A Problem-Oriented Approach to the HIPAA Security Standards

Every practice will have to comply with HIPAA. You can take the first step by performing a self-audit of your practice's current security measures.

David C. Kibbe, MD, MBA

CME

S: Physicians and others in health care complain of being anxious and confused about the costs and hassle of complying with the privacy and security standards in the Health Insurance Portability and Accountability Act (HIPAA). The discomfort is intensified when listening to lawyers discuss HIPAA in the media and at compliance seminars. Awareness of the discomfort is very recent, but its duration is expected to last several years.

O: A wide gap is noted between the level of office security required by HIPAA and that found in most medical practices. A large number of consultants and "experts" are noted moving into the area. Conspicuously absent is any systematic approach that will decrease the discomfort. A new avoidance reflex, associated with acute inflammation of the regulatory gland, has appeared.

A: HIPAA-titis.

P: Read this article. Approach HIPAA security standards in a systematic manner, starting with a self-audit of your practice's current security measures. Then, concentrate on closing the gap where the security risks and the benefits of addressing them are highest.

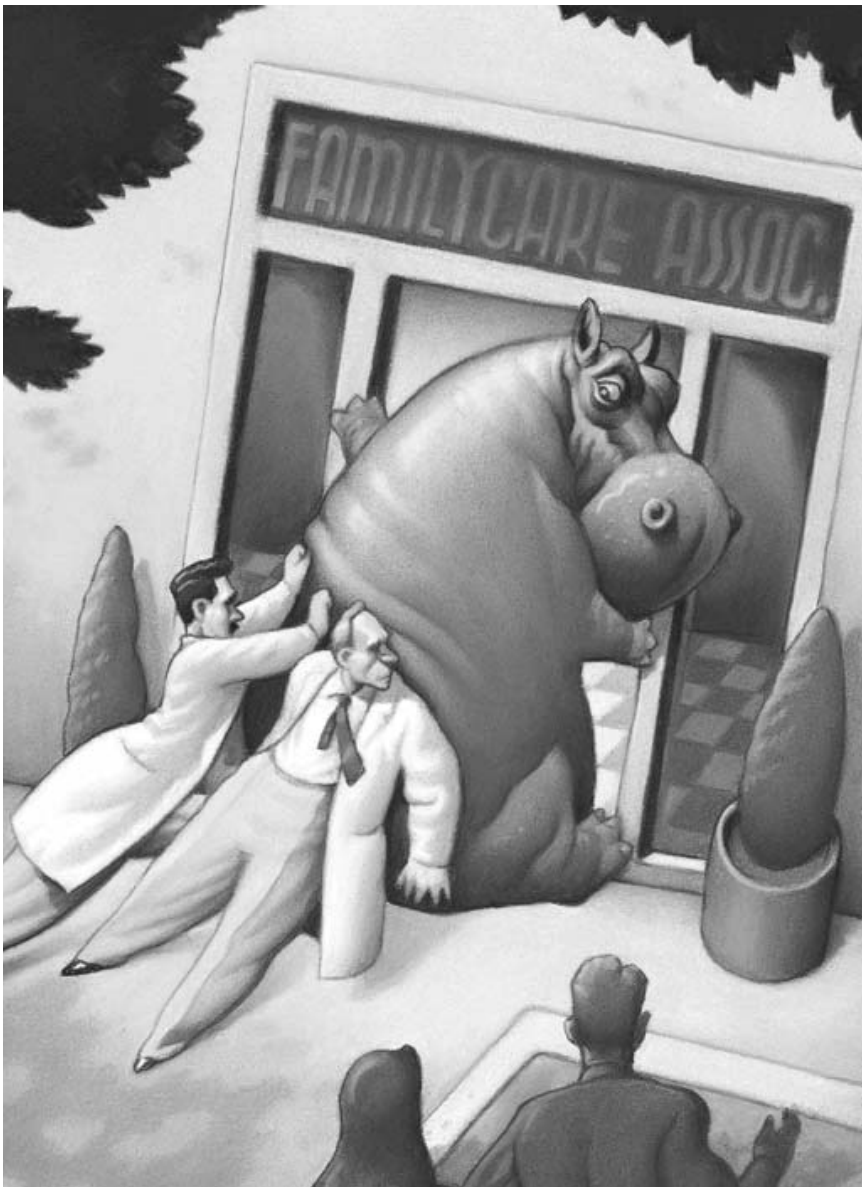

ILLUSTRATION BY GREG TUCKER

Dr. Kibbe is a family physician and is chair and co-founder of Canopy Systems Inc., an Internet clinical software application and services firm based in Chapel Hill, N.C. He is also a contributing editor to Family Practice Management. *Conflicts of interest: none reported.*

SPEEDBAR®

There's a wide gap between the proposed HIPAA security regulations and the level of security found in most medical practices today.

According to the author, the best way to approach HIPAA's many security mandates is to use the same problem-oriented approach you use to evaluate patients.

To assess how much your practice may have to do to comply with the proposed HIPAA regulations, conduct a self-audit of current security measures.

Practices will have two years to comply with the HIPAA regulations once the final rules have been published.

Clearly, a sense of humor is necessary in the treatment of HIPAA-titis. But the HIPAA security regulations pose such an overwhelming challenge to medical practices' way of doing things that you'll need more than humor to get your practice through the next couple of years.

In this article, I suggest that the best way to approach HIPAA's many security mandates is to break them down into manageable categories and tasks. The familiar problem-oriented approach you use to evaluate patients' medical problems can be helpful as you assess your current security situation and prioritize what needs to be done to meet the HIPAA challenge. The idea is to manage HIPAA compliance the same way you solve your patients' problems – one at a time and as the result of careful examination, diagnosis and, where necessary, consultation.

The best way to approach HIPAA's many security mandates is to break them down into manageable categories and tasks.

First things first

HIPAA is actually three sets of standards (transactions and code sets, privacy and security) developed by the Department of Health and Human Services at the behest of Congress, which passed the HIPAA legislation in 1996. The goals of the standards are to simplify the administration of health insurance claims and lower costs; give patients more control and access to their medical information; and protect individually identifiable medical information from real or potential threats of disclosure or loss. Every practice, regardless of size, has two years from the date the final rules are published in the *Federal Register* to comply. And the clock is ticking. The final rules for transactions and code sets were issued last fall, and the privacy regulations took effect after a brief delay this spring. Only the final rules for the security standards have not been published, and they are expected by the end of the year.

Privacy and security are closely linked, so it's important at the outset that you understand the difference:

KEY POINTS

- Every physician, every practice and every health care entity that handles protected patient health information will have to comply with HIPAA regulations.
- Complying with the security standards will require most practices to adopt new policies and procedures and to make hard choices about implementing and enforcing them in a manner that's "reasonable and appropriate."
- Begin your compliance efforts by doing a self-assessment of the security measures already in place in your practice.

Privacy is the patient's right over the use and disclosure of his or her own personal health information. Privacy includes the right to determine when, how and to what extent personal information is shared with others. The HIPAA privacy rules grant new rights to patients to gain access to and control the use and disclosure of their personal health information. [For more information, see "What You Need to Know About HIPAA Now," *FPM,* March 2001, page 43.]

Security is the specific measures a health care entity must take to *protect* personal health information from unauthorized breaches of privacy, such as might occur if information is stolen or sent to the wrong person in error. Security also includes measures taken to ensure against the loss of integrity of personal health information, such as might occur if patients' records are lost or destroyed by accident. The HIPAA privacy rules require general security measures be put in place, and the proposed security rules prescribe a detailed and comprehensive set of activities to guard against unauthorized disclosure of personal health information stored or transmitted electronically or on paper.

Your practice does not have to invest in Fort Knox-type security to comply with HIPAA.

There's one more definition that will help you as you learn about HIPAA:

Protected health information (PHI) is the HIPAA term for health information in

any form (i.e., paper, electronic or verbal) that *personally identifies* a patient. This includes individually identifiable health information in paper records that have never been electronically stored or transmitted. It does not include data that have been "disidentified" by removal of identifying information, such as name, address, ZIP code, etc. Generally, the proposed security regulations will apply only to PHI. And while the security regulations are likely to change somewhat during the two years leading up to the implementation deadline, I suggest that you begin your compliance efforts now by assessing how PHI may be vulnerable to loss or misuse in your own practice.

Use "reasonable and appropriate" as your guide

Physicians have always honored patient confidentiality, the ethical principle that communication between a patient and his or her physician should not be shared without the patient's consent, or unless required by law.

> **Most of the security components prescribed by HIPAA are already being used by other industries, such as retail and banking.**

Under the HIPAA security regulations, this principle is extended to include the physical office environment, office staff and computer equipment. The proposed HIPAA security regulations are long and complex and are written in "security speak," but they clearly stress that the security measures you adopt be "reasonable and appropriate." Your practice does not have to invest in Fort Knox-type security to comply with HIPAA. In fact, because most of the security components prescribed by HIPAA are already being used by other industries, such as retail and banking, you won't have to reinvent the wheel. The bad news is that even basic security measures are new to the health care industry, generally considered to be 10 years to 15 years behind other industries with regard to security.

For a number of reasons, most practices have not developed a program to protect the PHI stored in their offices or to prevent accidental or purposeful disclosure of PHI by employees. Under HIPAA, all health care entities will be required to develop and document a security program to guard PHI against real and potential threats of disclosure or loss. This will include administrative policies and procedures and safeguards to protect PHI stored on your computer system and in your physical office space. A good way to begin developing a security program is by first evaluating the security measures already in place in your practice. Remember to use "reasonable and appropriate" as your rule of thumb.

Don't wait to begin your self-audit

Assessing your practice's current security need not be complicated or expensive. It's relatively easy to think through the most obvious security safeguards in your practice (or their absence). Begin your self-audit by documenting all the things you already do to safeguard PHI. Certainly every practice has locks and keys to prevent intrusion and theft. Your practice may also have a sprinkler system to protect the integrity of paper records, computer systems and other equipment from fire. If your practice is computerized, you probably use passwords or other means to control access to electronically stored PHI, to monitor information use and to prevent unauthorized persons from viewing information they are not meant to see. When an employee quits or is fired, you may routinely change locks or combinations and remove the employee's password and identification from the computer system. Make a list of these and any other security measures you are using in your office.

When you think you've documented all of your current safeguards, take a look at them again from another angle. Think of the PHI in your practice as a valuable asset in need of protection and begin to consider how it might be lost, stolen or damaged. Ask yourself the following questions:

- How does PHI flow in my practice?
- How and where is it stored?
- Who handles it?
- What's the protocol when a new employee joins the practice?
- What measures do we have in place to safeguard PHI when an employee leaves?
- Who has keys to the office?
- Who in the practice is responsible for the medical records and computers?

HIPAA will require that you name a security officer, so now is the time to think about

SPEEDBAR®

The HIPAA regulations are actually three sets of standards: transactions and code sets, privacy and security.

The final rules for privacy and transactions and code sets have been published. The final security rules are expected to be published by the end of the year.

Under HIPAA, health care entities must take specific measures to guard protected health information (PHI) from unauthorized disclosure.

PHI is information in any format (paper, electronic or verbal) that personally identifies a patient.

SPEEDBAR®

All health care entities will be required under HIPAA to develop and document security programs to guard PHI against loss or unauthorized disclosure.

The proposed regulations clearly stress that these security measures be "reasonable and appropriate" in nature.

Don't wait for the final security rules to be issued. Start now by documenting what security measures your practice already has in place.

To make the task easier, focus on three major categories: administrative procedures, physical safeguards and technical security.

assigning this task to a very responsible member of your staff (or taking this responsibility on yourself).

You will also find it helpful at this point to create a high-level flow diagram of how PHI is created, stored, transmitted and disposed of from the time patients enter your practice, through the course of treatment and during the referral and payment processes.

A basic self-audit consists of asking yourself common-sense questions about how you and your staff currently handle PHI.

The impending HIPAA regulations are a powerful incentive for you to perform an audit of your practice's security. And as I've outlined above, a basic self-audit consists of asking yourself common-sense questions about how you and your staff currently handle PHI. (If you want to conduct a more structured, formal self-audit than what's described here, there are HIPAA self-assessment tools to assist you. See the list of tools and other resources below.) To make the task more manageable, I suggest taking a closer look at the three major categories of the proposed HIPAA security regulations (administrative procedures, physical safeguards and technical security) using a problem-oriented approach, addressing the largest category – administrative procedures – first.

Administrative procedures

There is no doubt that the administrative procedures section of the proposed HIPAA security rules is complex and multifaceted: there are 12 subsections. However, some administrative procedures are likely to be more relevant and of higher priority to your practice than others. I suggest you direct your initial compliance efforts to three areas, using what is "reasonable and appropriate" as your guide: contingency planning, information access controls and staff training.

HIPAA RESOURCES FOR SMALL PRACTICES

Articles

"What You Need to Know About HIPAA Now." Kibbe DC. *FPM.* March 2001:43. Available online at www.aafp.org/fpm/20010300/43what.html.

"Understanding HIPAA Transactions and Code Sets." Rode D. *J AHIMA.* Jan. 2001;72:26-32. Available online at www.ahima.org/journal/features/feature.0101.2.html.

"What Physician Executives Need to Know About HIPAA." Fitzmaurice JM, Rose JS. *The Physician Executive.* May/June 2000;26:42-49. Available online at www.ahcpr.gov/data/hipaa1.htm

Web sites and compliance tools

The Maryland Health Care Commission Web site (www.mhcc.state.md.us) offers a concise overview of the HIPAA privacy standards. Its *Guide to Privacy Readiness* designed to assist small facilities and practitioners with the HIPAA privacy regulations also includes a checklist of items for meeting HIPAA privacy regulations. It is currently in the draft stage and should be available shortly.

The Massachusetts Medical Society Web site (www.massmed.org/pages/hipaa_impact.asp) includes a suggested HIPAA implementation planning schedule and tracks the status of pending HIPAA regulations.

The North Carolina Healthcare Information and Communications Alliance Web site (NCHICA) (www.nchica.org/HIPAA/HIPAA_intro.html) provides links to major online HIPAA resources and "HIPAA Early View," a gap-analysis tool for large organizations ($150). (The small practice version is in development and scheduled for release within 45 days of publication of the final HIPAA regulations for security.) The site also includes guidelines for implementing the HIPAA regulations and other educational information.

The Privacy and Security Network Web site (www.privacysecuritynetwork.com/healthcare/default.cfm) includes "HIPAA Calculator," a gap-analysis tool, and an example contract to help with HIPAA compliance.

The U.S. Department of Health and Human Services Web site on Administrative Simplification (aspe.os.dhhs.gov/admnsimp) has links to all of the HIPAA regulations (both proposed and final) as well as summary and background materials.

The Utah Health Information Network Web site (www.uhin.com) includes a glossary of HIPAA terms. "USET," a software tool to educate small practices about the basic security standards and help them write policies and procedures is expected to be released by the end of the year.

Contingency planning. Contingency planning simply means describing the formal processes your practice uses to analyze and inventory the types of data that are stored electronically and how you protect the integrity of that data in the event of emergency, disaster or theft.

There is little question that it is good business practice to have the ability to recover quickly from a system failure of any kind. Under HIPAA, you'll need to document how electronically stored and transmitted PHI is safeguarded. Your practice, like many others, probably uses a computer for some aspects of practice management, for accounting purposes, for writing letters and storing written documents, and for both internal and external e-mail messaging. Some of you may also have electronic medical records systems. As you begin to think about documenting or improving documentation of your procedures, ask yourself the following key questions:

- Is all of the computing hardware and software that is used to process PHI inventoried and documented somewhere?
- Is there a written procedure for backing up data containing PHI? Will the procedure enable us to recover exact copies of PHI if the original data are lost?
- Is there a written disaster recovery plan and a plan for operating in an emergency in the event of fire or system failure?

Information access controls. The HIPAA security regulations will require you to clearly define who in the practice has access to PHI, the rules determining a person's right of access, and the reasons for denying access to some individuals.

Controlling access to PHI is a basic security measure. It is also one of the areas most vulnerable to security breaches. Most software programs allow you to configure access control so that, for example, physicians and nurses are able to read and edit documents, but other staff members can only read them. Access controls are important to consider when a person's role or job changes.

Some key questions to consider when developing and documenting a plan for access control in your practice include:

- Is there a written policy (or policies) that describe who has access to PHI? Does it define circumstances under which access is granted (e.g., right-to-know, need-to-know)?
- Is there a process for changing or revoking access if a staff member leaves or changes positions?
- Is there a policy for providing access to PHI to other entities, such as law enforcement, public health or law firms?

Staff training. HIPAA security regulations will require that you provide staff members with training and education about handling PHI. This basic-level security training should include measures such as password management, virus protection and monitoring of logs and audits. You'll probably agree that it is "reasonable and appropriate" for your staff to know about and understand basic HIPAA security issues before they start handling PHI or before they log onto computers storing it. Key questions to ask about staff training include:

- Does staff currently receive training about safeguarding PHI?
- How often should reminders and refresher courses be provided?
- Does the training content meet all the HIPAA training requirements, such as user education in password management?

Of course, until the final security rules are released you won't know whether your training meets HIPAA requirements. But at this point you *should* be aware that all compliance training is not equal. For example, I've been at HIPAA seminars run by lawyers who view HIPAA strictly in terms of the law or as a means of getting your business. They fail to take into account what is "reasonable and appropriate" in a health care setting and, as a result, end up really scaring people. So always consider the source. I've read the proposed security rules more than once. They won't demand the impossible of you.

> **I've read the proposed security rules more than once. They won't demand the impossible of you.**

Thinking your way through these issues and taking notes on what security measures your practice already has in place, what you need to do to minimize security risk and what you don't have enough understanding or information about to analyze, will not make your practice HIPAA compliant. But it is an effective and organized way to start. And, should anyone ask, it indicates your

SPEEDBAR®

Under administrative procedures, focus on contingency planning, information access controls and staff training.

Think about and begin documenting your practice's procedures for safeguarding PHI in the event of an emergency, disaster or theft.

The proposed HIPAA security regulations will require you to clearly define who in the practice has access to PHI and for what reasons.

Staff members will need to know about and understand basic HIPAA security issues if they handle PHI or log onto computers storing it.

SPEEDBAR®

To assess your practice's physical safeguards, focus on areas where PHI is most vulnerable: in medical records storage areas and at fax machines and workstations.

Begin by writing down everything you currently do to prevent unauthorized persons from gaining access to your patients' PHI.

Technical security (i.e., protecting the privacy and integrity of electronically stored or transmitted PHI) is probably the easiest HIPAA mandate to implement.

Start checking with your software vendors now to inquire about audit-tracking capabilities and to make sure they are working toward HIPAA compliance.

serious intention to decrease the security risks in your practice.

Physical safeguards

Physical security requires that you think carefully about who, besides your staff, has access to your practice's PHI. Keeping in mind "reasonable and appropriate" as the rule of thumb, I suggest focusing on three main areas where physical security is most vulnerable: medical records storage areas, fax machines and workstations. Here again, you may already have policies and procedures to prevent unauthorized persons from gaining access to your patients' PHI. For example, you might have a shredder for destroying paper medical records that are duplicates or are no longer needed. Your practice may house its computer servers and fax machines in a locked room that is keyed separately and away from public traffic flow. Or, you may already keep a log of the maintenance work done by outside contractors on office equipment that handles PHI such as computers, fax machines and copiers. All these measures should be written down as part of your overall security plan. Additional questions to ask include the following:

- Is there a policy to keep PHI out of view at workstations and on computer screens, for example by having the computers set to automatically log out users after a few minutes of inactivity?
- Are workstations for staff that handle PHI set up so that people passing by cannot easily view computer monitors?
- Do all of the practice's computer programs require a password and identification to log in, or is it possible to access some PHI without them?
- How are computer equipment, backup tapes and storage devices accounted for when they are removed from the office (i.e., when they are out for repairs or when the backup tapes are taken to their off-site repository?) Is there a log?
- How easy or difficult is it for people passing by to view documents that are being faxed, printed or copied?
- Are printed versions of PHI left unattended in public areas of the practice?
- What procedures are in place for disposing of PHI, both in paper and electronic format?

Unmanned workstations in public areas are an open invitation to violate privacy and security. PHI should be protected from public viewing to the extent possible, for example by having computer screens automatically time out after a few minutes of inactivity to ensure that no unauthorized users view or enter data. Fax machines should be given the same consideration. The content of faxes should never be left unattended or out in a place where unauthorized people could view them. Make a list of all the people who have physical access to your practice's computers or computer room, and ask yourself these questions:

- How easy or difficult would it be for someone to copy patient records onto a floppy disk and walk out of the office?
- Who has access to the backup tapes on a daily or weekly basis?

Technical security

Due to the proliferation of Internet security software and devices, this area, although complex, will probably be the easiest of all the HIPAA security mandates to implement. Passwords, identification, digital signatures, firewalls, virus protection, virtual private networks and encryption are standard measures to protect the privacy and integrity of information flowing within and between computer networks. However, there is no guarantee that the current state of your computing environment, the connections between your office and the local hospital or the virus protection software you use in your office today will be adequate under HIPAA. Because technology is changing rapidly in response to the widespread use of the Internet and increasing concerns about privacy, the whole area of technical security mechanisms is something of a moving target.

Technology won't guarantee security. Even the very best technological security features are worthless in the hands of poorly trained or unmotivated staff. Take a moment to notice what a small portion of the HIPAA security regulations deals with technology. As any security expert will tell you, this is because humans and our behaviors pose most of the risks to security.

Begin your compliance efforts by creating a list of your hardware and software vendors. Include your Internet service provider (e.g., America Online or EarthLink) if you have one. (If you have Internet access from your local area network, your computers and their data are potentially vulnerable to attack

from anywhere on the World Wide Web.) Also include any dial-up connections that, for example, allow you to reach a hospital and any dial-up capability that allows outside users access to your computers.

Again, using "reasonable and appropriate" as your guide, consider how you monitor or audit activity on your computer and fax systems. For example, say you needed to go back and see who accessed or changed data on a patient on a particular day. Perhaps a computer report was faxed to the wrong entity, a patient complained and you need to understand how the error occurred. (Error monitoring of this kind will be a HIPAA requirement.) The proper use of passwords and identification is critical to audit accuracy. If your staff members share passwords or identification, you won't be able to identify which user logged onto the system with any degree of certainty. You must also determine whether your software has the ability to produce audit reports (referred to as "logs" in the security regulations) of an event in question. In the scenario I just presented, the event in question would be the identity of the person who accessed a particular patient's information on a certain day. Ask your software vendors to explain their products' audit-tracking capabilities and start checking in with them now to make sure they are working toward HIPAA compliance.

Here are some other questions to ask yourself and your vendors about technical security:

- How can we tell if an unauthorized user accessed PHI through the practice's computers and/or networks? What safeguards are in place to prevent unauthorized access?
- What activities need to be monitored and logged, and what level of detail is reasonable and appropriate?
- What technology is in place to assure the true identity of (i.e., to "authenticate") users? What about passwords and IDs? Digital signatures? Telephone callback?
- How often does the system issue prompts to change passwords? Has staff been trained to create hard-to-break passwords?
- How much risk of message interception or unauthorized access to PHI is posed by the practice's use of wide-area networks or the Internet?

A word of caution: The information technology environment of even small medical practices is changing very rapidly. The use of multiple computers and servers, palm-top devices that connect to personal computers, connections to the Internet and remote applications are becoming more common in medical practices. Threats to data integrity and data transmission in this environment are real but widely misunderstood. No one can be certain of the absolute level of risk to PHI. Talk to your vendors about the potential risks in your practice, but if you don't have any real worries about your data integrity, don't spend a lot of money addressing these risks. Also, be wary of consultants and software vendors who tell you that your risks are great and can be minimized by spending a lot of money on their products!

> **It's time to pay attention to and begin treatment for HIPAA-titis before it becomes an acute medical management emergency.**

Meeting the challenge

Keep in mind that you will have two years from the date the final HIPAA security rules are released to reach compliance. There is no need to panic or to spend a lot of money hiring a consultant to audit your practice. By reading this article, you've already begun to build an awareness of the proposed HIPAA security standards and what the regulations will require of you and your staff. Now is the time to begin a thoughtful analysis of the swirl of personal health information your practice is responsible for, and to assess how this information may be vulnerable to loss, damage or misuse. The standards have basically been set for safeguarding PHI. It's time to pay attention to and to begin treatment for HIPAA-titis before it becomes an acute medical management emergency. FM

Editor's note: Information about the HIPAA security regulations in this article is based on the proposed HIPAA security rules published in the *Federal Register* in August 1998. The final security rules are expected to be published by the end of 2001.

Send comments to Dr. Kibbe at fpmedit@aafp.org.

SPEEDBAR®

There is no need to panic, hire a consultant or to spend a lot of money trying to comply with the proposed HIPAA security regulations.

Begin building an awareness of the proposed security regulations and what they will require of you and your staff.

Assess how the PHI in your practice is currently being safeguarded and how it might be vulnerable to loss, damage or misuse. Document these safeguards.

This will prepare you for the additional steps you'll need to take to comply with HIPAA once the final security rules have been published.