HIPAA Security: Compliance in Radiology—An Academic Radiology Department’s Plan Contrasted with a Small Private Practice

Nogah Haramati, MD

ABSTRACT

In complying with the HIPAA security regulations, the large, multi-site academic radiology department is quite different from the small, private radiology practice. This article compares and contrasts the methods each of these two model organizations use to achieve compliance. In common between the two organizations is that complete documentation of the procedures and processes involved in data management must be prepared and reviewed. Although not required in the regulations, having the documentation conform to the regulation allows for easy monitoring, auditing, and certification of compliance by future independent bodies. The level to which each organization must secure their data, perform threat assessments, and implement security procedures and intrusion detection systems are very different. The regulations do not specify what level of due diligence is required. This must be determined by each organization using their own common-sense dictum. Although the solutions used by these two types of organizations may not be the same as those adopted by other radiology departments and practices, the approaches may still serve as useful templates to guide compliance efforts by others.

KEYWORDS

• HIPAA
• Security
• Radiology
• Compliance
• Implementation
• Assessment
• Academic medical center
• Private practice
• Group practice
Introduction

In complying with the HIPAA security standard, the large, multi-site academic radiology department is quite different from the small, private radiology practice. This article details an approach to security standard compliance for both types of organizations. To demonstrate the similarities and differences in security standard compliance between the two sample organizations, the large, academic center is described as a center composed of three, free-standing 800-bed hospitals each with an annual study volume of 250,000 examinations. Each of the three hospitals is under different ownership and has a different billing procedure. However, all three are connected with a common picture archival and communications system (PACS), have the same academic staff, and share residents and one chairperson. Each facility does, however, have a different radiology information system (RIS) and the hospitals have different hospital information systems. The small, private office has a single site, three radiologists, and an antiquated billing system with no PACS or teleradiology capability. The computed tomography (CT) and magnetic resonance (MR) in the small, private office are of the same vendor and are networked together.

What Is Covered?

The applicability of the security standard to all healthcare data is demonstrated by the following excerpt from the standard: “The security standard is applicable to all healthcare information electronically maintained or used in an electronic transmission, regardless of format; no distinction is made between internal corporate entity communication or communication external to the corporate entity.” From the above excerpt it is clear that the transmission of covered data between two devices is part of the security standard. The issue of the scope of what electronic data is specifically covered by the security standard is detailed in the following excerpt from the security standard: “Individually identifiable health information’ means any information, including demographic information collected from an individual, that—

a. Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
b. Relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payments for the provision of healthcare to an individual, and
(i) Identifies the individual, or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

The scope of this excerpt is quite encompassing. The security standard does not clarify whether digital information converted to analog is still covered throughout the lifetime of that analog data. An example is a patient’s CT scan.
The transmission to a film printer is a covered action. Once film is printed, that data is analog. The security standard does not specifically include or exclude analog data or data that was once electronic. Until this issue is resolved by the federal government, prudent action would be to assume that once data is in a form that is covered by the security standard, that data will remain covered regardless of the forms that it may take. This means that even a printed procedure schedule listing patient names should be considered to be covered by these regulations—and the access to and disposition of that simple sheet of paper must be included when preparing a compliance plan!

The Initial Assessment

The first part of security standard compliance is to perform a complete assessment of the organization’s security practices and its data flow. Careful attention needs to be given to all areas where patient data is collected, input, generated, accessed, stored, distributed and, when no longer needed, destroyed. Table 1 provides a framework for the initial-assessment stage. In very large organizations, each of the twelve categories listed might be represented by more than one individual. In order to keep the working group manageable, limiting the size of the team to twelve members is a prudent step. In small organizations, one or two individuals may perform the entire assessment. The existing practices, policies, and procedures for those twelve areas need to be carefully reviewed. (Unfortunately, many organizations, large and small, find that their policies and procedures do not reflect their real-time practices.) At the

Table 1. HIPAA Security Standard—Initial Assessment, Organizational Perspective

<table>
<thead>
<tr>
<th>A. Organizational Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security and confidentiality policies</td>
</tr>
<tr>
<td>2. Information security officers</td>
</tr>
<tr>
<td>3. Education and Training Programs</td>
</tr>
<tr>
<td>4. Sanctions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. Technical Practices and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Individual Authentication of Users</td>
</tr>
<tr>
<td>2. Access Controls</td>
</tr>
<tr>
<td>3. Audit Trails</td>
</tr>
<tr>
<td>4. Physical Security and Disaster Recovery</td>
</tr>
<tr>
<td>5. Protection of Remote Access Points</td>
</tr>
<tr>
<td>6. Protection of External Electronic Communications</td>
</tr>
<tr>
<td>7. Software Discipline</td>
</tr>
<tr>
<td>8. System Assessment</td>
</tr>
</tbody>
</table>

conclusion of this initial assessment stage, the team should have a very clear idea about the status of each of the twelve organizational perspective items.

**Information Security Officer.** If such a position does not already exist within the organization, a suitably talented individual should be appointed. This is a critical position for security standard compliance, as this person will be responsible for the overall supervision of the compliance program, once the initial assessments are completed and a plan for compliance is developed. In small groups such as the private practice, an existing staff member—such as an office manager, corporate officer, or applications manager—may assume this role and add these duties to his or her many other duties.

**Initial Plan Development**

With the security standard team in place and the information security officer appointed, the group is ready to begin development of the actual compliance plan. The team should take the data from the initial assessment and, using the security standard, determine the areas that are compliant and those that are deficient. Even in a private practice setting there are multiple areas where covered data is stored on media, such as a receptionist’s PC saving data to tape, CT and MR saving to different optical media, and ultrasound saving to videotape. In the academic center, the situation is similar, but the magnitude is increased. For those areas that are compliant, the documentation needs to be assembled at this time, as the documentation is available following the initial assessment. I recommend that the documentation be organized in a manner similar to the security standard, as this will ease the future tasks of demonstrating compliance to internal and external auditors.

**Documentation**

The standard states: “The proposed standard requires that each healthcare entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement and maintain appropriate security measures. Most importantly, these measures must be documented and kept current.”1 Note that the emphasis is placed on the documentation! Security standard compliance should not be viewed as a binder that must be filled with pages and left to collect dust until required for an audit. It should become a vibrant document that actively reflects the ongoing efforts of an organization to protect confidential patient data while ensuring availability of that data when needed. The security standard, when complete, should be made part of the organization’s policies and procedures manual and should be easily accessible to authorized individuals whenever required. Having a Web-based manual would make that document available and relevant to anyone who has need and authorization to access it. Updating the manual is then also simplified.
HIPAA Security Standard—Implementation

The following outline expands on the requirements listed in the security standard, supplying definitions for various items whose meanings may be doubtful and offering insights and suggestions valuable to the compliance efforts of both the academic center and the private practice. Some of the categories listed in the security standard are self-explanatory and will not be discussed, while some will be extensively discussed. To reduce redundancy, the same explanations and discussions are given only in the area to which they are most applicable and are listed only once. The reader is encouraged to review the discussions relevant to both the academic center and the private practice, as some discussion relevant to both will be listed only with one.

1. Data Integrity, Confidentiality, and Availability

A. Administrative Procedures

1. Certification—Defined by the security standard as: “The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.”

The organization must develop a set of security standards that will apply to each network and computer system used. These standards may be the same or different for different systems within an organization. After these standards are developed, the organization must periodically review those systems and determine if they are or are not, indeed, compliant with the current standard.

*Academic center:* Hospital network audited and certified by internal management information systems (MIS) department. Dedicated networks installed for the use of a single vendor’s equipment audited by MIS and vendor. Final certification needs to come from MIS.

*Private practice:* Vendor or third party supply the standards, perform the audits, and certify the compliance or departures of each element. The standards that apply to a private practice need not be as rigid as those that apply to the large academic centers.

2. Chain of Trust Partner Agreements

*Academic center:* Each hospital executes agreements with all its vendors, insurers, third-party payers, affiliates, and providers.

*Private practice:* Executes agreements with its third-party payers, insurers, vendors, and moonlighters.
3. Contingency Plan (include all of the following)
   a. Application and data criticality analysis—an assessment needs to be made for each application concerning access to data and the effect of time delay on patient care.

   **Academic center:** RIS data concerning previous examinations and allergic and other adverse reactions are critical to patient care. PACS image unavailability is life-threatening to patients in critical care, emergency departments, and operating rooms.

   **Private practice:** Lack of image data from previous examinations is inconvenient, but is not usually life-threatening as a private office is not normally an acute care setting. If the delay or unavailability of image data is of short duration, inconvenience to patient and referring physician is the most likely outcome.

   b. Data backup plan—mission-critical data must be stored in a manner that has a high probability of disaster survival.

   **Academic center:** All RIS and PACS data must be considered mission critical and stored securely. The use of on-site and off-site mirrored tape archival allows a high degree of certainty that data will be retained if transmission is interrupted suddenly or if one geographic site sustains a calamity.

   **Private practice:** The use of a PACS archive allows the data to be stored should the CT or MR device sustain a significant failure. Having mirrored tapes or archive media allows for the salvaging of data should one media be corrupted.

   c. Disaster recovery plan—allow and plan for how data is to be recovered in the event of data loss.

   **Academic center:** Recovery plan needs to be robust and be able to be implemented without the assistance of any specific vendor.

   **Private practice:** Plan may be largely or entirely dependent on one vendor. The economic viability of the vendor is a factor when considering long-term disaster recovery options.


   **Academic center:** Requires both a paper-based approach to replace RIS functions and a film-based approach to replace PACS functions. Manual accessing of the PACS image repository, if possible, will likely be required.

   **Private practice:** If the failure is severe enough, the private practice may actually be paralyzed until the system is restored.

   e. Testing and revision.
**Academic center:** Completes each plan with the aid of the vendor and MIS. As PACS is in place, careful attention needs to be given to the PACS functioning, backup, and redundancy of data. Methods of data extraction from the PACS archive(s), in the event of PACS failure, need to be documented. Duplication of archived data might be prudent and should be considered. If the PACS long-term data archive format allows for some data to be irretrievably lost during the archival process, the institution must assess and certify that such data loss does not compromise the value or usage of the data.

**Private practice:** Storage of digital archival media for CT and MR on removable media requires that media to be securely maintained. Loss of that media would result in permanent loss of patient data. Centralized archiving should be considered as an alternative to removable media. The use of a commercial data warehouse for this image archival might simultaneously be both cost-effective and compliant. Implementation of digital computed radiography (CR), direct radiography (DR), or other devices whose outputs are printed on film rather than archived should be re-evaluated. Digital archives might ease compliance. A film file room that is tracking the location of the only hardcopy image of a study might have no data recovery option should that film be lost.

4. Formal Mechanism for Processing Records
5. Information Access Control (include all of the following)
   a. Access authorization.
   b. Access establishment.
   c. Access modification—Access is defined by the security standard as: 
      “The ability to read, write, modify or communicate data/information or otherwise make use of any system resource.”

**Academic center:** Access to hospital-wide systems controlled by a department security officer and monitored by MIS. Access to data on a specific modality may not be controllable digitally. Access to PACS data though a workstation requires user login, but viewing of an examination on the acquisition device (CT or MR) cannot be logged or controlled digitally. The policy must be very clear as to who may or may not access images via such devices. Access to file room images that are covered by the security standard should also include verification of the access privileges of the requester. Optimally, the requester should log the request into a verification system such as a compliant RIS before the file room grants the requester access to the images.

**Private practice:** Images sent to referring physicians should be placed in a jacket that has a clearly visible warning to unauthorized recipients. A sample text is: “The documents herein are intended for the use of
the individual to whom, or entity to which, it is addressed and may contain information that is privileged, confidential, and exempt from disclosure. If the recipient of these documents is not the intended recipient, you are hereby notified that any access, viewing, copying, dissemination, or unauthorized use thereof is strictly prohibited, and please notify us immediately so that we may arrange for the return of these documents.”

6. Internal Audit—Important for both the academic center and the private practice to ensure that the policies and procedures are being followed.

**Academic center:** The key to proper implementation of policies and procedures is the training of appropriate personnel in those procedures. Periodic drills using key personnel and simulating various extents of data interruption is an excellent method of evaluating the appropriateness and value of the policies and procedures. Internal auditing of compliance with policies and procedures as well as robustness of the emergency plans is of critical value in preparing for untoward events.

**Private practice:** Audits may be as simple as periodic reviews that ensure data backups are performed properly and on schedule and that appropriate staff are familiar with the emergency procedures.

7. Personnel Security (include all of the following)
   a. Ensure the supervision of maintenance personnel by an authorized, knowledgeable person.
   b. Maintain a complete record of access authorizations.
   c. Ensure that operating and maintenance personnel have proper access authorization.
   d. Personnel clearance procedure.
   e. Personnel security policy/procedure.

8. Security Configuration Management (Include all of the following)
   a. Documentation.
   b. Hardware/software installation and maintenance review and testing for security features.
   c. Inventory.
   d. Security testing.
   e. Virus checking.

**Academic center:** Compliance with the HIPAA security standard and with the institution(s) security standard policy and procedures must be carefully examined as part of all new equipment acquisitions. HIPAA compliance must also be part of any request for proposal that is issued for new equipment. With regards to existing equipment that have deficiencies related to the security standard, if the equipment is not likely to be replaced, a security standard policy and procedure needs to be developed for that equipment.
9. Security Incident Procedures (Include all of the following)
   b. Response procedures.

10. Security Management Process (Include all of the following)
   a. Risk analysis—Defined by the security standard as: “A process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.”
   b. Risk management—Defined by the security standard as: “The process of accessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.”
   c. Sanction policy—Defined by the security standard as: “Policies and procedures regarding disciplinary actions which are communicated to all employees, agents, and contractors.”
   d. Security policy—Defined by the security standard as: “The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities and organization commitment for a system.”

11. Termination Procedures (Include all of the following)
   a. Combination locks changed.
   b. Removal from access lists.
   c. Removal of user account(s).
   d. Turn in keys, tokens, cards, and all other access devices.

   Academic center: The security standard termination procedures should be part of the human resources termination procedure. Using token-based access to facilities enhances the access control, monitoring, and auditing. For example, having keycard capability within the hospital identification tag would allow for that ID tag, with an additional password, pin, or biometric (if needed) to control access to everything from the parking lot to the hospital information system. Disabling that access as part of a termination procedure eases the termination process (see Token 1.C.5.c.3).

   Private practice: Changing combination locks might result in other staff no longer having access.

12. Training (Include all of the following)
   a. Awareness training for all personnel including management.
   b. Periodic security reminders.
   c. User education concerning virus protection.
   d. User education in the importance of monitoring login success/failure, and how to report discrepancies.
   e. User education in password management.
Academic center and private practice: Training is time-consuming. Because different people learn at different rates, the training component is optimal for Web-based training. This would allow different people to learn at their own rates, verify their mastery of the subject matter using on-line testing, document awareness and comprehension of policies, allow for easy verification of training compliance, and obtain anonymous feedback.

B. Physical Safeguards

1. Assigned Security Responsibility—Defined by the security standard as: “Practices put in place by management to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.”

2. Media Controls (Include all of the following)
   a. Access control—who can access the media and how is that access granted, logged, and monitored.
   b. Accountability (tracking mechanism).

Academic center and private practice: Have a clear policy related to the various media that are used. If media are not actively in use, they should be kept secure. Access to those media should also be logged. If the media are kept in a locked cabinet, a signature sheet noting the identity, time, date, media ID, and purpose for media removal and time of subsequent return would fulfill this requirement.

c. Data backup.

Academic center and private practice: A policy also needs to be created for all the different devices that require backup. The backup procedures and integrity of that media should be the subject of frequent internal audits.

d. Data storage—site and security of where and how the media are kept.

Academic center: Having data stored simultaneously both on-site and off-site greatly enhances the media security. Data warehousing options are available as alternatives for off-site storage. Such options may complicate or simplify emergency data recovery plans depending upon configuration and availability of telecommunications and manual transport capabilities.

Private practice: May be solved simply by having the media locked in a specific location and using a logbook to record access to media and data. Audits then become important in ensuring that the logbook approach is being faithfully and properly used.
e. Disposal.

**Academic center and private practice:** Disposal of media is not simply the discarding of the media but also the verification that all data on that media is no longer accessible. This not only applies to imaging data, but to all patient data, such as hard drives of machines used in transcription. Software for data wiping should be available within the organization for such procedures. Alternatively, a vendor may be contracted to assume responsibility for destroying all data on discarded media. Note that the vendor, like most others, needs to complete a chain of trust agreement.

3. Physical Access Controls (include all of the following)
   a. Disaster recovery.
   b. Emergency mode operation.

   **Academic center and private practice:** What will be the procedure if one or more systems, media, or data elements are not available?

c. Equipment control (into and out of site).

   **Academic center:** Procedures need to be in place to control and monitor the movement of equipment into and out of a facility. Having a centralized archive is not much help if the entire archive is stolen. As most large facilities have a pilferage problem, instituting lock-down devices in unmonitored areas whereby the user has no access to the disk drives on the unit and cannot copy data to a disk reduces the risk of illicit data removal. Keeping the data on networked drives, implementing thin clients, and never actually running the data on the local workstation also reduces the risk of data pilferage.

d. Facility security plan.

   **Private practice:** Ensuring that the computer server is maintained in a secure room is a basic step.

e. Procedures for verifying access authorizations prior to physical access.

f. Maintenance records.

g. Need-to-know procedures for personnel access.

h. Sign-in for visitors (and escort, if appropriate).

i. Testing and revision—Defined by the security standard as: “The documented process of periodic testing to discover weaknesses in such plans and the subsequent process of revising the documentation if necessary. . . . Testing and revision of programs should be restricted to formally authorized personnel.”

   **Academic center:** Testing and revision should be done with MIS along with the vendor.
Private practice: The vendor must certify that all hardware and software undergoes periodic (according to a set schedule) testing and revision in compliance with the security standard. Those certifications should be sent to the designated practice security officer for inclusion into a manual in which all compliance steps taken are documented and available for internal and external auditing.

4. Policy/Guideline on Workstation Use

Academic center and private practice: That policy guideline should be available at the workstation. Having the nonconfidential portions of the policies and procedures manual available on-line would make that document meaningful to any who have need for it.

5. Secure Workstation Location

6. Security Awareness Training

Academic center and private practice: See Training (1.A.12).

C. Technical Security

1. Access Control

   a. Procedure for emergency access (required).

   b. One of the following is also required:

      i. User-based access—Defined by the security standard as: “A security mechanism used to grant users of a system access based upon the identity of the user.”  

      ii. Role-based access—Defined by the security standard as: “An alternative to traditional access control models (for example, discretionary or nondiscretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. . . . Each user is assigned to one or more roles and each role is assigned the level of privileges needed for that role.” 

      iii. Context-based access—Defined by the security standard as: “An access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The external factors might include time of day, location of the user, strength of user authentication, etc. part of access control on the matrix.”
Academic center and private practice: Context-based access is not as flexible an access control as role-based access. Because either role-based or user-based access is required for authorization control (see 1.C.ii), context-based access should be considered only if user-based and role-based are already implemented.

iv. Encryption

Academic center and private practice: Encryption of data serves a valuable function in other areas of security standard compliance, but it is not the preferred method of general user access. However, in specific situations it may be of value. If data is being sent through a non-secure open link (Internet) or even through the mail, if the data is first encrypted using strong public key cryptography, that data may be accessed only by the recipient possessing the appropriate private key.

2. Audit Controls—Defined by the security standard as: “The mechanisms employed to record and examine system activity.”

Academic center: This is a combination of audit trails, system logs, network monitors, and intrusion detection systems for networked systems.

3. Authorization Control—Defined by the security standard as: “The mechanism for obtaining consent for the use and disclosure of health information.” (One of the following is required)
   a. Role-based access. See Access Control above (1.C.1).
   b. User-based access. See Access Control above (1.C.1).

4. Data Authentication—Defined by the security standard as: “The corroboration that data has not been altered or destroyed in an unauthorized manner.”

   Data or document authentication may be done by a number of means, including checksum, double keying, and message authentication code. To truly authenticate the data, the document creator generates a checksum or similar value.

   Academic center: Should create a certification authority for internal certificates. Any authorized user within the academic center can verify the authenticity of a signed document and identify its author. External, third-party certificate authorities exist. These same authorities can make digital certificate verifications available on a restricted basis.

   Private practice: Document authentication should be performed using third-party digital certificate vendors.

5. Entity Authentication
   a. Automatic logoff (required).

   Academic center and private practice: The time until a workstation automatically logs the user off the system should be adjusted on the basis
of the security of the workstation location. When the workstation is in a public area, the logoff time should be short, and when the workstation is in a very secure area, it can be longer.

b. Unique user identification (required). This is the user ID.

c. One of the following is also required:

i. Password

**Academic center:** Attention should be given to third-party password and authentication systems that would verify a user but not maintain a password file. Centralized user-based access could be controlled from this system and the user need only remember one password for many systems. This way the probability that the user could remember the current version of a regularly changing password is increased.

ii. PIN (basically just a glorified password)

**Academic center and private practice:** Passwords and PINs are the current standard. They also fulfill the security standard requirement. The problem with passwords and PINs is that people pick values that are easy to remember and easy to crack. Having the system select random passwords and PINs that expire results in people writing those values in insecure places or forgetting the values and losing access.

iii. Token—Defined by the security standard as: “A physical item that is used to provide identity.” An example is an electronic key or a keycard containing a uniquely encoded serial number within. Use of a token does not guarantee the identity of an individual since the token could have been lost or stolen. Therefore, tokens are usually coupled with another security feature such as a password or biometric.

iv. Biometric—Defined by the security standard as: “An identification system that identifies a specific individual from a measurement of a physical feature or repeatable action of an individual (for example, hand geometry, retinal scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints and hand written signatures.”

v. Telephone callback—Defined by the security standard as: “A method of authenticating the identity of the receiver and sender of information through a series of ‘questions’ and ‘answers’ sent back and forth establishing the identity of each.” In the example of a user dialing to a host machine, after identification is completed the host disconnects and calls the user back at a predetermined number.

**Academic center and private practice:** Needs to be implemented for all modalities in which a vendor has a dial-in remote diagnostic
capability. In those cases, the unit should be required to call the vendor back. Otherwise, an illicit backdoor is opened for unscrupulous access of healthcare data. Another approach would be to use a virtual private network (VPN) in which access to the network requires authentication. The VPN can be established and maintained by a third party.


A. General Issues Affecting All Networks and Communication

1. Entity Authentication (required)—Defined by the security standard as: “Corroboration that an entity is the one claimed [ISO 7498-2]. . . . To irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs and processes.”

   **Academic center and private practice:** Disable all generic logins such as “radiology,” “lab,” and “registration,” and require individual logins.

2. Audit Trail (required)

   **Academic center:** This section specifically deals with networking. Maintaining an audit trail of the managed-network use is still not always being done. In addition, all future information systems should be purchased with audit trails. Old systems without audit trails should be replaced. If they do not have audit trail capability, the odds are that they also do not fulfill many of the other functions that are deemed essential.

   **Private practice:** There is a very real possibility that many small private practices have unmanaged networks. In this situation, audit trails of the network use either cannot be done or would be very rudimentary. In a practice with a small, unmanaged hub, the log file of the server probably fulfills the security standard requirement. Further guidance from the Department of Health and Human Services will be required for this issue to be resolved.

3. Event Reporting (required)

   **Academic center:** This includes not only supervision of network traffic and network health, but also implementation of intrusion detection systems and other such features to increase the likelihood that illicit network entry or usage is detected.

   **Private practice:** There must be a log kept of every major event that occurs on the network. This is especially true of untoward events. Data integrity in the era of networked communication requires that the health of the network be optimized and any evidence of “disease” or infiltration be identified.
4. Alarm (required)

**Academic center:** The academic center should have a qualified and authorized network engineer available around the clock for network emergencies. All detected network aberrations should be logged. Serious aberrations should result in the network engineer being contacted. The network engineer should have access to and be familiar with the policies and procedures to be followed in cases of network compromise. In the event that healthcare data is being compromised, a mechanism needs to be in place so that the illicit access is closed. This may include shutting down external access sources, or even all or part of the network. A procedure needs to be created so that the network engineer knows whom to contact for the necessary authorization. The policies concerning the contacting of law-enforcement agencies also needs to be part of this procedure.

**Private practice:** As networks become larger, the practice should consider the possibility of outsourcing the network management and oversight to a third party. The documentation and monitoring obligations are then assumed by the third party.

B. Open/Internet—Issues Specific to Open Communications or Internet Transmissions

1. Message Authentication (required)
2. Integrity Control (required)—Defined by the security standard as: “Security mechanism employed to ensure the validity of the information being electronically transmitted or stored.”
3. One of the Following is Required
   a. Access controls—Defined by the security standard as: “The protection of sensitive communications transmissions over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient.”
   b. Encryption.

**Academic center and private practice:** See discussion related to Data Authentication (1.C.4). Establishing a virtual private network (VPN) satisfies all the requirements of this portion of the security standard, including message authentication, integrity control, access control, and encryption, and may actually be less costly than other methods of performing similar functions. The VPN may be contracted from a third party who would then ensure these functions.

3. Digital Signature

A. Message Integrity (required)
B. Non-repudiation (required)
C. User Identification (required)
D. The Following Are Optional
1. Ability to Add Attributes (such as time/date stamp).
2. Continuity of Signature Capability—Defined by the security standard as: “The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date.”
3. Countersignatures—Defined by the security standard as: “It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party.”
4. Independent Verifiability.
5. Interoperability—Defined by the security standard as: “The applications used on either side of a communication, between trading partners and/or between internal components of an entity, being able to read and correctly interpret the information communicated from one to another.”
6. Transportability—Defined by the security standard as: “A signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document.” Concerning the digital signature, see discussion related to Data Authentication (1.C.4).

Conclusion

HIPAA is first and foremost a call for complete and relevant policies and procedures to protect patient data and access to that data. All aspects of the HIPAA security regulations that are relevant to a specific organization must be reflected in the policies and procedures. When the HIPAA-related policy and procedure documentation is assembled, the need for periodic review and updating of this documentation is essential as processes, procedures, hardware, and software continually change. Periodic internal and external audits aid in identification of shortcoming in procedures and compliance with existing policies and procedures. New threats to data confidentiality and security are inevitable, and the organization and the information security officer need to be vigilant in ensuring that the organization is in compliance with federal regulations. Diligence in compliance with the HIPAA regulations will ease the burden of other periodic inspections such as Joint Commission and others. Based on past experience with healthcare regulations, more regulations are certain to follow.

References
About the Author

Nogah Haramati, MD, is director of informatics and associate professor of radiology and orthopaedic surgery at Montefiore Medical Center and the Albert Einstein College of Medicine. Dr. Haramati is also president of RADCS, LLC, a consulting firm specializing in healthcare information technology and integration.