Avoiding HIPAA Hype: Preparing for HIPAA Affordability

BY BECKI WEBER, CPMA; BOB ALCARO; AND VINCE CIOTTI

In the scramble to prepare their organizations for HIPAA compliance, healthcare financial managers nay believe they must commit significant funds to overhauling information systems and hiring consulting firms. But security and confidentiality policies required by HIPAA cannot be implemented solely by upgrading computer systems. HIPAA compliance requires a wholesale change in staff attitudes and behavior regarding patient security and confidentiality. Healthcare organizations can prepare to comply with HIPAA regulations practically and affordably by combining in-house expertise with limited assistance from outside consulting firms. An added benefit of emphasizing the use of in-house resources to prepare the organization for HIPAA compliance is that the organization can develop and retain its own experts on HIPAA.

Healthcare facilities are being deluged with proposals from vendors and consulting firms offering to help them comply with Health Insurance Portability and Accountability Act (HIPAA) regulations. The following marketing claims from HIPAA consultants may seem familiar to healthcare organizations that were bombarded by claims of consultants offering programs for Year 2000 (Y2K) readiness:

· *Act now.* There is only a short time to prepare.

· *Hire us.* Healthcare organizations should not rely on in-house expertise or resources to cope.

· *Spend more on IT*. The board should budget for new information systems.

· *Huge risk.* Healthcare organizations that do not heed the above advice will find it difficult to survive.

Although HIPAA regulations represent a major compliance challenge, healthcare organizations need not spend a fortune to prepare for these regulations. Rather, by combining in-house capabilities with limited outside assistance, healthcare organizations can prepare for HIPAA in a practical and affordable fashion. In addition to saving money, this approach allows the organization to keep its HIPAA expertise within the organization, which is likely to prove valuable as the organization modifies its compliance efforts in response to the possible evolution of HIPAA regulations.

Is HIPAA an IT Problem?

The greatest myth about HIPAA is that it is an information technology (IT) problem that requires the purchase and installation of new hardware and software throughout the facility. This notion is incorrect. HIPAA is a security and confidentiality challenge that applies to every medium through which patient information is recorded and communicated. For example, a new computer system is of little help in eliminating the following compromises of patient confidentiality:

· *Casual conversations.* Conversations by clinical staff about a patient's condition can be overheard if they occur in a public place, such as an elevator.

· *Unshredded trash.* A record of a patient's medical condition, such as a laboratory test result, can be removed from a waste receptacle.

· *Unsecured passwords.* Yellow stick-on notes containing the passwords of nurses and physicians commonly decorate computer monitors in healthcare facilities.

· *Unsecured modem lines.* These lines allow a vendor to dial into a "turnkey" system at any time at its convenience to diagnose system errors, for example.

· *Nonterminated security codes.* Terminated employees' security codes frequently remain "live" long after the employee has left the organization.

· *Breaches of e-mail messages.* Unsecured e-mail can make confidential patient information available to anyone who can access the system.

HIPAA concerns the totality of confidential information about a patient, whether it is communicated on a paper chart, a fax, or through verbal conversation. IT is a major conduit for patient information, and thus needs to be a key focus of HIPAA preparation, but HIPAA concerns cannot be "cured" simply by spending money on new systems. HIPAA compliance requires an institutional effort that focuses on education, behavior modification, and organizationwide cooperation.

Nonetheless, certain IT system features can facilitate the process of HIPAA compliance at relatively little cost. These features include capabilities for timed sign-offs, biometrics, journaling, and electronic signatures.

Timed sign-off. A security breach can occur when a physician or nurse signs on to a terminal to enter an order, then leaves the terminal without formally signing off. The next person to use the terminal can enter another order using the first person's code. A good hospital information system is programmed to log out automatically after a certain number of seconds have elapsed without a keystroke and to require password verification before any order is transmitted. The system should allow these variables to be adjusted according to user needs. For example, a biller normally needs a longer interval before sign-off because of the high volume of keystroking this work involves. Having to sign in repeatedly would be a waste of time with little accrued value.

Biometrics. This technology allows the system to recognize fingerprints, voices, or retinal images of authorized users. Its great advantage is that it "remembers" the user's unique fingerprint or other physical identifying characteristic. Early versions of this technology are relatively inexpensive and are being used successfully for applications such as time-and-attendance systems and pharmacy-dispensing devices. Biometrics technology promises to end the need to memorize and frequently change multiple passwords, while vastly improving security.

Journaling. Modern systems that are based on a relational database can record who entered every piece of data and when it was entered, allowing the trail of original entries and subsequent modifications to be audited efficiently. Such systems provide far more capability for auditing who has had access to what patient records than older flat-file systems that do not record such information.

Electronic signatures. Electronic-signature technology allows physicians to bypass physically signing a document to confirm a telephone order or complete a dictation by entering a special security code assigned solely to them instead. If an organization decides to use electronic signatures, however, it should implement encryption technology to ensure message integrity, user authentication (such as a hashing algorithm or passwords), and a nonrepudiation feature that does not permit a user to later deny that the electronic signature was sent.

These three safeguards are especially important if access to the information system is remote to the local area network of the entity covered under HIPAA because the digital certificate attributes are more vulnerable to exposure as they travel over external telephone lines. These technologies do not ensure HIPAA compliance (indeed, no computer system can guard against the mistakes of uneducated or

unconcerned users). But they can help simplify the complex task of preparing a healthcare facility to abide by HIPAA regulations.

HIPAA Preparation: A Case Study

Following is a list of the steps taken at Meridian Health Systems (MHS), a three-hospital integrated delivery system in Wall, New Jersey, to prepare for HIPAA compliance. These steps allowed HIPAA preparation to be accomplished using mainly in-house staff and modifying existing information systems rather than replacing them. The primary steps are executive briefing, organization, assessment, education, remediation, and ongoing monitoring.

Executive briefing. This step is essential to ensure that the organization's top-level executives commit themselves and the organization's resources to the HIPAA project. It is common for an organization's upper management to view an in-house speaker as less credible than someone from outside the organization. At MHS, the decision was made to hire an expert speaker who had worked at CMS (formerly HCFA) and had experience in writing regulations. The affordable cost of hiring the speaker for one day was well worthwhile because the speaker convinced MHS senior management of the severity of the HIPAA challenge and was instrumental in gaining their commitment to undertake subsequent HIPAA initiatives.

Organization. Preparation for HIPAA compliance should be undertaken by a committee led by a representative of the IT department and composed of representatives from nursing, the medical staff, healthcare information management, finance, human resources, and major ancillary departments. If the executive briefing has been successful, senior managers should be convinced of the need to assign the best employees to the committee. Because IT has the smallest number of employees handling confidential patient information, its leadership role should lessen gradually as other departments gain knowledge of HIPAA issues.

Many HIPAA consultants recommend the formal appointment to the organization staff of a security officer concerned with access to protected health information. This person should hold a position on the committee. In the case of MHS, the security officer possessed valuable experience from heading the organization's Y2K efforts, so he was well known to the staff and was able to contribute knowledge of tools and data that also are needed in preparing for HIPAA.

Assessment. The assessment, or data-gathering, phase is laborious, but necessary to collect and analyze information from throughout the facility about the following:

· Current privacy and security policies;

· Disciplinary actions established for violators of security policies;

· Policies on record-keeping of patient information;

· Policy for release of recorded medical information;

· Policies for information system security documentation;

· Access control policies and procedures;

· Job descriptions;

· Past security breaches;

· Recovery procedures for computer failures;

· Policies for volunteers regarding patient privacy; and

· Policies on the use of electronic media, such as e-mail.

To keep costs down and raise internal awareness of HIPAA, the assessment can be performed internally by the HIPAA committee. At MHS, consultants were employed for only a few days to provide guidance about the type of data to gather and to design a questionnaire to reveal how users handle confidential data. The MHS security officer also began gathering data on the following IT aspects of security and confidentiality:

· Data access by user job class;

· Security code assignment procedures and forms;

· Data exchanges/EDI protocols and policies;

· Security threats and measures for remediation; and

· Encryption techniques.

MHS currently is reviewing every vendor contract for clauses relating to confidentiality definitions and obligations; system security, especially for Web-enabled systems; chain-of- trust agreements; and responsibilities for meeting regulatory changes.

MHS reviewed some contracts with in-house legal counsel and renegotiated others to ensure that its vendors are contractually obligated to modify their systems in any way required by HIPAA as part of ongoing software maintenance. It is important to define software-maintenance terms thoroughly to avoid being charged for new "HIPAA-compliant" software releases. MHS takes the position that modifications that are needed to comply with HIPAA are part of the vendor's cost of doing business. Hospitals and healthcare systems may wish to leverage their influence to encourage vendors to accept this view.

Education. The next step is to conduct education sessions for middle management, including the directors, managers, and supervisors of user departments. At MHS, these education sessions are being planned by the internal HIPAA committee with the assistance of the consulting firm that conducted the executive briefing. It was thought that this combination of outside and in-house expertise would yield the optimum results.

Education assistance from a consulting firm may cost in the low five-figure range, particularly if the organization has a number of locations. MHS still is in the planning stages of user training, but is considering using a combination of "train-the-trainer" classes conducted for mid-level managers, who then would lead brief sessions conducted by outside experts for all users.

After the initial classes are conducted, a special HIPAA orientation inservice will be created for all new employees and new physicians. This orientation will target volunteers, agency nurses, and other temporary employees because the nonpermanent nature of their jobs makes them more likely to treat security issues casually.

Remediation. Concurrent with the education sessions, remediation efforts are needed to correct the organization's weakest links in patient confidentiality protection. A gap analysis should be at the heart of remediation efforts. The MHS gap analysis is being created during the HIPAA assessment phase, in which access to patient information and the organization's level of exposure for each point of access is

catalogued. One of the following numeric grades should be assigned to each point of access to confidential patient information:

0= No identifiable process or control;

1= Informal or partial process or control;

2= Controls implemented for most elements of HIPAA compliance;

3= Controls fully implemented for all elements of HIPAA compliance; or

4= Process or controls exceed levels required by HIPAA.

Management then must decide where to spend funds first. A good example of a high-risk problem with a relatively low-cost solution is computer printouts that contain confidential patient information. Whether the printout is an interim radiology report printed at a nursing station or a UB-92 form with a diagnosis code generated by the business office, such printed material should be shredded rather than merely discarded into trash cans. At MHS, a series of blue bins similar to the red bins in which medical waste is discarded are picked up periodically by maintenance workers, and the contents are transferred to special containers for shredding and/or confidential disposal.

The result of remediation efforts should be a written plan of action that governs exactly which procedures should be changed, which policies should be strengthened, what penalties are appropriate, and what (if any) IT systems need security augmenting. If security issues are found that cannot be corrected in a timely manner using internal resources, it may be necessary to obtain consultant assistance. In most cases, minimal funds will have been spent on consultants up to this point, so consultant assistance to address security issues speedily may be within the organization's budget.

Ongoing monitoring. One goal of a HIPAA compliance process is to change the thinking of healthcare personnel about patient confidentiality. To achieve this goal, the following ongoing activities should be undertaken:

· *Inservices.* These should be conducted routinely whenever HIPAA regulations are modified.

· *Periodic quizzes for all employees.* Such quizzes should be department-specific and designed and administered to help determine where further training or emphasis is needed. They should not be presented as a way to uncover noncompliant behavior or to punish individual employees.

· *Posted reminders encouraging awareness of confidentiality issues.* For example, a hospital may post signs outside elevators reminding staff not to discuss patients' conditions in the elevator. Notices should be posted throughout the organization's facilities, perhaps even on the sign-on screens of HIS systems.

· *Annual reviews.* Annual employee review forms should contain a section wherein the employee's compliance with HIPAA security measures is reviewed.

· *Security checks.* Efforts should be made to monitor employee access to patient data. Again, these efforts should not aim to punish offenders, but to reveal which systems or policies should be strengthened.

Technology can be used to heighten security, rather than adding to the risks. The many "rules engines" that vendors are marketing to improve patient care (eg, those that prompt a physician to order generic, instead of name-brand, drugs) can be used to improve HIPAA compliance.

For example, it is relatively simple for information systems vendors with relational database systems to provide lists of which users entered or inquired into patient data by recording every user who accesses a field with the date, time, and terminal identification. However, these lists may become voluminous. Rather than painstakingly reviewing these lists to uncover one or two inappropriate events, rules could be implemented to narrow the search. For example, the system could be directed to flag only those inquiries into a patient's record by a nurse from floor A for a patient on floor B. The resulting report would be brief, readable, and simple for nursing administration to review with the nurse in question. This technology also allows access to patient charts only by specific physicians, such as attending physicians and physicians consulting about the case. (Ideally, patient information should be available to physicians only on a "need-to- know" basis.) Again, this protocol yields a relatively short list of accesses to be reviewed and is a good alternative to allowing physicians either unrestricted access or no access at all to patient health information.

Conclusion

At a time when hospitals are experiencing severe strain on their bottom lines due to managed care pressures, the out-patient prospective payment system, and the Balanced Budget Act, HIPAA is threatening to further reduce scarce financial resources. Healthcare providers need to be as self-reliant as possible in ensuring HIPAA compliance. Consulting firms can provide some expertise and hands-on assistance, but an organization should create its own internally directed HIPAA compliance project in addition to possibly engaging a consulting firm.

ABOUT THE AUTHORS

Becki Weber, CMPA, is vice president and CIO, Meridian Health Systems, Neptune, New Jersey.

Bob Alcaro is a principal, HIS Professionals, LLC, Washingtonville, New York, and president-elect of HFMA's Hudson Valley Chapter.

Vince Ciotti is a principal, HIS Professionals, LLC, Santa Fe, New Mexico, and a member of HFMA's New Mexico Chapter.

Questions or comments regarding this article may be sent to Bob Alcaro at ralcaro@hispros.com or Vince Ciotti at vciotti@hispros.com.

Reprinted from the August 2001 issue of Healthcare Financial Management.