CHAPTER 2

Health Insurance Portability and Accountability Act

Samuel J. Dwyer III, PhD
Alfred C. Weaver, PhD
and Kristen Knight Hughes, Esq.

The Health Insurance Portability and Accountability Act (HIPAA) was passed by the U.S. Congress on August 21, 1996. HIPAA had its roots in an invited industry workshop held in 1991. This workshop was convened by then Secretary of Health and Human Services (HHS), Louis Sullivan, who sought to identify the most significant issues facing the health care industry. At the time, considerable government concerns centered on rising health care costs. One of the key issues identified was that almost 40 cents of every health care dollar were being spent on administrative overhead (*1,2*). In response to the Sullivan forum, a number of industry groups were organized. One of these was the Workgroup on Electronic Data Interchange, which called for the voluntary adoption of the Accredited Standards Committee (ASC) X12 standard for administrative and financial transactions. However, the health care industry was slow in rallying support to achieve this goal. At the time that the HIPAA legislation was introduced, more than 400 different "standard" claim forms were in use. In 1996, Senator Nancy Kassebaum (R–KS, retired) and Senator Edward Kennedy (D-MA) introduced the adoption of standard transactions and privacy and security measures to protect health information and insurance portability, prevent fraud and abuse, create medical savings accounts, and identify standards for patient medical record information (for future regulations).

HIPAA is also known as Public Law 104–191. The Act has five top-level titles:

- Title 1. Health access, portability, and renewability.
- Title 2. Preventing health care fraud and abuse (administrative simplification), which includes: (1) transactions and code sets; (2) identifiers; (3) privacy; and (4) security.
- Title 3. Tax-related health previsions (medical savings accounts and health insurance tax deductions for self-employed individuals).
- Title 4. Group health plan provisions.
- Title 5. Revenue offset provisions.

The first "A" in HIPAA is for "accountability" and implies accountability in insurance claims (combatting fraud). This is accomplished for the most part by computer software. The "IP" in HIPAA is for insurance portability. It limits exclusions that insurers can use, enables credits for past insurance, and attempts to enable individuals to purchase insurance. However, it does nothing about the cost of insurance, instead seeking to ensure that insurance is available to those who can pay for it.

The privacy rule concerns policies regarding the flow of information, rights for patients to review and amend data in their medical records, and administrative requirements. It applies to all individually identifiable information, including that contained in electronic, paper, and oral communications.

The security rule requires that administrative safeguards, physical safeguards, and technical safeguards be implemented by a covered entity to "ensure the availability, confidentiality, and integrity" of all electronic protected health information (PHI).

HIPAA applies only to covered entities. Covered entities include health plans, health care clearinghouses, and health care providers.

The transaction rule applies to any covered entity that transmits any health information in electronic media form in connection with HIPAA transactions. The security and privacy requirements of HIPAA apply to an individual's identifiable patient information.

HHS has issued several regulations to implement the HIPAA requirements, including those discussed in the following sections:

Transactions and Code Sets

- Final rule, standards for electronic transactions (*Fed Reg*. Aug 17, 2000;65:50312); proposed rule (*Fed Reg*. May 7, 1998;63:25272).
- Final rule. Modifications to transactions and code set standards for electronic transactions (*Fed Reg*. 68;Feb. 20, 2003;8381); proposed rule, retail pharmacy transactions (*Fed Reg*. May 31, 2002;67:38044); proposed rule, regarding modifications to the transactional standards.

Privacy

- Final rule modifications, standards for privacy of individually identifiable health information (*Fed Reg*. Aug. 14, 2002;67:53182); proposed rule (*Fed Reg*. March 27, 2002;67:14776).
- Final rule, standards for privacy of individually identifiable information (*Fed Reg*. Dec. 28, 2000;65:82462); proposed rule (*Fed Reg*. Nov. 3, 1999;64:59918).

Security

- Final rule. Health insurance reform, security standards (*Fed Reg*. Feb. 20, 2003;68:8334); proposed rule (*Fed Reg*. Aug. 12, 1998;63:43242).

Identifiers

- Final rule, national standard employer identifier (*Fed Reg*. May 31, 2002;67:43242); proposed rule (*Fed Reg*. June 16, 1998;63:32784).
- Proposed rule, national standard health care provider identifier (*Fed Reg*. May 7, 1998;63:25320).

Enforcement

Interim final rule, civil money penalties: procedures for investigations, imposition of penalties and hearings (*Fed Reg*. April 17, 2003;68:18895).

The compliance dates for each HIPAA regulation (*4*) are presented in Table 2.1.

TABLE 2.1
Compliance Dates for each Hipaa Requirement

Compliance Date	Requirement
October 15, 2002	Electronic health care transactions and code sets (submit an extension forum)
October 16, 2002	Electronic health care transactions and code sets (except those who files for an extension)
April 14, 2003	Privacy (all covered entities except small health plans)
April 16, 2003	Electronic health care transactions and code sets (covered entities started software and system testing)
October 16, 2003	Electronic health care transactions and code sets (all covered entities who filed for an extension and small health plans)
April 14, 2004	Privacy—small health plans
July 30, 2004	Employer identifier standard (all covered entities except small health plans)
April 21, 2005	Security standards (all covered entities except small health plans)
August 1, 2005	Employer identifier standard (for small health plans)
April 21, 2006	Security standards (for small health plans)

HIPAA TRANSACTIONS AND CODES

HIPAA is named for its contribution to portability of insurance and accountability for insurance claims. The administrative simplification section of HIPAA requires the standardization of identifiers, code sets, and transactions. HIPAA provides various safeguards for the insurance options of individuals and groups. The regulation provides limits to the exclusions that insurers may use, provides credit for past insurance, and attempts to assure that insurance can be purchased. As stated previously, HIPAA ensures only that insurance is available, not that it is inexpensive.

HIPAA required the implementation and acceptance of standards for financial and administrative transactions. These include:

- Health care claims and encounter data;
- Health care payment and remittance for the explanation of benefits;
- Health care claim status;
- Enrollment and disenrollment in a health plan;
- Health plan premium payments;
- Patient certification and authorization;
- Health claims documents; and
- First report of injury.

Providers submit claims, receive advice, coordinate benefits, review claims status information, determine eligibility verification, provide first report of injury, and file health claim documentation. HHS has not yet promulgated a regulation addressing "first report injury."

HIPAA includes the designation of funds for fraud investigation. For HIPAA compliance, the American National Standards Institute (ANSI) develops standards for interindustry electronic exchange of business transactions. ASC X12 develops, maintains, interprets, publishes and promotes the use of standards for electronic interchange formats. The largest subcommittee in X12 is the Insurance Subcommittee, called X12N (responsible for the development and modification of standards and guidelines for insurance). A standing task group of the X12N is the X12N Insurance Subcommittee , which develops standards and industry implementation guides in the areas of health care and health insurance administration. The average intended flow of X12N transactions is illustrated in Figure 2.1 (*5*). The numbers in the figure are used to reference the standards. For example, the claim is called 837, the remittance 835, and the managed care request is 278.

The fields in the transactions are filled with data from identifiers and code sets. Final regulations on these identifiers have been published. The effective date for the national provider identifier identifier is May 23, 2005, and for the employer identifier was July 30, 2002. The national provider system has two sets of identifiers: the national provider identifier (an 8-digit alphanumeric identifier) and the national provider file (many fields that contain checkboxes for information about the licenses held by the provider and the location of the provider).

Code sets that are specified in the X12N standard include:

- *International Classification of Diseases*, 9th edition, Clinical Modification (ICD 9-CM) volumes 1, 2, and 3. The ICD10-CM Classification is soon to be released.
- *National Drug Codes*.
- *Code on Dental Procedures and Nomenclature*.
- *Health Care Financing Administration Common Coding System*.
- *Current Procedural Terminology*, 4th edition.

The use of HIPAA transactions and sets has been estimated at an annual savings of between $8.9 and $20.5 billion (*6*).

HIPAA PATIENT PRIVACY REQUIREMENTS

On April 14, 2003, all health care providers, health plans, and health care clearinghouses were to be in compliance with the standards designed to protect the privacy of an individual's health information. An exception was made for small health plans, for which compliance was delayed by 1 year. The privacy standards were mandated by HIPAA (Act of 1996) and were the result of two rule makings (one issued on December 28, 2000, and another issued on August 14, 2002). Responses to these two proposed rules were extensive. More than 52,000 responses were received by HHS regarding the original proposed rule, and an additional 11,400 were received regarding the March 2002 proposed modifications (*7*). As the health care

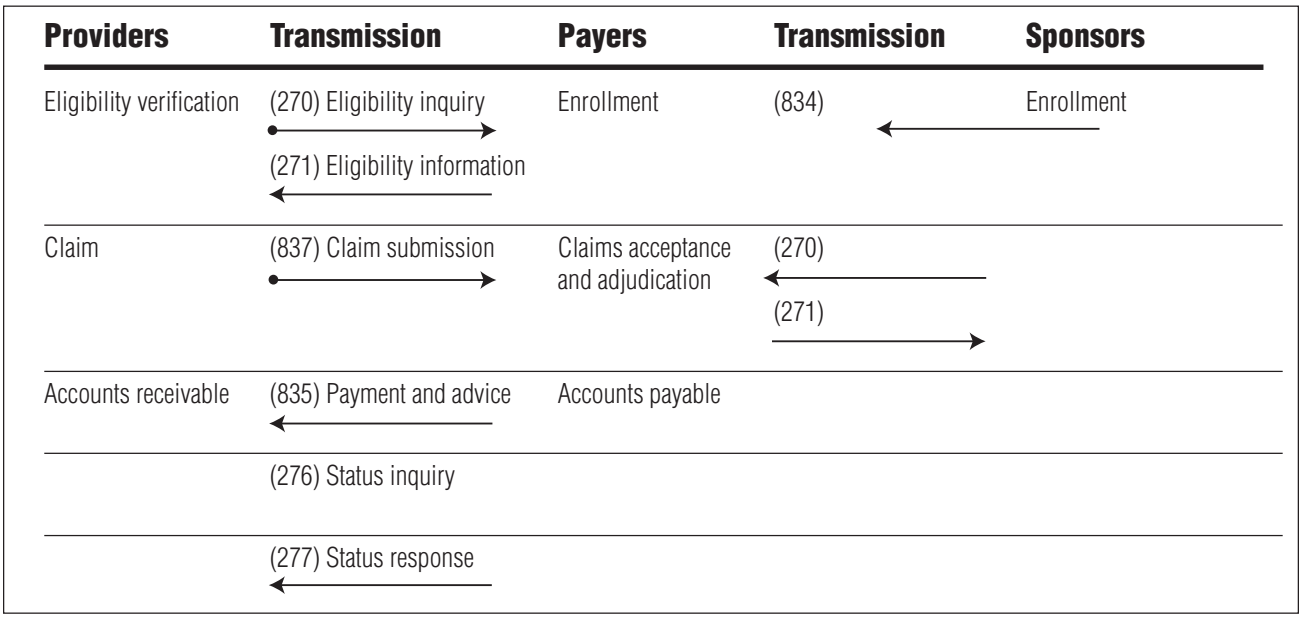

Figure 2.1 Typical Flow of X12n Transactions

industry continues toward compliance with the privacy regulation, it is also working toward compliance with the HIPAA security standards. The final HIPAA standard security rule was developed to parallel the privacy rule.

In addition to the previously cited final rules, HHS has issued the following sets of regulations to implement the HIPAA privacy rules:

- Office of Civil Rights (OCR): statement of delegation of authority (*Fed Reg*. Dec. 28, 2000; 65:68238).
- Notice of address for preemption exception determinations (*Fed Reg*. March 11, 2003;68:11554).
- Notice of addresses for submission of HIPAA health information privacy complaints, 68 (*Fed Reg*. March 20, 2003;68:13711).

The OCR, located within the HHS, has the authority to administer the HIPAA privacy standards. OCR makes decisions about the privacy standards, including their enforcement and civil monetary penalties.

The HIPAA regulations pertaining to the privacy of individually identifiable health information are in U.S.

Code of Federal Regulations (CFR), Title 45–Public Welfare, Part 160, General Administrative Requirements, which applies to all HIPAA standards, not just privacy, and Part 164, Security and Privacy. The privacy standards govern the use and disclosure of PHI and give individuals control over their PHI. The December 2000 final rule required health care providers to obtain written consent from each individual before providing treatment. Because this requirement would have been overburdensome and would undoubtedly have had a negative effect on patient care, HHS eliminated this consent requirement in the August 2002 final modification and now simply requires that covered entities inform patients of information privacy practices and policies. The final regulations allow covered entities to use and disclose PHI for treatment, payment, and health care operations (TPO), which encompass a vast array of health-related activities, thus relieving covered entities from the administrative burden created by the former consent requirement.

Without obtaining the individual's authorization, covered entities are permitted to utilize or disclose PHI:

- To the individual to whom the PHI pertains;
- For purposes of TPO;
- To another covered entity for the health care operations of the entity receiving the information;
- With valid authorization;
- If the covered entity has received the individual's oral agreement for the use of the PHI; and
- In instances where the law requires such disclosure.

The privacy standards require all covered entities to make "reasonable efforts" to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request of PHI (45 *CFR*, Part 164, Security and Privacy, Section 164.502 (b) (1), minimum necessary). Covered entities are required to develop policies and procedures that address the minimum necessary standard, which is intended to be consistent with professional judgment and standards based on their own assessments of what PHI is reasonably necessary for a particular purpose. There are exceptions to the minimum necessary requirements, such as in the case of "incidental disclosures," provided that the covered entity has taken appropriate actions to comply with the general privacy provisions. For example, a situation in which information is inadvertently overheard by a third party during a conversation with the patient is not necessarily considered a violation of the privacy standard. Many providers were initially concerned that HIPAA privacy requirements would include extensive measures, such as building soundproof rooms or eliminating patient sign-in sheets. However, because of the "incidental disclosure" exception, covered entities have an easier task.

HIPAA prohibits the disclosure of PHI data that identifies an individual patient or is believed to identify an individual. HHS has proposed two methods to release PHI data under some circumstances.

De-Identified Data

De-identified (45 *CFR*, Part 164, Security and Privacy, Section 164.514 (b) (2) (1)) data refers to the removal of the following classes of data from a PHI file:

- Names;
- Geographic subdivisions;
- Dates directly related to an individual (birth date, admission date, etc.);
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan identifiers/numbers;

- Account numbers;
- License numbers;
- Vehicle identifiers and serial number;
- Device identifiers and serial numbers;
- URL Web resource locators;
- Internet protocol (IP) address number;
- Biometric identifiers;
- Face photographic images; and
- Any other unique identifying number or characteristic code.

It is clear that de-identifying individually identifiable health data requires the removal of so many items that the remaining data is useless for many purposes.

Limited Data Set

A HIPAA limited data set using PHI is intended to accomplish the purposes of research, public health, or health care operations (45 *CFR*, Part 164.514 (e) (1)). The limited data set also is PHI, and other restrictions of the privacy standards apply.

Individuals' Rights

The HIPAA of 1996 grants individuals rights regarding their personal health information. These rights include:

- The right to notice of the uses and disclosures of PHI that a covered entity may have made (45 *CFR* 164.520);
- The right to request (not necessarily receive) restrictions on the use and disclosure of PHI (45 *CFR* 164.522);
- The right to access PHI (45 *CFR* 164.524);
- The right to request amendments (not necessarily receive) to PHI (45 *CFR* 164.526); and
- The right to an accounting of certain disclosures of PHI (45 *CFR* 164.528).

Any denial of an individual's rights under the privacy rule is subject to enforcement by the HHS OCR.

Under the privacy regulations, individuals have the right to request restrictions upon the use and disclosure of PHI (45 *CFR* 164.522). However, covered entities may exercise discretion in honoring such requests. Individuals are limited to the types of uses and disclosures for which they may request a restriction. Covered entities must permit individuals to request restriction of:

- Uses and disclosures of PHI about the individual to carry out TPO; or
- Disclosures permitted under 45 *CFR* 164.510 (b), uses and disclosures to family members and to others involved in the individual's care.

Covered entities are required to take action on a request relative to PHI within 30 days of the request when the PHI is on site. The action must be taken within 60 days when the data are not on site. An additional 30 days are provided if the covered entity provides a written statement to the individual stating the reason for a delay and the date by which the covered entity will take action.

An important right provided to the individual by the HIPAA privacy standard is the right to amend his or her health information (45 *CFR* Part 164.526). It does not ensure that all requested amendments will be made but, instead, provides a mechanism for requesting changes to erroneous or incomplete information. An individual is provided the right to have a covered entity amend PHI in a record set for as long as the PHI is maintained in the designated record set. However, this request can be denied by a covered entity, provided that it complies with the administrative and procedural requirements prescribed by the privacy regulation specifically pertaining to the circumstances surrounding such denials, including:

- The covered entity did not create the PHI or record;
- The PHI or record is not part of the designated record set;
- The PHI or record would not be available for inspection (45 *CFR* Part 164.524); or
- The PHI record is accurate and complete.

Under the HIPAA privacy standards, individuals have the right to receive an accounting of certain disclosures of their respective PHI made by a covered entity (45 *CFR* Part 164.528). Disclosures regarding TPO do not need to be accounted for. The exceptions to this portion of the HIPAA privacy standards include:

- Time exclusions (accounting of disclosures is limited to 6 years before the date of request);
- Subject matter exclusions (individuals do not have the right to an account of disclosures that were TPO, permissible disclosure, purposes of a limited data set, purposes under 45 *CFR* Part 164.510;
- Authorization provided by the individual;
- Recipients (made to the individual or made to law enforcement officials under 45 *CFR* Part 164.512 (k) (5));
- Research;
- Victims of neglect or child abuse; or
- Suspension of accounting rights.

The final privacy standards that govern disclosure as of April 14, 2003, specify six circumstances under which a covered entity is permitted to use or disclose PHI:

- When the disclosure is to the individual to whom the PHI pertains;
- For treatment, payment, or health care operations (TPO) in compliance with 45 *CFR* Part 164.506;
- As long as compliance with the minimum necessary standard of the rule (45 *CFR* Part 164.502 (b), 164.514 (d)) and the administrative requirements (45 *CFR* Part 164.508) are satisfied;
- When the covered entity receives a valid authorization (45 *CFR* Part 164.508);
- When the covered entity has obtained the individual's oral agreement (45'*CFR* Part 164.510); or
- When the covered entity is permitted to do so (45 *CFR* Part 164.512).

The privacy standards require that a covered entity disclose PHI in the following two circumstances:

- When an individual requests an accounting of the disclosures of his/her PHI (45 *CFR* Part 164.528); and
- When requested by the Secretary of HHS (45 *CFR* Part 160.306 (c)).

The HIPAA privacy standards no longer require a patient's consent to conduct health care treatment, payment, or operations. Section 45

CFR 164.509 enables covered entities to use or disclose PHI without an individual's prior permission or authorization. State laws that require consent for the use of PHI have precedence over the HIPAA privacy standard. HHS often describes the HIPAA standards as a "floor."

The HIPAA privacy regulations require that a covered entity may not use or disclose PHI for nonroutine purposes without a written authorization. Research is not considered a routine purpose, except for certain studies such as those on quality assurance or management functions. The use or disclosure of PHI for research requires a written authorization from the individual from whom the PHI is collected. The privacy rules now authorize several methods for disclosing PHI without an individual's authorization:

- The use of de-identified PHI;
- A limited data set; or
- Approval of an institutional review board or privacy board to waive informed consent requirements.

Under 45 *CFR* Part 164.508, a covered entity that generates PHI for the purpose of research must obtain an authorization for the use or disclosure of such information.

The HIPAA privacy requirements state that covered entities must protect all PHI regardless of how it is generated, transmitted, or stored, by implementing reasonable safeguards to ensure that PHI is not used or disclosed in an improper manner. Documents on paper that contain PHI must be protected. This requires written protocols to protect the storage of paper-based data. CDs containing PHI must be protected. Protecting PHI during telephone calls in which such information is requested or disclosed can be difficult. It is important to create safeguards to make certain that persons who call with requests for PHI are who they claim to be. Patient privacy can be violated when PHI and patient names are left in voice mail messages or on telephone answering machines. E-mails are easy to send to many people and are accessible to others.

Health care providers and other covered entities typically require the services of various third parties to assist in effective administration operations. The business associate rules in the HIPAA privacy requirements (45 *CFR* Part 164.502 (e) and 45 *CFR* Part 164.504 (e)) require that a covered entity (such as a health plan, hospital, or medical group) ensure that these third parties adhere to information privacy standards at least as stringent as those imposed on the covered entity. The covered entity is required to obtain a written agreement, executed by the business associate, granting the covered entity adequate assurances that it will safeguard any PHI it receives, maintains, or uses in the course of performing functions on behalf of the covered entity.

Another obligation imposed on covered entities under the HIPAA privacy standard is conducting an ongoing effective and comprehensive training program for all members of the entity's workforce. Appropriate training is of utmost importance in achieving and maintaining compliance with HIPAA privacy requirements.

HIPAA SECURITY REQUIREMENTS

The HIPAA security standards are intended to protect electronic PHI while at "rest," during processing, and during transmission (*8*). The structure of the HIPAA regulations is as follows:

- 45 *CFR*, subchapter C, Administrative Data Standards and Other Related Requirements presents the HIPAA regulations.

- 45 *CFR* Part 160 presents the general administrative requirements for all HIPAA regulations. These include transactions and code sets, identifiers, privacy and security.
- 45 *CFR* Part 162 presents the transactions and code sets as well as the national identifier regulations.
- Subpart A of Part 164 contains the general provisions that apply to both privacy and security.
- New Subpart C, Part 164.302–164.318, presents the security standards for the protection of electronic PHI.
- Subpart E, Part 164.500–164.534 presents the requirements specific to privacy.

HIPAA regulation 45 *CFR* Part 164.104 requires that the privacy as well as the security standards apply to (a) health care plans; (b) health care clearinghouses, and (c) health care providers who transmit health data in electronic form for transactions. Covered entities that require assistance or service from third-party business organizations must have business associate agreements in place to comply with both security and privacy rules.

The final Security Rule requires that covered entities assure the integrity, confidentiality, and availability of PHI that is electronically transmitted, created, maintained, or received, by implementing appropriate and reasonable administrative, technical, and physical safeguards. A covered entity is also required to protect against any reasonably anticipated threats or hazards to the security or integrity of protected information, as well as against reasonably anticipated uses or disclosures. Further, the covered entity's entire workforce must undergo training to ensure the most complete levels of compliance possible.

Researchers, however, are not covered entities unless they are part of a covered entity's workforce. Researchers then are not subject to the security standards but are subject to the use and disclosure requirements of the privacy standards. The security standard applies to PHI that is transmitted or maintained in electronic media. It protects a smaller range of information than the privacy standard, which does not distinguish the stored form of information (paper, oral, electronic).

The security requirements remain technologically neutral and are intended to be scalable to each organization. Considerations such as cost, available resources, risk assessments, etc., remain to be considered by each organization on an individual basis when determining what measures will constitute "reasonable," for compliance purposes.

The HIPAA security standard is organized into the following three major areas:

- Administrative safeguards (45 *CFR* Part 164.308);
- Physical safeguards (45 *CFR* Part 164.310); and
- Technical safeguards (45 *CFR* Part 164.312).

There are also two administrative standards:

- Organizational requirements (45 *CFR* Part 164.314); and
- Policies and procedures and documentation requirements (45 *CFR* Part 164.316).

The security standards' implementation specifications are designated as either required or addressable. Each standard gives the covered entity information on what is required, whereas the implementation specifications indicate ways in which the standard may be met. Where the implementation specifications list options for the covered entity, the specification will be deemed "addressable." Alternatively, the regulation will deem an implementation specification "required," indicating the HHS position that compliance with the specification is essential to the overall security objectives.

Some of the implementation specifications are "required," and others are "addressable." Required implementation specifications must be implemented. Table 2.2 is the security matrix that appears in the final rule.

The HIPAA privacy standards regulate information practices and grant individual rights with respect to the control of personal information, including the determination not to have such information divulged or used by others against their wishes. The HIPAA security requirements apply to the physical, technical, and administrative safeguards imposed to protect patient's data while in electronic form. The security rule identifies 14 standards for the administrative, physical, and technical safeguards with "required" and "addressable" implementation specifications for covered entities.

Both the privacy and security rules require covered entities to designate an individual to be responsible for the oversight of policies and procedures within each covered entity. The privacy officer is responsible for the development and implementation of the policies and procedures for the privacy of PHI in any format (45 *CFR* Part 164.530(a)(1)(i)). The security officer is responsible for the development and implementation of the policies and procedures regarding the security of the entity's electronic PHI (45 *CFR* Part 164.308(a)(2)).

TABLE 2.2
HIPAA Security Matrix

Standards	Sections	Implementation
ADMINISTRATIVE SAFEGUARDS		
Security management policies	164.308 (a) (1)	Risk analysis (R) Risk management (R) Sanction policy (R) Information system review (R)
Assigned security responsibility	164.308 (a) (2)	(R)
Workforce security	164.308 (3)	Authorization (A) Workforce clearance (A) Termination procedure (A)
Information access management	164.308 (a) (4)	Health care clearinghouse (R) Access authorization (A) Access establishment (A)
Security awareness and training	164.308 (a) (5)	Security reminder (A) Protection software (A) Log-in monitoring (A) Password management (A)
Security incident procedures	164.308 (a) (6)	Response and reporting (R)
Contingency plan	164.308 (a) (7)	Data backup (R) Disaster recovery plan (R) Testing procedure (A) Application and data analysis (A)
Evaluation	164.308 (a) (8)	(R)
Business associate	164.308 (b) (1)	Written contract (R)
PHYSICAL SAFEGUARDS		
Facility access controls	164.310 (a) (1)	Contingency operation (A) Facility security plan (A) Access control and validation procedure (A) Maintenance records (A)
Workstation use	164.310 (b)	(R)
Workstation security	164.310 (c)	(R)
Device and media controls	164.310 (d) (1)	Disposal (R) Media reuse (R) Accountability (A) Data backup and storage (A)
TECHNICAL SAFEGUARDS (164.312)		
Access control	164.312 (a) (1)	Unique user identification (R) Emergency access procedure (R) Automatic logoff (A) Encryption and decryption (A)
Audit controls	164.312 (b)	(R)
Integrity	164.312 (c) (1)	Method to authenticate electronic protected health information (A)
Person or entry authentication	164.312 (d)	(R)
Transmission security	164.312 (e) (1)	Integrity controls (A) Encryption (A)

R = required; A = addressable.

The first two implementation requirements for the security management process require a covered entity to conduct a risk analysis and implement a risk management program. The final security rule defines the specification (45 *CFR* Part 164.308(a)(1)(ii)(A)) and requires the covered entity to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." The risk analysis is accomplished by the provider, identifying all possible vulnerabilities at each location of business that would threaten an ability to provide services. The second required implementation specification under the security management process is a risk management program (45 *CFR* Part 164.308(a)(1)(ii)(B)). It requires that covered entities reduce risks to a reasonable and appropriate level to comply with general security standards (45 *CFR* Part 164.306(a)).

The contingency plan standard (45 *CFR* Part 164.308(a)(7)(i)) is an example of one of the security regulation's administrative safeguard standards. This standard has the following implementation specifications:

- Data backup plan (required);
- Disaster recovery plan (required);
- Emergency mode plan (required);
- Testing and revision procedures (addressable); and
- Applications and data criticality analysis (addressable).

As is true under the privacy regulation, HIPAA security requirements dictate that organizations provide security training to their employees. It is up to the covered entity to set the degree of training and the training programs by which the PHI security is achieved. Often, when a compliance date looms, it is attractive to train everyone at once. However, this method has drawbacks in terms of the bandwidth needs of a training system. Training software is expensive. It is best to provide training in waves (employees are given different start times to provide a staggered schedule). An attractive means is the use of a learning management system, an online system with Web applications, enabling access with a browser.

The fifth standard under technical safeguards is transmission security (45 *CFR* Part 164.312(e)). This standard requires that the covered entity must secure the internal and external transmission so as to receive the same level of protection. Virtual private networks (VPNs) can provide security. VPNs are often used to replace frame relay, dedicated leased lines, and dial-up lines. Firewalls are physical devices or software agents that filter packets going into or out of a site based on a set of policy rules. Hospitals often use firewalls for input/output of data for inter transmission. VPNs are used for inter transmission of medical data.

SECURITY ISSUES IN NETWORKS

45 *CFR* Part 164.306(a) of the security standards establishes four overall compliance requirements for covered entities:

- Ensure the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E (45 *CFR*, Part 164, Subpart E, Privacy of Individually Identifiable Health Information); and
- Ensure compliance with this subpart by its workforce.

A number of principles have been cited (*9*) and proposed to guide designers and administrators when building a network that is to meet defined security requirements.

- Know the configuration of the network's hardware and software;
- Identify the vulnerabilities of the configuration;
- Know the threat and consider it in relation to the vulnerabilities to assess the risks;
- Authenticate and authorize access to the network resources;
- Maintain audit logs;
- Develop plans to detect and respond to security incidents; and
- Ensure individual accountability.

Just as each covered entity will be affected by these regulations in different ways, specific departments within each covered organization will be impacted differently. Adequate representation and participation by each department within a covered entity's organization will produce significant benefit throughout the entire compliance process. Radiology, for example, will be substantially impacted by the Security Regulation, because of the nature of the information flowing through the department. With the growing use of electronic means to view, transmit, maintain, create, and store information, the se-

curity measures implemented by any covered entity will impact both internal radiology departments and outside sources transmitting and receiving images and related information. Department-specific measures may require more extensive consideration and evaluation in terms of storage requirements, specific technical security mechanisms, and physical security measures.

Evaluating and taking inventory of business associate agreements, now required under the Security Regulation, also will be a task that may have implications specific to radiology and should be brought to the attention of the organization's privacy officer or HIPAA compliance coordinator. Because of the potential risks associated with some functions performed by third-parties (for example radiology information systems, picture archiving and communications systems, and modality vendors with remote access) or those providing maintenance service (especially after hours, or off site), business associate agreements may be tailored to address certain functions that the organization's standard or boilerplate model does not take into account.

The "user friendly" nature of the final Security Regulation provides a better guide for covered entities and even for third-party industry partners than its predecessor, the proposed regulation. Covered entities should understand that implementation is an industry-wide learning process and will be modified over time, not only through individual application to each covered entity but also through enforcement and future litigation. Every organization will have a unique approach to compliance efforts. The "culture change" required, however, with respect to information privacy and security, spans departmental, organizational, and industry lines. Seeking cooperation both inside each covered entity organization as well as from outside sources, such as third-party business associates, will be instrumental in developing the most thorough and practical compliance strategies.

REFERENCES

1. Rada R. *HIPAA @ IT: Health Information Transactions, Privacy, and Security*. Hypermedia Solutions Limited; 2001:7.
2. Amatagakul M, Cohen MR. *HIPAA Transactions Made Simple*. Marblehead, MA: hcPro, Inc.; 2003.
3. Landrigan D, ed. *HIPAA Security Compliance Guide*. Washington, DC: Atlantic Information Services, Inc.; 2003:100.8.
4. Landrigan D, ed. *HIPAA Security Compliance Guide*. Washington, DC: Atlantic Information Services, Inc.; 2003:100.9.
5. Amatayakul M, Cohen MR. *HIPAA Transactions Made Simple*. Marblehead, MA: hcPro, Inc.; 2003:4.
6. Rada R. *HIPAA @ IT: Health Information Transactions, Privacy, and Security*. Hypermedia Solutions Limited; 2001:44.
7. Fernald FR, ed. *HIPAA Patient Privacy Compliance Guide*. Washington, DC: Atlantic Information Services, Inc.; 2003:100.7.
8. Landrigan D, ed. *HIPAA Security Compliance Guide*. Washington, DC: Atlantic Information Services, Inc.; 2003:100.7.
9. Landwehr CE, Goldschlag DM. Security issues in networks with Internet access. *Proc IEEE*. 85;1997:2034–2051.