10 STEPS TO HIPAA SECURITY COMPLIANCE

Protecting your patients' health information is more difficult and more important than ever. The author's strategy will help you meet this month's deadline.

David C. Kibbe, MD, MBA

CME Covered in *FPM* Quiz

The final rule adopting HIPAA standards for the security of electronic health information was published in the Federal Register *on Feb. 20, 2003 [and goes into effect April 21, 2005]. This final rule specifies a series of administrative, technical and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.*

– Statement on the Centers for Medicare & Medicaid Services Web site regarding the Health Insurance Portability and Accountability Act[1]

As family physician Dan Brewer, MD, once wrote on an e-mail discussion list, "I believe I would rather eat live cockroaches than learn about HIPAA security." Nothing, it seems, could be more boring and less related to the practice of family medicine than computer security.

But don't be fooled into complacency. You and your patients are probably more familiar with security risks and the costs or hassles associated with inadequate protection than you realize.

Consider these examples:

- Have you ever been the victim of a computer virus, or do you know someone who has?
- Are you concerned about what would happen if the computer hard disk storing your patients' medical information failed?

Dr. Kibbe is director of the AAFP's Center for Health Information Technology (CHiT). He thanks Steven E. Waldren, MD, CHiT's assistant director, for his assistance on this article. Conflicts of interest: none reported.

ILLUSTRATION BY JOHN UELAND

SPEEDBAR®

You are probably more familiar with security risks than you think.

To learn whether your computer security meets HIPAA requirement, you should perform a "gap analysis" of your current setup.

As you move toward HIPAA compliance, it is important to document the entire process.

The goal of computer security in most cases is to prevent personal health information from being stolen, altered or destroyed.

• Do you worry that someone might eavesdrop on your wireless communications?

• Were you concerned when a major pharmaceutical company unintentionally distributed the e-mail addresses of hundreds of patients taking an antidepressant medication?[2]

In addition to helping raise your awareness of what's at stake, this article will make computer security more understandable and relevant to your practice, and put you on the path toward complying with the HIPAA security standards.

After reading through these 10 steps, you should be able to compare your office's current computer security, or lack thereof, with that required by HIPAA. This type of comparison is known as a "gap analysis" and is an important component of meeting the HIPAA requirements.

Also be aware that HIPAA security compliance is like a clinical encounter: If it's not documented, then it didn't happen. Therefore, document everything and make it part of a security manual.

1 Understand why computer security is important. If you need a simple answer to the question, "Why is computer security necessary and important?" the answer is "because everyone cares about the privacy and integrity of their health information." In most cases, the point of computer security is to prevent personal health information from falling into the wrong hands or being inadvertently altered or destroyed.

The HIPAA security standards apply to protected health information (PHI) that is either stored or transmitted electronically. PHI is health information in any form that personally identifies a patient. (For more on PHI, see an earlier security article I wrote for *FPM*: "A Problem-Oriented Approach to the HIPAA Security Standards," July/August 2001, page 37.)

These security standards will apply to you on April 21 if any of these situations exist in your practice:

• You use computers in the office to store and manage administrative or clinical information;

• You have a computer or network connected to the Internet;

• You use e-mail or other forms of electronic messaging inside and outside the practice.

The widespread use of computers, software and networks to exchange digitized data creates new vulnerabilities. It also reveals new dimensions to old risks. Much of the problem with computer security is of our own making, the result of our love of convenience and our drive to be more efficient. Computers automate routine, mundane tasks. By storing compacted, bite-sized information inside machines, we are able to collect data more easily and cut down on storage costs.

But computer storage devices can be broken or damaged, and the information in them can be erased or corrupted, exposing the data to unexpected change or loss. It is possible to steal thousands of medical records by downloading them onto a small storage device, which can easily be hidden in a pocket.

Similarly, we find networks of computers wonderfully convenient for sending messages across any distance at almost the speed of light. We delight in e-mail, file downloads and instant messaging. But the Internet has no borders or natural boundaries, making it easy for attackers to strike from a distance and to hide their whereabouts. Any time we connect our computers to the Internet, we instantly become vulnerable to new kinds of attacks, such as viruses and worms that can literally get inside our computers and alter, destroy or release confidential information.

One problem merits special mention. Computers have made the issue of identity much more problematic. People have always been able to use someone else's identity for criminal purposes, but the problem is exacerbated when we can't use a person's face, signature or other physical means to confirm their identity. How do you know the person

KEY POINTS

- Practices will need to ensure that their current computer security complies with the HIPAA standards that take effect April 21.
- Physicians should take responsibility for understanding how health information technology is used in their practice
- By taking a proactive approach to your computer security now, you will be able to detect and prevent trouble later.
- There is no one-size-fits-all approach for computer security.

sending you e-mail is truly the person he or she claims to be? How do you know the person whose name is attached to an electronic health record (EHR) entry really made it? It's difficult. Hackers use computer viruses to get into e-mail programs and propagate their nastiness by sending new e-mails that appear to come from a friend. As the public does more online shopping, identity theft using computers has become a common way for criminals to steal money and goods.

The bottom line is this: Computer security is a requirement for any sound business, including your medical practice. Computer security is needed to protect the privacy of those whose information you store and manage. It is also needed to protect you and your practice from the risk of penalty and legal liability if private information is used or released by your practice.

You have two choices: Either delay learning about computer security and risk playing catch-up when an attack or accident causes harm to a patient or your practice, or be proactive and begin to install protections that will allow you to detect and prevent trouble down the road.

2 Make certain your colleagues and staff take security as seriously as you do. The HIPAA security standards require your practice to have written security policies and procedures, including those that cover personnel training and sanctions for security policy violations. Your office staff and colleagues must truly understand basic security logic and take their role in protecting patients' privacy very, very seriously. Most security breeches occur when insiders – people working for the organization – exercise faulty judgment or fail to follow protocols in which they've been trained.

Consider two highly people-dependent areas of computer security: physical access and password management.

Physical access to computers and software is a foundation of computer security. Physical access means that someone can approach a computer or monitor and see what's on the screen. Do you want everyone in the office, including patients, family members or your cleaning crew to be able see what is displayed on a computer screen? Of course not. But you probably work in a busy, sometimes hectic, environment that makes it difficult to closely monitor the flow of people and information at all times.

This means two things. First, you should carefully consider the location and design of display devices in your office. Don't place monitors in busy corridors, and ensure that the display image has a 30-second time-out feature. Second, employees and staff must have a heightened awareness regarding access to computers, monitors, printers, fax machines and other display devices. They should strive to avoid creating insecure situations.

Password management is another area that requires staff to be security conscious. Passwords and IDs allow computers to control access to personal health information based on a person's role, authority or need to know. They identify or authenticate a computer user via a secret password. Obviously, passwords should be kept secret to avoid unauthorized access to or manipulation of protected information. But passwords are clumsy to use and difficult to remember, especially as they become more complicated (thus increasing their secrecy). It's tempting for users in small offices to share passwords or keep them written on a piece of paper tucked into the top drawer next to the computer station. I've even found passwords on sticky notes attached to computer monitors!

These actions completely undermine the security system. Why pay for a software system that uses passwords if you don't take the protection they provide seriously?

So while it does make sense to worry about hackers and intrusions from outside your office walls, remember that your co-workers pose the most likely security risk. Your computer security is only as

Your computer security is only as good as the weakest human link in your office.

SPEEDBAR®

In addition to protecting important data, computer security is also needed to protect you and your practice from the risk of legal liability.

Most computer security breaches occur when insiders exercise bad judgment or fail to follow established protocols.

Monitors should not be placed in high traffic areas, and time-out features should be used.

Computer passwords should never be shared or kept near the computer, even in small offices.

SPEEDBAR®

HIPAA requirements include a detailed description of how your hardware, software and network components collect, access, store and transmit patient health information.

The HIPAA security standards also require your practice to appoint a security manager.

Even if someone else is named as the security manager, physicians need to understand completely how health information technology is used in their practices.

The most important part of preparing for a disaster is having a backup system in place.

good as the weakest human link in your office.

3 Catalog all the information system components that interact with protected health information in your office. To assess your office's current security risk, you have to know, in detail, the capabilities and weaknesses of your information systems. No two medical practices have exactly the same information system components, nor do they manage the flow of information precisely the same way. Some practices still manage most information on paper and have a single computer for billing and accounting purposes. However, most practices, even small ones, have complicated information technology environments that include multiple components. These might include the following:

- Hardware – Computer workstations in the front office, tablet computers in the clinical areas, printers in the back office, server in the computer closet, personal digital assistants, scanning devices and modems used to connect to the Internet.
- Software – Operating systems, billing software, practice management software, browsers, e-mail client software, EHR software, and database and office productivity software.
- Network components – Routers and hubs, dedicated phone or cable lines, wireless systems, firewall software and firewall hardware.

You should make a detailed list of all of the components that play a role in either storing patient health information or transmitting it within the practice or to outside settings. You then need to create either a flow diagram or a detailed description of how this collection of hardware, software and network components collects, accesses, stores and transmits patient health information.

This detailed examination of your entire system is an important step for three reasons. First, it's required. HIPAA requires you to carry out such a risk analysis and base your new computer security policies and procedures on this analysis, which must be specific to your practice. Second, it's the only reasonable way to assess your risk of security breeches in your current systems and protocols. Finally, this exercise can be valuable in the acquisition and use of EHR systems if your practice is moving in that direction.

The HIPAA security standards require your practice to appoint someone as the security manager, so you might want to assign these tasks to that person. However, I can't stress enough the need for physicians to take responsibility for understanding how health information technology is used in their practice, especially small and independently owned ones.

4 Prepare for disaster before it occurs. An important aspect of computer security involves protecting electronic data from loss or corruption – that is, ensuring its integrity. Although there are many ways data integrity can be affected, the most common is loss of data from some sort of emergency or disaster, including human error, mechanical hard disk failure, equipment damage due to flooding, or computer virus infection.

A solid computer-system contingency plan is composed of a number of steps, including performing backups, preparing for continued operations in an emergency and recovering from a disaster.

The most important part of a contingency plan is having a backup system. A backup system is a combination of hardware and software that lets you retrieve exact copies of information if the originals become lost or damaged. There are several kinds of commonly used backup systems, including those that store data to tapes, compact discs or off-site devices. The equipment and service can cost from hundreds to thousands of dollars, and the best method for your practice can only be determined after you know how much data needs to be backed up. Your choice also will be influenced by cost, convenience and ease of use.

The most important part of a contingency plan is having a backup system.

At a minimum, your practice's backup

system should store all of the critical data needed to run the practice in the event of a disaster. Practices should conduct an analysis to identify these critical data.

5 Make sure your network and communications safeguards are intact and robust. It is increasingly difficult to find a computer that is not attached to some sort of network. Most computers in your practice are connected to the Internet, a particular kind of public network that has its special risks. Although network security is a complex subdomain of computer security, the basic threats and protective devices are not difficult to understand.

Networks work by routing packets of information among and between users at various computers. Generally, networks use devices known as routers to send the packets to correct addresses. Therefore, networks need to defend themselves against attacks from unauthorized users and from infiltration of unauthorized information packets through the routers.

Firewalls are hardware and software devices that protect an organization's network from intruders, such as hackers or data thieves. Think of firewalls as sentries at the boundaries of private networks and the public networks they are connected to: They check credentials, permit passage of authorized parties and communications, and keep a record of what crosses the boundary. Firewalls deny access to unauthorized users and applications, and they create audit trails or logs that identify who accessed the network and when. Firewalls may also issue alarms when abnormal activity occurs, such as a repeated unsuccessful attempt to enter the network.

6 Be certain that you have anti-virus software and keep it up to date. Even if you are in solo practice and use only one laptop computer for all your data capture, storage and transmission – and therefore may not require a network firewall – you probably connect to the Internet for e-mail and Web browsing. In terms of risk to your computer's data, connecting to the Internet is the most dangerous activity in which you can engage.

Malicious software, sometimes called malware, has become a familiar form of computer attack. Viruses, worms and "Trojan horses" are among the most common forms of malware that your computer security must protect against.

There is no single solution to the problem of computer viruses. Vigilance is essential.

Viruses can attach themselves to e-mails, program files and data files. They can infect all your hard disks and change or erase data while spreading to floppy disks and e-mails to infect other machines. Worms are self-replicating programs that attack networked computers. The now infamous Nimda virus was a worm spread via e-mail attachments named README.EXE. It affected a wide variety of operating systems, including several versions of Windows. Nimda was responsible for tens of millions of "denial of service" events throughout the Internet, in large part because it was able to attack key Web servers that direct traffic across the Internet. It is estimated that worms like the Nimda cost U.S. companies billions of dollars each year in repairs and lost productivity.

The solution to malware is installing and updating anti-virus software, available from specialized software companies, on all of your computers. Anti-virus software works by scanning digital data, such as incoming e-mails, files, hard disks and CDs, and then automatically deleting or isolating viruses. Anti-virus software programs are great at detecting known viruses but not so good at detecting new ones. New malware appears all the time, so anti-virus software needs to be updated frequently.

Viruses, especially e-mail worms, are the price we pay for universal connectivity and communications over open networks, especially over the Internet. There is no single solution to the problem of computer viruses, and the problem seems to be getting worse as more information is delivered over the Internet all the time. Vigilance is essential.

SPEEDBAR®

If your computer is attached to a network, you need to make sure that network is protected by a firewall.

Firewalls are hardware and software devices that protect an organization's network from unauthorized users.

Even if you are in a solo practice and don't require a network firewall, you most likely still need to install anti-virus software.

Anti-virus software needs to be updated frequently.

SPEEDBAR®

The HIPAA standards do not require e-mails to be encrypted.

However, the standards do require you to assess whether your practice's unencrypted transmissions of health information are at risk.

Encrypting e-mail can be tricky because both parties of the e-mail exchange need to be using compatible encryption products.

The HIPAA standards require your practice to obtain assurances from business associates that they will secure the electronic health information they create, maintain or transmit on behalf of your practice.

7 Understand what encryption will do and when it is necessary. Contrary to what many people are saying, the HIPAA security standards do not require e-mails, or any other transmission from a doctor's office, to be encrypted. The standards do require your practice to assess whether its unencrypted transmissions of health information are at risk of being accessed by unauthorized entities. If they are, you should consider some form of encryption.

The basic idea behind cryptography, of which electronic data encryption is a branch, is that a group needs to keep a message secret from everyone else and therefore encrypts it. Encryption is the transformation of a message from plain text into nonsensical cipher text before the message is sent. Anyone who steals the cipher text message will not be able to understand it. Only those who have the code used to encrypt the message can convert it back from cipher to plain text and reveal its meaning.

For several reasons, encryption is generally not employed for information stored on a computer's hard disk or transferred within an office's local area network. First, the risk of disclosure to unauthorized parties is small in the closed environment. Second, encrypting data is costly. Third, encryption generally slows down the movement of information within software applications and databases.

Here is a list of electronic data transfers and communications commonly used in a medical office that could be considered for encryption:

- Patient billing and administrative information exchanged with payers and health plans;
- Utilization and case management data, including authorizations and referrals that are exchanged with payers, hospitals and utilization management organizations;
- Patient health information gathered from or displayed on a Web site or portal;
- Lab and other clinical data electronically sent to and received from outside labs;
- Word-processing files used in transcription and other kinds of patient reports that are transferred electronically;
- E-mails between physicians and patients, and between attending and referring physicians and their offices.

Encryption of e-mail messages merits special attention because e-mail is so common. Many patients enjoy direct online communications with their physicians via e-mail. The problem, of course, is that e-mail is the digital equivalent of a postcard. Anyone handling the message can easily read its contents. It doesn't even have an envelope! And e-mails are susceptible to forgery. How do you know for sure that the person listed in the "from" field of an e-mail is the person who actually mailed the message?

The problem with encrypting e-mail is that both parties of the e-mail exchange need to be using compatible e-mail encryption products. This is clumsy and, so far, rarely used. More commonly, encrypted e-mail message exchanges occur when both parties agree to use a secure server or portal system that requires both parties to use passwords and IDs to log on. The AAFP has a partnership with Medfusion that permits AAFP members free use of such a secure portal system for messaging with patients. For more information, see http://www.aafp.org/x23273.xml.

8 Consider chains of trust and your business relationships. Your practice shares security concerns with any businesses that are involved in the electronic transmission of your patients' information. In effect, the security capability of insurance companies, transcription and billing services, hospitals, labs and Internet service providers is your concern.

"Chain of trust" is a concept used in the computer security field to describe the contractual agreements made between parties to assure that the confidential information they share remains secure throughout its journey. There is no standard set of obligations for chain-of-trust agreements. However, such agreements obligate both parties to adopt a form of strong authentication such that data transmissions are attributable and nondeniable. (Otherwise, one party or the other could claim not to have received an important piece of information sent electronically.)

The HIPAA security standards require your practice to obtain assurances from business associates that they will implement the necessary safeguards to protect the confidentiality, integrity and availability of the electronic health information they create, maintain or transmit on behalf of the practice.

The important issue here is to "know thy

business partner." Every entity with which you share information electronically is an extension of your practice, whether you want them to be or not.

9 Demand that your vendors fully understand the HIPAA security standards. As you become better informed about computer security and the HIPAA security standards, you will realize the extent to which compliance makes you dependent on hardware, software, network and other information technology (IT) vendors. Their products and services, whether out-of-the-box computer hardware or hands-on-in-the-office IT services, will enable you to meet many of the security standards – or not.

A good example is the requirement for audit controls. Audit controls that permit you to record and examine activity in information systems can require a combination of hardware, software, network and procedural mechanisms to act in concert. If these components have been purchased from separate vendors, it might be necessary to coordinate their setup and configuration to meet the audit control requirement of the HIPAA security standards. Who will perform this coordination in your office?

work more closely with the vendor to ensure that all the facets of your computer system satisfy your practice's HIPAA security plan. Some EHR vendors will even help you do a gap analysis as part of their purchase program. But because most EHR vendors don't install the hardware and networking components, your choice of a local contractor for these services should be made with HIPAA in mind. Be certain that your local contractor is fully aware of the HIPAA security standards and is willing to assist you before you proceed.

10 Start with a plan – and the end – in mind. My hope is that after reading to this point you have a much better idea of the breadth and scope of the HIPAA security standards, and that you are better prepared to tackle the task of assessing your practice's current state of computer security. There are some excellent tools that can assist you in performing a gap analysis for this purpose without having to hire a consultant. (One place to start is the Needs Assessment page on the CHiT Web site, available at http://www.centerforhit.org/x69.xml.)

Remember that there is no cookbook or one-size-fits-all approach for computer security. What counts is being "reasonable and appropriate" when matching security measures with the level of risk that pertains to your situation. These 10 steps should help you recognize a number of places where your organization's computer security could be improved and where some deficiencies might be easily addressed. FPM

Send comments to fpmedit@aafp.org.

It might be a fortunate coincidence that the HIPAA security standards have been mandated just as many family physicians are acquiring EHRs.

It might be a fortunate coincidence that the HIPAA security standards have been mandated just as many family physicians are acquiring EHRs for their practices. Many are choosing integrated EHR systems – that is, products that include billing, scheduling and clinical information software from the same vendor. This integration can greatly simplify meeting the HIPAA security challenge – if you select the right EHR vendor. (To see EHR reviews by your colleagues, check out the AAFP's Center for Health Information Technology (CHiT) Web site at http://www.centerforhit.org/x290.xml.)

A single-vendor solution for small and medium medical practices allows you to

1. Available at: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp. Accessed March 4, 2005.

2. O'Harrow R Jr. Prozac maker reveals patient e-mail addresses. *Washington Post.* July 4, 2001:E1.

SPEEDBAR®

The integration offered by some EHRs can simplify your practice's effort to comply with the HIPAA security standards.

Some EHR vendors will help you do a gap analysis.

If you are thinking about converting to an EHR, be sure that your hardware and networking contractor is aware of the HIPAA standards before proceeding.

There is no one-size-fits-all plan for computer security.