HIPAA Final Security Rule Overview

The final HIPAA Security Rule proposes standards for the security of electronic individual health information for use by covered entities. As a physician, you must use these standards to develop policies and procedures that will maintain the security of your patients' electronic individual health information. (Note: The final rule does not outline a specific electronic signature standard as originally proposed; this is forthcoming in a separate regulation. This course includes discussion of electronic signatures, however, as it is important to start integrating them into your security policy.)

One of the important parts of HIPAA is the designation of a security officer. In a large organization, this job likely will fall on either the computer network administrator or a physician who happens to be skilled with information systems. In a smaller organization such as a solo or small group practice, this job likely will fall on a physician or office manager, neither of whom may be very experienced with computers. Unfortunately, HIPAA mandates fines of up to $250,000 and imprisonment for up to 10 years for severe violations. Thus, choosing and educating a competent security officer is vital.

Fortunately, HIPAA is designed to be scalable. For a one-physician office practice, the HIPAA Security Standards may require no more than proper use of security software and a couple of pages detailing where you keep the backup computer discs. Large entities such as hospitals and physician provider networks, however, may need reams of written policies, complex security software, and regular outside audits by third-party consultants.

Contingency Plan

Every computer system must have a documented and audited backup and full recovery plan in case of an emergency. The initial step in developing the plan is to assess applications and data to determine what is critical to daily operations. The plan must include an emergency operating procedure to use until systems can be placed back online and testing procedures to ensure a system can be restored fully from backups.

Without this plan in place, your practice can and will fall prey to a number of debilitating situations. Natural disasters, power outages, computer viruses, or even a simple program crash could shut down permanently any organization that is not prepared.

The plan also must address how your practice handles backup media, as doing so in an insecure manner could give an unauthorized person complete access to your computer system's files. You must store all backups in a secure location, and it should be off-site; otherwise, a fire could wipe you out completely. Typical backup storage locations are on a remote server, in a bank deposit box, or at a remote building under your control.

You should not store backup media near the primary data. This could lead to a total loss of data if a major disaster occurs, such as a fire or terrorist attack.

Secure Records Processing

To keep a patient's record confidential and secure, a formal and documented policy must govern the handling and processing of patient records in your practice. You should set up procedures for the creation, receipt, handling, storage, destruction, and transmission of records to reduce the chances that they become lost or inadvertently disclosed. Without processing standards in place, for example, records could be left in compromised locations or computer screens could end up within line of sight of patients. Both of these situations could lead to problems if an unauthorized individual inadvertently viewed a patient's record.

Information Access Control

Security in any computer system requires formal policies and procedures for granting and controlling access to available resources. Your practice should develop specific criteria for granting defined levels of access to all users and adopt the required mechanisms to maintain access control.

Before you grant a user access to your practice's computer system, you must determine his or her level of access based on job role and the information that person needs to get the job done. For example, a billing department employee will need access to a patient's financial information as well as scheduling information to determine when the next office visit is due. On the other hand, a receptionist might need access only to the scheduling system; if the receptionist in your practice has no reason see the financial or personal medical data of patients, you should establish a method to restrict his or her access to that data.

Note that in the HIPAA final rule, the term "access control" was removed as being too narrow. Nevertheless, access controls will form the basis of your HIPAA security plan, so it is important that you understand them.

Internal Audit

Auditing also is an important part of any secure system. Through the regular review of system logs, procedures, and incidents, you can learn about security risks and even potential system compromises. Therefore, your practice must have an internal auditing policy with guidelines and standards to regulate auditing tools and procedures. Note that in the HIPAA final rule, "audits" have been renamed "information system activity reviews." However, it is more practical to stick with the industry standard term, "audit," when developing your policies.

You must perform two main types of audits:

- **Reactive audits** can detect events that already have occurred, such as failed login attempts. By performing internal audits on log files, an administrator can determine if a system has been compromised, and in the case of a successful attack, use the audit to determine how the attacker gained access to the system.

- **Proactive audits** are valuable to prevent possible problems. For example, a proactive password audit can quickly uncover weak passwords or poor password creation policies. By using the same tools and techniques an

attacker would use, an administrator can detect and then close off weak spots in the computer system. A little preventive maintenance in the form of an audit can help reduce the risk of a successful attack.

Audits can be both reactive and proactive. The former is useful when an incident already has occurred; the latter will allow an administrator to correct a potential problem before it becomes an incident. Each has its place, and both are equally important.

Personnel Security

All personnel who deal directly with confidential health information must have an appropriate security clearance to help prevent unauthorized, inadvertent access to sensitive data.

To properly manage personnel security, you should create set of written procedures that outline how your practice grants and controls system access and how it trains employees in personnel security. In addition, you must diligently maintain a record of who has access to information and how much access each person has. For example, you either should assign maintenance personnel to an appropriate level of security, based on a set of pre-qualifying criteria, or arrange for someone with the proper clearance to chaperone them when they need access to a secure area, such as a patient file room.

Security Configuration Management

Every computer system requires a documented method for maintaining a secure configuration. Your practice should adopt procedures for installing new hardware and software, upgrading existing hardware and software, controlling inventory, and testing security. An employee not adhering to such procedures could install a third-party program (such as a computer virus) that might allow an attacker access to the computer system.

Security Incident Response

In the event that a computer system is compromised, you should have a documented plan in place that outlines your immediate response. The plan should include procedures for reporting, monitoring, or, if necessary, isolating the compromised system. Without a formal response plan, an employee inadvertently could warn a computer hacker that the hacker has been detected. Unfortunately, once hackers know they have been detected; they often will delete the files on the compromised computer to cover their tracks. In doing this, a hacker might not only remove evidence of intrusion but also destroy your computer system.

An employee who suspects his or her account has been hacked or the computer system compromised should STOP working and discreetly alert the appropriate personnel. Attackers usually monitor a compromised system for indication that they were detected. If the attack is from within the organization, even a suspicious physical action by the targeted user (e.g., a shout or warning yell) could be enough to tip off an attacker. You must train

all employees how to respond to a security incident.

Security Management Process

Due to the complex nature of controlling a computer system, your practice should have an explicit security management process that outlines the steps required to create, implement, and enforce all security policies. Without a management process, it is highly likely that any security measures put in place will degrade over time. Issues such as patches, risk assessments, personnel security, and more are dynamic. You will need to update the policies by which your practice manages each of these issues to reflect personnel, corporate, legal, hardware, or software changes that impact the effectiveness of your security.

Termination Procedures

Personnel changes create a gaping security hole in many computer systems. When an employee is hired and assigned a security level, he or she receives access to numerous systems and programs. Your practice might provide the new employee everything from security access cards to voice mail passwords. However, if you do not remove each of these items when the employee leaves, he or she, as an ex-employee, could get back into the system to cause harm. This type of retaliation occurs regularly, and it often results in an embarrassing situation for the compromised organization. For this reason, each time an employee is dismissed, you should follow a formal, documented procedure that also covers the actual dismissal actions. Even if an employee is to leave voluntarily, it may be in the best interest of the practice to monitor all outgoing e-mail or to restrict the user to a tightly controlled environment to limit theft or digital vandalism.

Testing

Before you put a policy into effect, you should test the standards and procedures of its implementation to ensure that they work and do not inadvertently disable or violate another policy. In addition, you should periodically test existing security measures to be certain they remain effective, especially in the event of a system change. Your practice should create a documented policy to ensure that proper system testing occurs.
For example, if you decide to update an Internet use policy to state that all peer-to-peer sharing programs will be disabled, the person in charge of the Web monitoring software would have to define a rule, then implement and test it using a step-by-step procedure. The testing process should include audits, both internal and external, to ensure the new policy does not create new security holes or have some other negative affect on your software. In the event of a policy change, you should inform your staff immediately; depending on the severity of the change, related procedures may need sequential updates.

Testing is an invaluable way to prevent serious and irreversible problems. Countless critical systems have been taken out of commission due to an improperly tested patch or procedure, even if it came directly from a vendor

such as Microsoft.

Training

Training is the key to gaining employee support for any security process. Without training, employees will not understand the importance of security polices and often will ignore or bypass security measures meant to protect the computer system. You should provide training to all staff members, including all physicians, to ensure they are aware of the requirements and the consequences of not adhering to security policies. In addition to initial training, you should maintain a consistent policy of sending out reminders and warnings about current security trends or issues (e.g., computer viruses).

The three main pillars upon which computer system security is built are confidentiality, integrity, and availability (CIA). By learning and applying these three fundamentals of information security, you can greatly reduce your risk.

- **Confidentiality** ensures that a patient's data is not disclosed to an unauthorized person. For example, a loss of confidentially can occur when you transfer a patient's record via an insecure line of communication, such as a Web-based e-mail provider or instant messaging program. Improperly configuring a file system to allow anyone to view a patient's record also can breach confidentiality.

- **Integrity** is a state of being pure or free from flaw or inconsistency. When applied to computer systems, integrity describes the state of data, including modifications to the data made by a process or person, whether authorized or not. You must be able to guarantee that your system has internal checks and balances that keep unauthorized people out and to monitor those who do not have access.

- **Availability** is simply the state of being accessible by a person or process. An available system is one that users can access in a timely and efficient manner. Even if a system is up, it also must be able to handle the workload and provide the resources as defined by its purpose, including secondary services that ensure data recovery, integrity, and security in general. For example, if a system is up, but the auditing feature is offline due to a technical problem, then it is not fully available. In this case your security officer would not have available the tools and information needed to do the job.

CIA (confidentiality, integrity, and availability) are most valuable when applied as three equal parts across a system. As in a triangle, any one part missing or inadequately implemented adversely affects the entire security structure.

The rest of this section is devoted to the key physical safeguards. It is important to recognize why these safeguards exist and to what part(s) of CIA they apply. Too often, safeguards that are put in place perform redundant or irrelevant checks. CIA serves as not only a guideline for your safeguards but also a reality check of their

value. For example, while it is important to maintain a backup to ensure availability, you are defeating the purpose if you store backup tapes in the same general location as the primary computer system they are protecting. A fire would damage both the primary and backup data.

Assigned Security Responsibility

Implementing, testing, and maintaining physical safeguards is a complex job. If even one part of the security process is weak, the system is vulnerable. Regardless of the restrictive measures in place, one misplaced password can lead to a complete system compromise. Therefore, your security officer must be in charge of managing physical as well as software safeguards. Your officer will focus your practice's security efforts and ultimately be responsible for any security breaches.

Media Controls

While much of your interaction with a computer is in the virtual world that the computer monitor projects, do not forget that the computer itself still has a physical presence. Computers (and even some copiers and fax machines) have hard drives and other forms of data storage. This means that a physical medium can come to have a value far greater than its original cost. In fact, on a typical $100 hard drive, it is feasible to find hundreds of thousands of dollars worth of data, when measured in terms of time and resources. Therefore, secure organizations must have safeguards installed to protect the media.

Access

First, your practice must control and monitor access to the physical media. Too often, organizations spend thousands of dollars on antivirus software and firewalls (programs or devices that create a security boundary between internal computer resources and external network users) but forget about the actual physical devices that hold the data. If a computer system is placed in an unoccupied room with no security measures in place (e.g., a lock or motion detector), what is to stop someone from simply walking into your building and walking out with a hard drive or a laptop? You must control physical access to help reduce this security risk. Locks, solid walls (i.e., no drop ceilings that someone can crawl through from an adjacent room), window bars, sensors, access cards, and more can help ensure data remains in its designated location.

Protecting physical media requires more than a lock on a door. You need to control alternate routes of access as well. Air vents, drop ceilings, windows, fire escapes, and more can provide a point of access to an intruder.

Accountability

The value of controls is hindered without proper accountability. For example, if 10 people have keys to a locked server room, but there is no form of monitoring who

comes and goes, a theft becomes difficult to trace. Without accountability, you cannot place blame. Depending on the situation, access cards, human guards, or a simple padlock on computer media can help maintain accountability.

Backup

Data backup is also essential for any organization that wishes to remain in business after it suffers a hardware loss. Therefore, the backup media is just as valuable to your practice as the original media. In addition, losing your data to a competitor can be even more costly. Store backup media in a secure place such as a safety deposit box or in an offsite safe.

Disposal

The final issue regarding security of media involves its disposal. Organizations are constantly disposing of digital media because of upgrades, hardware failures, or changing needs. When a hard drive appears to go bad, they typically pulled it out of the host system and toss in the trash, failing to realize their trash can be very valuable to thieves. What if a file containing a patient's medical history had been stored on the discarded hard drive? A malicious person could dig through your trash, replace the malfunctioned drive part, and gain access to your patient's file. To control this, you should have a documented and formal disposal procedure that defines how to destroy or wipe clean digital media before it is trashed. The use of drills, hammers, and even fire is not uncommon to dispose of sensitive media.

Do not overlook the disposal of physical media as an aspect of computer security. It is very common to find sensitive data on discarded hard drives, CD-ROMs, or floppies. You must destroy physical media before it leaves the control of your practice.

Computer Access Controls

Physical access control is not the same as computer access control. You must take steps to prevent people from gaining physical access to sensitive information that should be available only to authorized personnel. For example, you should never allow a maintenance person inside a file storage area or computer server room without an authorized chaperone to prevent the person from accessing personal information. Maintenance personnel who are granted access to a sensitive area should not be exposed inadvertently to patient information.
To help regulate access control, you should develop a mandatory sign-in system to track entrance to sensitive areas and assign accountability for sensitive material that leaves a monitored area. Staff members who need to remove a patient's file from a secure area must understand and adhere to the guidelines for removal — such as honoring a nondisclosure agreement — and the consequences if they fail to meet the expected guidelines.

Policy/Guideline on Workstation Usage

Every practice must define policies to regulate proper workstation (computer) usage. Your policies should outline logging on/off requirements and general rules to control how the workstation is used. For example, a workstation policy should restrict the use of Web browsers to view pornography and the use of peer-to-peer (file sharing) programs. This can help curb wasted productivity as well as reduce the chance of a liability due to inappropriate activity.

Secure Workstation Location

Related to workstation use is the subject of workstation location. When a computer is in use, typically anyone directly behind or to the side of the monitor can view the screen. This is a problem if the monitor is in a public area where unauthorized personnel or clients inadvertently can see the screen. While direct viewing is the most serious issue, be aware that people can view screens by alternate methods, too. The use of mirrors, location of a monitor next to a window, or even the use of a video camera can create a compromised system. In fact, it is possible to use the reflection from a glass-framed picture hanging behind a computer monitor to read the screen from over two miles away. While this is an extreme circumstance, it demonstrates the thought that needs to go into proper computer placement in a sensitive environment.

Improper computer monitor placement is one of the most overlooked methods of breaching patient confidentiality. Pay attention to who can read the monitor directly as well as environmental issues such as the location of mirrors

Security Awareness Training

At the core of maintaining proper computer access control is user training. You should train all employees, agents, and contractors. All staff must understand security responsibilities and possible consequences of policy violation.

Often when organizations look at computer system security, they focus on the actual device performing the computing. How is the computer secured? How can a user be authenticated to a system? How do we control access to system resources? These questions all assume that data reside only on the physical computer system.

Behind most computer systems, however, is a network of communication channels that move data from one device to another. Ironically, even though they pay great attention to keeping a computer secure, many organizations fail to secure the data in transit. This habit can not only violate a patient's privacy if the wrong person captures and views this data, but also lead to a complete system compromise if an attacker captures sensitive identification information (i.e., a username/password combination). To control all access to data and reduce the risk of a potential security breach, it is important to incorporate security mechanisms to protect communications containing heath information. The following sections outline the components for secure networking.

Required Controls

HIPAA requires the following two controls as security mechanisms to secure network traffic.

Integrity Controls

When one computer transmits data to another computer on a network without security controls, a very limited number of checks occur to ensure that the data sent are the same as the data received. So, if a computer sends a patient's name and Social Security number across a network, how can the receiving computer "know" that no one tampered with the information during transmission? An attacker could capture, alter, and then retransmit the data by numerous methods without anyone being the wiser. To prevent this, you must establish a form of integrity control.

Integrity controls simply verify that the data sent are actually the data received, typically through a mathematical algorithm in which a numerical "fingerprint" (called a hash) is calculated based on unique characteristics of the original message. Once the message is transmitted and received, the receiving computer calculates a new hash value using the same mathematical process. A new hash value that matches the original hash value indicates that the message has remained intact. Calculating and comparing a "before" and "after" hash value on a message can prove that no one has tampered with the message in transit.

Message Authentication

Another method of ensuring that data are not tampered with en route is message authentication. Message authentication verifies that a message did indeed originate from the claimed location, that the file's uniqueness was maintained, and that the file was not altered. Similar to integrity controls above, this is accomplished via a hashing algorithm that creates an alphanumeric value based on the content of the original message, merged with a unique identifier of the sender. Once the message is received, the hash value is recreated using the sender's information. If the message is from the stated source, and it was not altered, the hash values will match.

Optional Controls

You can use one of two techniques to implement security controls over network traffic. The following sections will describe these two techniques, which HIPAA deems optional.

Network Access Control

As previously discussed, access controls regulate who has access to what data. Using a combination of authentication and identification measures in combination with physical security measures, your practice can regulate the type of access a user has to network traffic. For example, one of the key places to gain unauthorized access to network data is through a network's wiring system. If the cables or wires of a network run along an exposed, insecure area, an attacker easily can gain access to network traffic by plugging a computer device directly into the wiring.

Another point of concern is the ability of an employee to turn his or her machine into an unauthorized listening device. By adjusting the way a computer communicates

with the network, a disgruntled or mischievous employee can capture traffic passing between any two devices on the local network, enabling him or her to view everyone's e-mails, chat messages, Web pages, documents, or any other form of data being transmitted on the network. To reduce this risk, your practice needs to monitor its network for indications that this type of listening is occurring. In addition, you should control each user's workstation using a documented procedure. By implementing global policy controls over network computers, your practice can control how much access a user has on his or her machine. For example, it is possible to restrict all users except administrators from installing third-party software programs or accessing network settings. This would reduce the chance that someone could turn a computer into a listening device.

Data Encryption

If secure information needs to be transmitted over a network outside the control of the organization (e.g., the Internet), encryption is essential. Because there are no guaranteed controls on public networks, or even on a partner's network, all data that are transferred must be encrypted. This is to prevent someone from being able to eavesdrop and capture data sent to or from your practice's network.

Consider, for example, public e-mail service providers. When a medical facility connects to an offsite e-mail server to send and receive its e-mail, that traffic generally is sent as plain text. Thus anyone with access to any one of the many public devices between the facility and the e-mail server can gain access to the information within the e-mails. This includes the actual e-mail content and documents, images, and other attachments. To prevent this gaping breach of security, you should send and receive e-mails using an encrypted connection.

Other possible areas of concern are online Web portals that provide sensitive medical information via the Internet (not to be confused with in-house Web portals set up within the local area network). Since it is easy to capture Web pages as they are downloaded from the Internet, any Web site that offers confidential information must use encryption.

Chat or instant messaging programs, such as AIM, ICQ, or MSN, also are cause for concern. These programs generally send their traffic as plain text, making it easy for a hacker to collect and recreate entire conversations. Obviously, two medical staff members discussing confidential patient information across the Internet using a chat program is a serious security problem.

Most chat programs offer little or no security and transmit the chat text in the clear with no encryption. This is potentially dangerous if used to discuss sensitive or confidential information because anyone with the ability to capture the chat text can easily read the contents.

Required Controls for Open Systems

If your organization uses network controls to protect data traveling on an open (insecure) system, then HIPAA says you must implement all of the following security mechanisms.

Alarms

No organization is 100 percent impervious to attack. For a quick response to incursions, you need a way to warn administrators when an attack or intrusion is underway — an alarm. This kind of alarm often is not an audible bell or whistle but a simple entry in log files, e-mails, or in some cases, pages or text messages. Regardless of the type of alarm, they all serve one purpose: to alert administrators of suspicious activity.

While alarms can be useful to draw attention to a specific activity, they easily can turn into a useless annoyance. This is much like the story of the boy who cried wolf. With an overly sensitive alarm system, administrators become so used to false alarms that they start to ignore all alarms. In this situation, alarms defeat themselves and become useless.

Audit Trail

As your practice defines its access controls and implements authorization and authentication systems, you also must include an auditing feature to monitor who does what on your computer system. You might need to monitor and log everything from login attempts to file access — not to micromanage or spy on users but to facilitate an audit trail so that, if necessary, an administrator can determine how the system is being used (or abused).

For a user-identifiable audit trail to work, each user must have a unique identifier — one user name and password that links only to them. No group accounts or shared identifiers are allowed. For this reason, the individual user must keep his or her account information secret. The unique identifier is an intrinsic part of how an audit trail works.

Audits work only if users keep their authentication information secret. Sharing passwords or user accounts destroys the ability of an auditing system to maintain user accountability.

With a proper logging system in place, an administrator can recreate the actions of a hacker who gains access to your computer system. For example, depending on the attack technique, the logs could show an attacker repeatedly entering wrong username/password combinations in an attempt to guess the correct account information. If an attacker gained unauthorized access, the audit trail could provide a sequential listing of the files and folders the hacker accessed. If the hacker changed any files, an audit trail could provide a list of these files, which would have to be replaced with a valid copy from backup.

Entity Authentication

As previously discussed, authentication controls are required to control user access

and to provide user accountability for all activity that occurs on a computer system. To ensure that entity authentication is a reliable method of meeting these goals, implement these prerequisites:

- Each user must have a unique user identifier for the purpose of auditing and user accountability.

- Each user must have a strong password. A strong password is a string of seven or more characters (letters, numbers, or symbols) that cannot be guessed easily and are not a dictionary word. Weak passwords are birthdays, names, places, events, or any other word/character combination that people use in everyday life.

  A strong password will contain a combination of upper and lower case letters, numbers, and at least one symbol character. The following list contains examples of strong passwords. Note that you can read each password as a phrase to make it memorable, but each contains numerous odd characters to make it a strong password.

  Art*1s*Fun (Art*is*Fun)
  1L0veD@cs (I Love Docs)
  sK11ng&sl0pes (skiing & slopes)

- If at all possible, passwords should be global; one password should grant a user access to every application, file, folder, and service he or she needs to use on a network. This eliminates the need for remembering numerous passwords. Forcing too many passwords often encourages users to write them down in obvious places, thus defeating the whole point of entity authentication.

- Passwords should have a limited lifespan. In addition, you should implement a password control policy to restrict reuse and minimal changes (e.g., sequentially increasing a number at the end of the password each time it is changed). A typical lifespan is 60 to 90 days. Some passwords systems require the user to carry a device that dynamically recreates a password every five to 10 minutes, reducing the chance that a password will be easily guessed or captured and then abused.

- You should require a multifactor authentication system for any application/service that is accessed via an insecure route, such as the Internet. Using a second identifier such as biometrics or a personal identification number in conjunction with a password provides an extra layer of authentication.

Event Reporting

Use event reporting in conjunction with auditing and logging systems to provide feedback to administrators, managers, and end users about computer activity. Event reporting not only reveals unauthorized access attempts but also ensures that users and managers can review their own activity, or the activity of those staff members for whom they are responsible. This provides a human layer of monitoring to detect suspicious activity that is not necessarily in violation of a system policy. For example, a user who shows activity on a week he or she was on vacation warrants further

investigation, and the only way to detect such activity is through event reporting and monitoring. Since by default the user's activity is not against system policy, it normally would not trigger any system alarms.

Wireless Networks

Wireless networks have become a popular way to provide physicians and other health care providers with the ability to stay connected to computer systems and their resources with out the need to maintain a wired connection. All sorts of industries are implementing this technology, not just health care. Unfortunately, little attention is paid to the security of wireless networks and the potential risks they create. This section will examine the risks of wireless networks as they apply to the technical security mechanisms that HIPAA requires.

When data is transmitted over a wirelesses connection, anyone in range with a wireless device can capture it. In other words, you should assume that all traffic passed over a wireless network is available to the general public.

As previously stated, two security mechanisms are required on a secure network: integrity controls and message authentication. Unfortunately, a default wireless network does not meet either of these requirements. While some integrity controls and message authentication schemes are built into wireless networks, they require the use of encryption to become effective — and many wireless networks use a weak form of encryption that has been proven to be insecure. As a result, neither data integrity nor message authentication can be established using default equipment and configurations. At the time of this writing, *most physicians using wireless networks for patient care are in active violation of HIPAA regulations.*

A lack of wireless security is a consistent problem in the majority of medical organizations. Despite repeated warnings and demonstrations, unprotected wireless networks are used to transmit sensitive data at medical facilities. Most physicians using wireless networks for patient care are in active violation of HIPAA regulations.

In addition to integrity controls and message authentication, one of the following must be implemented for adequate security: network access control or data encryption. Unfortunately, a default wireless network does not include either of these features. While it is possible to establish a simple form of access control via the use of a pre-shared password, which also can be used to encrypt the wireless traffic, it has been proven that the encryption scheme many wireless network devices use is easy to crack due to an inherent flaw in its implementation.

Currently, certain wireless equipment vendors have implemented some measures of protection to correct the problems that have plagued wireless networks. However, even these measures are not enough to secure a wireless network to the point where it can be considered a closed or secure system. As a result, you must treat a wireless network as an open network, which means it must contain *all of* the following security mechanisms: alarms, audit trails, entity authentication, event reporting, and third-party encryption. The following list outlines how each of these should be used in a wireless network.

- **Alarms.** A digital firewall must separate a wireless network from the closed network. The firewall must be able to control access based on entity authentication. In addition, the firewall (or other device) must include alarm features.

- **Audit trail.** In addition to a firewall and alarm system, you should maintain a complete log of all wireless activity to provide administrators with a means to perform security audits.

- **Entity authentication**. Every wireless user must provide unique identification information before being allowed to connect from a wireless network to an internal network. This provides not only a layer of protection from unauthorized access but also a means of irrefutably identifying authorized users and their activities.

- **Event reporting.** Your practice should monitor wireless devices and traffic continuously to ensure they are operating properly, especially given that they are extremely vulnerable to numerous types of attacks that focus on functionality. For example, it is possible for an attacker to use a high-powered wireless device to completely overpower an existing wireless device, thus rendering it useless. If an access point detects a significant drop in users, or the existence of a competing access point, it should send an event alert to the administrator.

- **Third-party encryption.** Although it is possible to rely on a wireless device's encryption scheme to secure the network traffic, it is not recommended because of the weakness described above. To compensate, you should use additional encryption to secure your network, typically a virtual private network (VPN), which tunnels the wireless traffic into an encrypted tunnel inside the wireless network. In other words, a VPN wireless user will encrypt the traffic twice. This way, if the encryption provided by the wireless devices is weak, another layer of encryption is in place to protect the data from attackers.

Wireless networks offer a convenience that is difficult to ignore. For example, through the use of a wireless network, physicians in several exam rooms can connect to a patient's history in real time. In additions, physicians can update or alter records on the fly with progress notes, EKGs, and even CT scan images. This can eliminate bulky paper charts and help prevent transcription errors. However, before you can realize the benefits of wireless communication, you must implement extensive security mechanisms to ensure that the traffic passed over the network is not compromised.