsibility for the level of HIPAA compliance by creating tools such as audit trails, logs, biometric devices, data encryption, and password protection. But what they're doing is basic security, nothing extraordinary."

Customers must become more involved in the process. They can start by identifying the security problems inherent in an environment such as a radiology department and then helping to develop the necessary security strategies, observers believe.

"Customers are going to have to collaborate with their vendors before we feel truly HIPAA compliant because there are more things vendors need to do," says Siegel. "But I don't really see as much of a dialogue between radiology organizations and vendors as there needs to be. I'm hoping that RSNA, the American College of Radiology, and other imaging groups will begin taking the lead for creating a list of what some of those requirements are and trying to figure out the best way to integrate them."

"The vendors have done a better job in terms of collaborating," says Kroken. "Many of them have been active for a couple of years." Still, compliance will ultimately depend on the customer. "While software can help a customer become compliant, it is still up to the customer to implement the upgrades," says Siegel.

Forsyth agrees. "*You* have to look at this situation in a certain way," he explains. "It is not the software that is HIPAA-compliant. It is the customers. We can build the tools into a software program. If the program features are employed properly, then users can be HIPAA compliant."

That point may seem obvious, yet it must be stated. Incredibly enough, some resistance to the technical innovations has been demonstrated. "I talked with one of the major PACS vendors, and they told me that when they've tried to build in some tighter security, they've either met resistance where the customers have told them to remove the feature, or the features have been put in but not utilized," recalls Siegel.

Recommendations for Users and Vendors

Siegel suggests specific strategies and needs that customers should discuss with vendors. Customers should ask vendors to provide the ability to produce an audit trail of all accesses to the PACS database, including patient images and studies reviewed during each session. "Many PACS vendors currently don't provide an audit of access to images," he says. "But we need to be able to record who has looked at what images on what patients. Also, we need to know who has looked at what reports on what patients."

Siegel also believes that systems should include a feature allowing customers to force users to change passwords periodically. Users, he says, should be required by a system to change passwords every three to six months. "Most workstation vendors don't force password changes, or even allow the ability to monitor how long it has been since someone has changed his or her password," adds Siegel.

Systems should have the capability to limit access to only one person with a given user sign-on at a time. “Most systems that I know of don’t monitor for multiple instances of the same user,” Siegel points out. “For instance, if I share my user ID and password with eight other physicians who don’t want to bother obtaining a password, then most systems will allow eight instances of me to be signed on at the same time, without creating an audit or denying access.”

In addition, Siegel believes, facilities should have someone monitor online usage, to spot instances of duplicate users, and implement a no-tolerance policy with regard to sharing passwords. Similarly, radiology departments and hospitals should eliminate the use of “generic” user names and passwords. Also, passwords or user identification codes should never be posted on or near computer workstations. “When I go to other hospitals, I see passwords posted right up on the monitors, or right by the workstations,” says Siegel, “and I often see workstations where people sign in and the ID and password are essentially ‘PACS’ and ‘PACS.” Siegel would like to see vendors provide more support for bioscanning devices, such as fingerprint or retinal scanning devices, face, voice, or signature recognition, or “smart cards” that can transmit or scan for information about users.

Oosterwijk agrees, saying, “The ~devices arel already being deployed at some airports for security checks. It’s nothing new.” Siegel recommends that vendors have the ability to restrict a user’s access to limited subsets of patient information, based on the user’s “need to know” characteristics. “It will be important for imaging departments to have policies about who has access to what images,” he says. “Right now you can walk up to a PACS workstation in most places and, once you’ve signed onto the system, you have full access to all information on all patients.” Some vendors have already started addressing the areas of concern that Siegel identifies. In their effort to design HIPAA-compliant features and tools, vendors have produced useful and inventive devices.

Vendor Visions

“New technologies are available now, such as the biometric tools,” says Cannavo, citing the BioLink U-Match Mouse, developed by BioLink Technologies International, Inc., which identifies a user’s thumbprint when he or she touches the computer mouse.

“It scans your thumbprint, then sends an algorithmic version of it to your hard drive,” he explains. “It blocks anyone without the identical thumbprint from using the computer. Before, it was just password and login.”

Similarly, Marconi Medical Systems has developed a proximity sensor that operates as an automatic log-onllog-off device. “It’s a badge users wear that logs them in when they approach the computer,” says Cannavo. “Conversely, it logs them off when they step away.”

Oosterwijk reports that companies have developed software for encryption, authentification, and data integrity. “Off-the-shelf solutions are available,” he says. “It is just a matter of integrating these into your applications. Accessing a patient record from your PC at home should not be different from buying a book on Amazon or tickets from Travelocity. The critical information is either anonymized or encrypted.”

GE Medical Systems has developed a clinical information system that includes a standard feature providing encryption over the Internet. It also has designed monitoring products that incorporate a configuration, which automatically locks down the operating system to required services only. This feature protects data from being intercepted and interpreted by parties other than the intended recipients, and it allows remote users to access clinical information in confidence. For audit trails, it has developed PathSpeed PACS that logs key user parameters, such as data access and transfers, log-inllog-out, and network associations. Its Catalyst IVIUSE product includes an authentication and authorization that identifies users by different levels of access control. That is, it can restrict access to data and functions

based on the user.

Acuson has developed KinetDx, which offers PACS security tools such as user logs, inactivity timeouts, and confidentiality warnings. Agfa Medical's IJVIPAX system offers user access tracking, medical records retention, and controlled access privileges with regard to viewing, printing, transmitting, and editing.

RIS Logic, Forsyth reports, is in the process of creating a tool tentatively called RIS Logic CS. In developing this new RIS product, the company is taking a different approach than other vendors. "We're actually building it from the ground up," says Forsyth. "The security features are not ones we tried to patch into an already existing product. Many other companies try to force the capabilities into their current products. They try to retrofit existing products to meet HIPAA requirements."

In designing the product, the company studied HIPAA requirements and then determined what elements were essential. Features will include tracking for individuals who make changes to patient records. The program ensures that patient information cannot be deleted. "Once the medical information has been created in the database, it will stay there," says Forsyth. "You cannot eliminate it because you are required to maintain patient medical information." The program will be able to determine, on a user-by-user basis, which screens and what types of information the user can view, access, and change. "HIPAA requires that you only allow people the amount of medical information they need to see and access to do their jobs," says Forsyth. "We are building that kind of security model into our system."

Recommendations for Administrators

In making his recommendations about technology, Siegel is not suggesting that HIPAA compliance depends only on what PACS and RIS vendors develop and provide. Once again, it is the facility that ultimately makes itself compliant. It returns to the 80:20 ratio. Siegel, a member of the Society for Computer Applications in Radiology (SCAR), recently cowrote and coedited the SCAR University Primer 1, Security Issues in the Digital Medical Enterprise. In the first chapter, "Clinical Impact of Security on Diagnostic Imaging," he and colleague Bruce I. Reiner, IVID, offer administrative suggestions. The following three are especially relevant to radiology as HIPAA approaches:

A. The imaging department and hospital should install written policies and procedures to allow access only to users who have legitimate needs to access images and should have written policies defining various levels of privilege for users both inside and outside the imaging department.

B. Imaging departments and healthcare enterprises should identify a person or persons responsible for electronic record security and establish a process to regularly assess the effectiveness of the electronic security program.

C. Ongoing education about the importance of confidentiality and security should be required for all healthcare providers and other employees.

For organizations just starting to move toward HIPAA compliance, Kroken suggests that they assess all operations within their practices, including how various sites communicate with each other and how much information is handled electronically. They also need to inventory all of their hardware and software, says Kroken. "Then, they must get in touch with their vendors and see where there vendors are," she adds.

Worth it in the End

Many might view HIPAA as some sort of amorphous and omnipresent dark specter. However, others see

it as a good idea whose time has arrived. Siegel feels that developments in technology necessitate something like HIPAA. He also feels the technology developed in response to HIPAA requirements will have a beneficial effect on the daily operations of radiology departments. The technology solutions, he writes in the SCAR Primer, "will actually streamline workflow by eliminating many of the steps associated with the use of PACS. Such solutions may help to gain support for the innovative systems that will simultaneously increase security and improve both productivity and patient care."

Kroken also is optimistic about HIPAA, as it essentially will force the healthcare industry to catch up with other business sectors in matters of security. "It just makes sense ~to implement HIPAAI because more and more practices have moved many of their procedures to electronic processes," she says. "In the end, I think it will have been beneficial to have gone through all of this. It is going to make radiology-actually, all of medicine-come up to many of the best practices to which other industries have had to comply for a long time."