'Information Security 101'

Complying with HIPAA and Staying Out of the News

By Jennifer Willcox

Recent headlines have reported a startling number of security breaches and information thefts. A major university notified 120,000 of its alumni after a computer containing fundraising information including addresses and Social Security numbers was hacked by an unknown intruder; a subsidiary of the Lexis Nexis group announced that the records of 32,000 individuals may have fallen into the hands of thieves using the passwords of legitimate subscribers; Bank of America reported the loss of backup tapes containing the financial records of up to 1.2 million federal employees; payroll outsourcer PayMaxx faced allegations that it had exposed 25,000 customer records, including W-2 information, online; and cell phone provider T-Mobile released information about a hacker who was able to exploit a security weakness in a commercial software package to access customer records, sensitive government documents, private e-mail and candid celebrity photos.

These stories have caught the attention of federal lawmakers, who are proposing legislation to address the security vulnerabilities in a world where personal data is increasingly available through digital media. But computer security is already a matter of law for many companies that provide health benefits for their employees. April 20, 2005 was the effective date for regulations regarding the security of electronic health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA Security Rule). (Note, "Small health plans," or those with less than $5 million in receipts, have an additional year to comply [April 20, 2006]. For further information on how to calculate "receipts" in determining whether your plan is "small," go to the Centers for Medicare and Medicaid Services [CMS] HIPAA Web site: www.cms.hhs.gov/hipaa/ hipaa2 /default.asp, select "Frequently Asked Questions" and then search for "small health plans.") As was the case with the HIPAA Privacy requirements that went into effect in April 2003, all individual or group health plans that provide or pay for the cost of health care are covered. This means employer-sponsored medical plans, medical expense reimbursement accounts, and any separate dental and vision plans, whether provided through the purchase of insurance (fully insured plans) or paid directly out of company assets (self-insured plans).

Information Covered By the HIPAA Security Rule

A health plan or health insurer's HIPAA Privacy program addressed all protected health information (PHI) maintained or created by or on behalf of the plan, whether on paper, in a computer system or communicated orally. The HIPAA Security Rule addresses a small sub-set of PHI: *electronic protected health information*, or e-PHI. This means information in databases, in word processing documents on computers, and conveyed in e-mails — in other words, all PHI that is maintained or transmitted electronically. If some or all of a plan's e-PHI is in the hands of vendors or third-party administrators, then the plan must enter into an appropriate contractual arrangement with the vendors and/or third-party administrators (*see* the discussion below regarding business associate contracts). Even if an employer has outsourced most of its plan administration functions to an insurer or a third-party administrator, it is probable that at least *some* e-PHI remains in-house, even if it is just e-mails responding to employee inquiries about benefits or coverage.

HIPAA Security Rule Requirements

If a plan maintains or transmits any e-PHI, it will have to satisfy all of the HIPAA Security Rule requirements. At a basic level, the Rule requires health plans to protect the *confidentiality*, *integrity* and *availability* of e-PHI. This goes beyond just privacy — the Security Rule is also intended to ensure health information is not improperly altered or destroyed, and that e-PHI can be accessed even in cases of emergency (system shut downs, for example). The Rule is broken down into three categories:

- administrative safeguards (business processes and policies for protecting e-PHI);
- physical safeguards (how equipment and facilities housing e-PHI are physically secured); and
- technical safeguards (electronic mechanisms and programs that protect hardware and software).

For each category, the Rule defines specific standards and "implementation specifications" that consist of basic security protocols, such as audit logs, unique user identifiers, and password management. Some of the implementation specifications are "addressable," meaning that you need to adopt them only if reasonable and appropriate for the health plan, but these decisions must be documented — "addressable" does not mean "optional." The HIPAA Security Rule

continued on page 4

Jennifer Willcox is an attorney in the Health Care and Employee Benefits departments at Wiggin & Dana, a New Haven, CT-based law firm with offices also in Hartford and Stamford as well as Pennsylvania and New Jersey. Willcox is part of the firm's nationally known HIPAA practice group, which assists clients ranging from Fortune 500 companies to small non-profit agencies in structuring and implementing their HIPAA compliance program. She may be reached at jwillcox@wiggin.com.

Information Security

continued from page 3

includes a chart listing all of the standards and implementation specifications; the chart and the regulation are available at www. cms.hhs.gov/hipaa/hipaa2/regulations /security/03-3877.pdf. (For more detailed information about the HIPAA Security standards, please visit the Wiggin and Dana LLP Web site at www.wiggin.com/pubs/advisories.asp, click on "HIPAA Advisory" and then select "Summary of HIPAA Security Rule.")

GETTING TO HIPAA SECURITY COMPLIANCE

Health plans that maintain and transmit e-PHI but which have not yet addressed HIPAA Security compliance should take the following steps:

- Appoint a "Security Officer" to oversee HIPAA Security implementation. This may be the same individual that serves as the HIPAA Privacy Officer, but it should be someone familiar with information systems and general information security practices. The Security Officer should also be someone with IT decision-making authority and responsibility in the organization.
- Assemble a multi-disciplinary team to oversee implementation and to participate in the decision-making concerning identified security risks and whether additional security measures should be implemented.
- Inventory all existing security policies, procedures and practices. Inventory all e-PHI and the flow of e-PHI into, out of and within the health plan by identifying the systems, hardware and software that maintain or transmit e-PHI in connection with the plan. Consider systems, hardware and software associated with the use of laptops, PDAs and other handheld devices, and maintenance and transmission of e-PHI through remote access (such as from home computers).
- Conduct a "risk analysis" that assesses the potential risks and vulnerabilities to your plan's e-PHI and measures the adequacy of the existing security measures. Risk assessments are familiar concepts to information technology (IT) professionals, and your company already may have a methodology in place. IT staff should be involved in the risk assessment; consider involving IT consultants if you do not have the appropriate in-house IT expertise. Where necessary based on the assessment, implement additional security measures to reduce unacceptable risks to a reasonable and appropriate level.
- Using your risk assessment results, review compliance with the Security Rule standards and implement additional measures where necessary.
- Develop policies and procedures for managing e-PHI or modify existing security policies to address changes made to your security practices. As noted below, where appropriate you may modify existing HIPAA Privacy policies to address security.
- Amend your plan documents to include the required language from the HIPAA Security Rule.
- Review your business associate agreements to determine whether they need to be updated to include additional HIPAA Security language.
- Train HR staff that have access to e-PHI on appropriate security measures.

PRACTICAL POINTERS

Most health plans will not be starting HIPAA Security from scratch. At least part of what you need probably is already in place, such as locks on the doors to your office and unique user IDs and passwords to log into your computer systems. As part of HIPAA Privacy implementation, you may have already "cleaned house" by limiting the PHI (electronic or otherwise) you receive from your vendors and TPAs. The HIPAA Privacy and Security Rules also overlap to a limited degree, and some of the work to comply with HIPAA Privacy can be used and/or supplemented to meet your HIPAA Security compliance obligations. For instance, as part of your HIPAA Privacy compliance you should have established a sanctions policy that addresses disciplinary action for the improper use or disclosure of PHI, and implemented a training program for educating employees about the importance of protecting confidential health information. These policies can be easily modified to include HIPAA Security.

Larger employers also may have information security programs already in place. Because the standards in the HIPAA Security Rule generally are derived from industry practices in information security, your existing program may be sufficient to meet many of the requirements. However, you still need to document what is in place, assess any additional measures that may be necessary, and document how you have complied with each of the Security Rule standards.

CONSEQUENCES

Like HIPAA Privacy, the government regulators charged with enforcing the HIPAA Security standards have stated that they will take a "complaint based' approach to enforcement, and that they will emphasize voluntary compliance , such as working with covered entities to develop corrective action plans. On March 25, 2005, the regulators published information about how individuals can file a complaint regarding noncompliance with HIPAA Security and other rules. The Centers for Medicare and Medicaid Services (CMS) has authority to impose civil monetary penalties for violations with maximum penalties of $25,000 *per standard* violated.

CONCLUSION

Computer and information security likely will continue to be a hot topic, both in the press and in legislatures around the country. Informing yourself about HIPAA Security and taking the necessary steps will ensure your health plan is in compliance now, and also will help prepare you for additional regulatory requirements that may be forthcoming. It cannot happen without the involvement of your IT staff, but it is not a question for IT alone. Pull together a cross-disciplinary team with the appropriate knowledge base, take a step-by-step approach to compliance, and build on what you already have. IT consultants and/or legal counsel may be necessary to give advice on questions specific to your health plan.

—❖—