

The Health Insurance Portability and Accountability Act: Security and privacy requirements

DENNIS A. TRIBBLE

In 1996 President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law.¹ The act is principally aimed at facilitating the continuation of health care insurance coverage for people leaving jobs. It contains five sections: Title I, on guaranteeing health insurance access, portability, and renewal; Title II, on preventing health care fraud and abuse; Title III, on medical savings accounts and coverage for the self-employed; Title IV, on enforcing group health plan provisions; and Title V, on revenue offset provisions. Title II contains a subpart, "Administrative Simplification," that deals with the electronic communication of patient data, primarily for claims adjudication, and that mandates regulations to protect the security and privacy of such information. The security regulations were issued for comment on August 12, 1998, and are expected to be finalized in the spring of 2001. The privacy regulations were finalized on December 28, 1998. Through this act, Congress hopes to reduce paper-processing costs by as much as \$2 billion per year.² The Department of Health and Human Services (DHHS) estimates that the cost of compliance will exceed \$5 billion over five years for the security regulations and \$3 billion for the privacy regulations.³

One cannot discuss the electronic

Abstract: The security and privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their implications for pharmacy are discussed.

HIPAA was enacted to improve the portability of health care insurance for persons leaving jobs. A section of the act encourages the use of electronic communications for health care claims adjudication, mandates the use of new standard code sets and transaction sets, and establishes the need for regulations to protect the security and privacy of individually identifiable health care information. Creating these regulations became the task of the Department of Health and Human Services. Regulations on security have been published for comment. Regulations on privacy and the definition of standard transaction sets and code sets are complete. National identifiers for pa-

transfer of health care information without first establishing a common dialect for the transfer of that information and without raising fears about loss of privacy. As a result, HIPAA calls for regulations that establish standards for encoded data and message syntax to provide a lingua franca for health care information exchange, regulations to provide for health care data security, and regulations protecting the privacy of health care records. It is un-

tients, providers, and payers have not yet been established. The HIPAA regulations on security and privacy will require that pharmacies adopt policies and procedures that limit access to health care information. Existing pharmacy information systems may require upgrading or replacement. Costs of implementation nationwide are estimated to exceed \$8 billion. The health care community has two years from the finalization of each regulation to comply with that regulation.

The security and privacy requirements of HIPAA will require pharmacies to review their practices regarding the storage, use, and disclosure of protected health care information.

Index terms: Administration; Costs; Health Insurance Portability and Accountability Act; Laws; Patient information; Pharmacy; Regulations

Am J Health-Syst Pharm. 2001; 58:763-70

likely that the HIPAA requirements involving data codes and message syntax will directly affect pharmacy practice. However, the data security and privacy regulations will require pharmacists to review their current information systems and practices regarding access to and use of patient medical records.

Ideally, all individually identifiable health care information would be released only to people who absolutely need it and only on the express

permission of the involved patient. Realistically, however, the daily conduct of health care (in terms of both rendering care and seeking reimbursement) requires that health care information be freely available to providers of care. In HIPAA terms, such uses or disclosures fall into the categories of treatment, payment, and health care operations.

HIPAA's privacy regulations therefore attempt to define what uses or disclosures of this information represent the normal conduct of health care and those that are exceptional and then to define control measures for each. Privacy regulations extend to individually identifiable health records from any source (not just electronic) and broadly affect who may see such records and what portions they may see. These regulations therefore affect clinical practice, research, and publication.

Storing, retrieving, and transmitting patient information electronically present hazards both in terms of increased availability of that information to unauthorized persons and in terms of that information not being available when needed because of system failures. The security regulations therefore attempt to define the measures that must be in place to ensure that electronically stored information is available to those who need it when they need it, that it is properly authenticated, and that it is protected from use or disclosure by unauthorized persons.

HIPAA perceives health care information as being appropriately distributed on a need-to-know basis. The use or disclosure of health care information for any purpose should be limited to that subset of the information necessary for the task at hand. It will therefore be important for pharmacists to establish their need for access to such information.

This article does not represent a legal opinion; rather, it is intended to identify the requirements of HIPAA

associated with security and privacy and to discuss the potential impact on pharmacy practice.

Scope of HIPAA

The act claims as its scope health care providers and payers who electronically maintain or transmit individually identifiable (protected) health care information. Such records are considered to come under HIPAA's jurisdiction if they are currently or ever have been stored electronically.^{4,5} Recently released privacy regulations have extended that jurisdiction to all protected health care information from any source. Thus, hospitals, home health care agencies, pharmacies, clinics, physicians' offices, extended care facilities, and research facilities fall under HIPAA's security and privacy regulations if any of the records they keep are included under this definition. Indeed, only an office that maintains entirely handwritten paper records could be exempted. Similarly, payers whose records fit the above definition, all or in part, are subject to HIPAA (and must retrofit their claims processing to comply with new message sets and codes). Finally, indirect providers, such as contract laboratories and outsourcing providers, fit this definition because their operations require them to keep individually identifiable health care information. These providers and payers are collectively referred to as covered entities.

Protected health care records

Neither the act nor the regulations specify what makes a health care record individually identifiable and therefore protected; that is left to the judgment of the covered entities. In a town of 50 people, identifying someone as a 35-year-old man with brown hair might provide enough information to identify a person. In New York City it surely would not. While it is possible to "deidentify" records

for various purposes (such as research), this process may render the data practically useless.⁶

The recently released privacy regulations describe deidentified health care information as that which "does not identify an individual and with respect to which there is no reasonable basis to believe that the information [within the record] can be used to identify an individual."⁷ Those regulations further indicate that the following identifiers cannot be present in deidentified health care information: name, geographic subdivision smaller than a state, any date or element of a date (other than year) referable to an individual, telephone number, fax number, electronic mail address, social security number, health plan beneficiary number, account number, certificate or license number, vehicle identifier and serial number (including license plate number), device identifier and serial number, web universal resource locator, Internet protocol address, biometric identifier (including fingerprints and voice prints), full-face photographic image and any comparable image, and any other unique identifying number, characteristic, or code.

As an alternative, the regulations permit a statistician to assert that the risk of identification is sufficiently small that protected information is considered to be deidentified, as long as generally accepted tools and techniques are used and the methods and results used to make this determination are documented.

Cost of compliance

The secretary of DHHS estimates that the total cost of implementing HIPAA will exceed three times the cost of the Y2K conversion. The privacy regulations contain estimates that first-year compliance costs will exceed \$2 billion, with an average annual cost thereafter of slightly less than \$1 billion.⁸

Enforcement

Congress established penalties for noncompliance and for unauthorized disclosure of protected information but did not establish or fund enforcement for HIPAA. DHHS has commissioned the Office of Civil Rights as the agency that will enforce HIPAA regulations,⁹ but funding and staffing issues have yet to be resolved.

DHHS recognizes that there is a broad spectrum of providers that fall under the definition of "covered entities" and that the regulations may be unduly burdensome for small provider practices. It therefore remains to be seen how it will enforce compliance. It also remains to be seen if other regulatory or quasi-regulatory agencies (such as the Joint Commission on Accreditation of Healthcare Organizations) will choose to enforce compliance with HIPAA as part of quality standards. Privacy litigation seems another likely method of HIPAA enforcement.

Security regulations

The proposed regulations for security identify four categories of security concerns: administrative, physical barriers, technical, and networking and communications. The regulations also address electronic signatures.¹⁰

The security regulations seek to impose reasonable safeguards as indicated by the potential sensitivity of the information. This means that a covered entity may choose not to implement, or may choose to minimally implement, some of the actions identified as "required" but that it must document its consideration of all the required actions and the rationale for enacting or not enacting these features.

Administrative security regulations. The proposed administrative security regulations establish the need for management oversight of information systems and for policies and procedures that define how security will be established, maintained,

and audited. Procedures must include the following¹¹:

- Contingency plans, including regular backup plans, emergency-mode operations, and testing.
- Formal mechanisms for processing protected information, including controls over access to protected information.
- Audit mechanisms to ensure that access controls are properly implemented.
- Security configuration management, including documentation, hardware and software installation and review procedures, security testing, and virus checking.
- Procedures for reporting incidents involving failure to comply with procedures.
- Procedures (1) for assessing the risk of unauthorized use or disclosure of protected information created by the use of information systems and (2) for minimizing that risk.
- User training and certification of competency in security procedures.
- Penalties for failing to comply with established policies and procedures and for knowing about but not disclosing breaches of information security.

For pharmacies that are part of larger institutions, these procedures may be written and implemented by an information systems or quality assurance department. It is likely, however, that the pharmacy department will be required to enact its own policies and procedures, at least those involving pharmacists' and other personnel's use of departmental and institutional information systems.

Regulations requiring physical barriers. The proposed regulations require physical barriers to the unauthorized use of terminals or workstations that might provide access to protected health care information. Pharmacies are perhaps fortunate in that they have other more pressing reasons for implementing controls

over access. Nonetheless, it will be important to ensure that more publicly available terminals (e.g., those at reception areas and in administrative offices) be appropriately secured against unauthorized use. This may involve restricting access to applications that may display protected health care information (such as billing and clinical applications) to terminals where access is more closely controlled or mandating password-controlled screensavers.

Maintaining limited access to terminals in more public areas of a hospital will be harder. Some pharmacists may use terminals placed on nursing units or mobile (i.e., wireless) terminals to access health care data. If left logged on, these terminals could be used to access protected information by those not authorized to do so. Provisions in the regulations on technical security address such issues.

Requirements for physical barriers include procedures for media control, including access control, backup, offline storage, and disposal of information, especially for removable media.¹² This would include proper use of log-ins, the transfer of protected information to floppy disks or CD-ROMs, proper management of backup data, and disposal of floppy disks or CD-ROMs that might have protected information on them. Also required are procedures for proper control of visitors, need-to-know access, emergency-mode operation, facility security, disaster recovery, maintenance records, and records of testing or revision of controls over physical access.

Technical security regulations. The proposed technical security regulations address the need to ensure that electronically stored data are available, that data are properly authenticated, and that data are displayed only to properly authorized users. Specified are software features needed to implement technical security¹³:

- *Access controls, including context-based access, procedures for emergency access, role- and user-based permissions, and optional encryption.* Software must be sufficiently “intelligent” that its display of information may be based on the user or the terminal location. Also, there must be plans to ensure the availability of electronically stored data when the information system is not available. For users whose systems become unavailable every night for several hours (e.g., for backup), there will have to be either procedures for acquiring data during that time or a defense that such loss of availability does not compromise clinical function.
- *Regular audits of software that accesses protected health care information to ensure that the software complies with technical requirements.* Pharmacists will probably have to review all their current software products against these technical requirements, perform the same review whenever those products are upgraded, and review any newly acquired software products as they are installed.
- *Controls to ensure that only authorized health care providers have access to individually identifiable health care data.* The software should use security levels or permissions to limit what any individual may see (as opposed to treating all users the same way).
- *Data authentication to ensure that the data have not been improperly altered.* It may be necessary to maintain trails of database changes for audits, use database read-write validation, and have both programmatic and policy-based limitations to accessing an underlying database without going through the application. For example, a program written in Microsoft Access that contained protected health care information would fail to comply with this requirement if anyone knowledgeable in the use of Access could modify the data and avoid detection.
- *Entity (user) authentication to ensure that the user is truly an authorized user,*

including at a minimum automatic log-off, unique user identification, and verification of user identity in the form of a password, telephone call-back, personal identification number, token, or biometric identifier. The regulations require unique user identification, automatic log-off, and one of the other items in the list. Compliance thus has both a technical and a behavioral component. The fact that a software product supports (for example) automatic log-off, unique user identification, and a password does not guarantee compliance. If the users of the software have the same identifier or password or share their identifiers or passwords (e.g., leave a note on the terminal with the log-in information), then the program is not HIPAA compliant.

Given the act’s emphasis on need-to-know information, it will be useful to maintain a document that records what permissions are to be given to each class of user and why those permissions are necessary to their function.

Security regulations for networking and communications. These regulations address protecting health care information as it is transmitted over networks within and among computer systems. Local area and wide area networks are similar to old-fashioned party-line telephone systems. All messages on the network go to all locations; destinations are simply polite enough not to listen to messages not intended for them. There are network applications called sniffers that lack such civility and scan every data packet that crosses their path. These are necessary and useful in managing and troubleshooting networks, but they can also be used to monitor data traffic on a network and acquire protected health care information.

Network security therefore requires that such records be transmitted over connections or in formats that cannot be readily read by

such devices. Encryption is a cornerstone of this type of security. However, not all transactions can be encrypted. For example, network printers currently do not support decryption of data streams. Therefore, information sent to network printers (whether for labels, patient profiles, face sheets, or just reports) are “sniffable.” Local area networks in hospitals are generally considered secure; the concern is directed primarily at communications over open lines, such as dial-in connections or the Internet.

The current wording of the proposed regulations requires that the following features be applied to the transmission of individually identifiable health records across a network¹⁴:

- *Message authentication to ensure that messages transmitted across the network are not corrupted and are completely received.* Most network operating systems and protocols (e.g., Transmission Control Protocol/Internet Protocol, or TCP/IP) provide this type of assurance.
- *Integrity controls to ensure that the data transmitted are properly qualified.* That is, it should be difficult or impossible to fake a transmission in such a way that a receiving system would perceive it as authentic when it is not. Electronic signature or other user authentication plays a role in this.
- *Access controls.*
- *Encryption of data if using the Internet or another open network system.*
- *Alarms.* The regulations do not specify what alarms are or how they should function. Presumably alarms would notify a responsible party if the security of a network had been compromised.
- *Trails of networked activity enabling tracking of what messages have been sent across the network.* Typically these “audit trails” keep only a limited amount of historical information.
- *Event reporting when significant untoward events occur.*

For pharmacists, these requirements focus concern on pharmacy information system applications and other software applications in a pharmacy (e.g., a system for compounding total parenteral nutrient [TPN] solutions) or an investigational drug-tracking system) that maintain individually identifiable health care records. Steps in dealing with these requirements include the following:

1. *Assessing current information systems in terms of the sensitivity of the information and liability under the act.*
2. *Assessing current features in information systems for meeting the security requirements.* For example, what features exist within the software for access control, and how are those features used? If an information system provides automatic logging off after a specified time, is that feature enabled? If a system provides user authentication with user identification and passwords, are they being used? Are users publishing their unique identifiers for other users?
3. *Assessing current procedures for use of information systems and compliance with those procedures.* Do procedures cover all the requirements of the regulations? If they do, are the procedures being followed?

Electronic signatures. Electronic signatures are not a de facto requirement of HIPAA. However, electronic signatures may be required for specific transactions in the HIPAA message standards, or an institution may elect to require electronic signatures for specific functions. HIPAA requires that, where an electronic signature is used, it be created as a cryptographically based digital signature that meets four tests:

1. *Intent—the electronic signature must be created and affixed to the information at the time the information is “signed.”* One may not affix a previously created and stored image of a signature to electronically sign a

document. The signature must be generated at the time signing occurs. This is consistent with other federal electronic signature requirements (e.g., 21 C.F.R. part 11 for FDA).

2. *Message integrity—the transmission containing an electronic signature must be confirmed as having been received intact.*
3. *User authentication—when a document is electronically signed, the identity of the user must have been positively confirmed.*
4. *Nonrepudiation—having electronically signed a document, a user may not reasonably challenge the authenticity of his or her electronic signature.*

To the extent that pharmacists interact with an electronic medical record, they may be required to obtain and use electronic signatures. These requirements place a burden on users not to share, publish, or otherwise compromise their electronic signatures and imply that there must be policies and procedures regarding the creation, maintenance, and validation of electronic signatures.

Electronic signatures may be of concern if the pharmacy receives electronic prescriptions, especially from hand-held devices or other mobile computing devices. A graphic signature may fail to meet the requirements. That is, a prescription from a personal digital assistant (PDA) or other mobile device that is signed directly on the device and displays the signature as a “picture” of the handwritten signature may not be electronically signed since (a) it may not be a cryptographically based digital signature, (b) the PDA application may not properly authenticate the user, and (c) the PDA application may not be able to ensure that the signature was not forged.

To be compliant, the PDA would have to authenticate the user on the basis of how the signature was written on the device (a biometric identifier), generate a cryptographic digital signature that is based on that identi-

fication (in addition to, or in place of, the handwritten signature), and unalterably mark the information being signed with the digital signature when the signature was written on the PDA.

Privacy regulations

HIPAA’s recently released privacy regulations focus on patients’ rights to control access to their health care information and include documentation of compliance with patients’ wishes. The privacy provisions also contain penalties for wrongful disclosure of individually identifiable information. Unlike the proposed security regulations, the privacy regulations claim jurisdiction over all health care information, not just information stored, accessed, or transmitted electronically. The intent is to inform individuals of their privacy rights; provide patients with access to their electronic records; create administrative and physical safeguards for records; permit the use of patient records for treatment, payment, and health care operations; permit the disclosure of individually identifiable patient records in cases of national priorities; and require written authorization for all other releases and uses of health care information.¹⁵

Use or disclosure. The privacy regulations distinguish between *use* of protected health care information, which occurs within a covered entity, and *disclosure*, which occurs when a covered entity conveys protected information to someone else. Review of patient data for pharmacokinetic dosing within a hospital would be use; sending patient data to an i.v. admixture outsourcing facility would be disclosure.

Levels of control. The privacy regulations recognize that it is impractical to require explicit patient consent for each use or disclosure of protected information. The regulations therefore allow that there are uses and disclosures that must occur as part of routine rendering of care and

classify those uses as necessary for treatment, payment, or health care operations. The regulations require that a general consent be signed by the patient to permit the use or disclosure of protected information for these purposes. A patient must specifically authorize any activities not necessary for treatment, payment, or health care operations. These activities include research if it is not conducted under the auspices of an institutional review board.

The regulations recognize uses and disclosures that are sufficiently innocuous that neither general consent nor authorization is required, as long as the individual has the opportunity to object. Placing the patient's name, location, and condition in a facility directory comes under this category. The institution would need to provide patients with the opportunity to ask not to be listed.

The regulations recognize uses and disclosures that may be mandated by law that require no consent or authorization, including reporting requirements for public health agencies, reporting required by law, and managing organ donation.

The concept of minimum necessary disclosure is central to these regulations. That is, for any particular use or disclosure of information, the amount of information disclosed should be limited to the minimum amount necessary to accomplish the purpose at hand.¹⁶ According to the privacy regulations, minimum necessary disclosure does not apply to providers using information for treatment, to the individual, or to DHHS.

The regulations also establish certain rights for individuals:

- The right to access protected health care information about them.
- The right to an accounting of disclosures of protected health care information for purposes other than treatment, payment, and health care operations.
- The right to written notice regarding practices for protected information

within covered entities.

- The right to request amendment or correction of protected information that is incomplete or inaccurate.
- The right to request restriction of disclosures otherwise permitted under the regulations if the covered entity agrees to those restrictions. The covered entity may refuse the request as impractical or burdensome but must document the decision in writing.

What these rights may mean for pharmacy is uncertain, but they appear to indicate that patients may request a copy of their profile and that a pharmacy may need to record each time it provides a copy of the information in a profile for any reason other than treatment, payment, or health care operations. Pharmacies, especially those that are not part of larger covered entities, will need to develop a public statement on how individually identifiable health care information may be disclosed and provide such information to the public on demand.

The privacy regulations do not recognize grades of sensitivity of health care information. That is, a covered entity may adopt measures consistent with the regulations that are appropriate for the most sensitive information processed but must then apply those measures to all protected information.¹⁷

Research. Uses and disclosures of individually identifiable health records for research without individual consent is permitted under the privacy regulations, subject to several conditions.¹⁸ First, a privacy board (this may be an institutional review board) must have reviewed the protocol and determined that appropriate criteria have been met. Second, the privacy board must certify in writing that it is competent to review such information, has no conflict of interest, and includes at least one person not affiliated with the institution. This document must be signed and dated.

Third, the research project must meet the following criteria:

- The use of individually identifiable health care information involves minimal risk to the subjects,
- The waiver or alteration of patient rights will not adversely affect the rights and welfare of the subjects,
- When appropriate, the subjects will be provided with additional pertinent information after participation,
- The research could not practicably be carried out without the waiver or alteration,
- The research project is of sufficient importance to outweigh the intrusion into the privacy of the individual whose information would be disclosed,
- There is an adequate plan to protect the identifiers from improper use and disclosure, and
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research.

Ideally, research data would be deidentified. It remains to be seen whether such deidentification can be performed without compromising the value of the research data. It seems likely that researchers will need to include disclosures in the materials they present to a patient they are recruiting for a study.

Business associates. The privacy regulations recognize that covered entities may render services by contracting those services to others. Outsourcing i.v. admixture services is an example of a business associate relationship; sending specimens to a reference laboratory is another. In both cases, individually identifiable (and, therefore, protected) information must be shared for the associate to perform work for the covered entity.

Under the privacy regulations, protected health care information can be shared with a business associate only if there is a contract in place that binds the associate to proper

management of protected health care information. Specifically, such a contract must

- Require that the associate follow the covered entity's rules for protection of protected health care information,
- Specify the minimum information necessary for business to be conducted,
- Prohibit further disclosure to or by the associate,
- Require the associate to report inappropriate uses that may occur,
- Require the associate to make books and records available to the covered entity,
- Require the associate to return or destroy any protected information at the end of the relationship with the associate, and
- Permit the covered entity to terminate the contract if it determines that the associate has violated the terms.

The regulations do not require the covered entity to police its business associates. However, the regulations do require that a covered entity that could reasonably be expected to know about inappropriate uses of protected information by a business associate attempt correction. Correction may take the form of demanding a cure, terminating the business associate relationship, or (if neither cure nor termination is possible) reporting the problem to DHHS.

For example, if a pharmacy were to outsource the production of TPN solutions, it would be required to have a contract in place that stipulated what protected information was transmitted to the outsourcing contractor, what protections were in place for that information at the contractor, and so forth. The pharmacy would not be required to routinely audit the outsourcing contractor but, if it were to become aware that the contractor was mailing marketing materials to patients, would be required to demand that the practice cease or to terminate the relationship.

Administrative burdens. The privacy regulations impose some specific administrative burdens in addition to general compliance with the act and documentation of that compliance. Specifically, the regulations require a covered entity to

- *Designate a "privacy official."* A full-time or part-time person must be assigned responsibility for managing compliance with the act and its regulations.
- *Designate a contact person or office.* A person or site representing the covered entity with which the public can interact regarding privacy issues must be designated.
- *Provide and document training.* Covered entities will need training in security and privacy matters (in addition to policies and procedures) and will need to document completion of that training.
- *Provide safeguards for the release of protected information.* Covered entities are required to positively identify persons unknown to them before transferring protected information. This includes obtaining positive identification from DHHS persons requesting such information on behalf of the secretary of DHHS.
- *Provide a process for handling patients' complaints.* Covered entities must have (and document) a process by which a patient can register a complaint about the distribution of protected information. A person or office must receive such complaints, and a record of the complaints must be filed.
- *Define sanctions.* Covered entities are required to define sanctions against employees who distribute protected information inappropriately. These sanctions are in addition to the penalties defined within the regulations.

Sanctions. HIPAA specifies penalties for failure to comply with the act and for wrongful disclosure of information. Failure to comply can result in civil prosecution, with penalties of

\$100 per violation up to a ceiling of \$25,000 per year.^{19,20} Performance failures that are not deemed to be willful neglect may be exempted from these penalties.

Wrongful disclosure is a criminal act subject to a fine of \$50,000 per incident plus one year of imprisonment, or both, unless the offense is committed under false pretenses or with malicious intent. Wrongful disclosure under false pretenses carries a fine of \$100,000 per incident or imprisonment for up to 5 years, or both; wrongful disclosure with malicious intent carries a fine of up to \$250,000 or imprisonment for up to 10 years, or both.^{19,20}

Privacy and the pharmacy. The privacy regulations require that the pharmacy review its practices relating to the use and disclosure of protected health care information. Most urgently, pharmacists must ensure that their institutions recognize their interventions as treatment; otherwise, significant limitations may be placed on their right to view and use information in patient charts. In addition, pharmacies will have to identify protected information existing within the department and create procedures for the control, use, and disclosure of that information.

Pharmacies that outsource some or all of their distributive functions will probably have to negotiate new contracts that comply with HIPAA requirements and will need to exercise due diligence to be sure that protected information disclosed to contractors is properly controlled. Pharmacies in larger institutional settings will need to learn how the institutions are approaching HIPAA's privacy regulations and determine which departmental policies and procedures may need revision.

Conclusion

Security and privacy regulations enacted under HIPAA will require pharmacies to review their practices

■ SPECIAL FEATURE Security and privacy requirements

regarding the storage, use, and disclosure of protected health care information. The act will necessitate the assertion of the pharmacist's role as a treatment provider and the review and upgrade of pharmacy information systems, policies and procedures, and contracts.

References

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. no. 104-191.
2. Braithwaite B. Administrative simplification: HIPAA privacy and security standards. Paper presented at Risks and Rewards: Implementing the HIPAA Privacy and Security Standards. Washington, DC; 2000 Mar 7.

3. *Fed Regist.* 1999; 64:60005-7 (codified at 45 C.F.R. parts 160-4).
4. Sanches L. Getting to final: standards for privacy of individually identifiable health information. Paper presented at Risks and Rewards: Implementing the HIPAA Privacy and Security Standards. Washington, DC; 2000 Mar 7.
5. Standards for privacy of individually identifiable health information. *Fed Regist.* 1999; 64:59927 (codified at 45 C.F.R. parts 160-4).
6. *Ibid.* p 59935.
7. Standards for privacy of individually identifiable health information. *Fed Regist.* 2000; 65:82818 (codified at 45 C.F.R. part 160 and 164).
8. Standards for privacy of individually identifiable health information. *Fed Regist.* 2000; 65:82761 (codified at 45 C.F.R. part 164.514).
9. King M. HIPAA final privacy rule. Paper

presented at HIPAA Privacy Standards: The Final Rule. Washington, DC; 2001 Jan 16.

10. Security and electronic signature standards. *Fed Regist.* 1998; 63:43242 (codified at 45 C.F.R. part 142).
11. *Ibid.* p 43251.
12. *Ibid.* p 43253.
13. *Ibid.* p 43254.
14. *Ibid.* p 43255.
15. Standards for privacy of individually identifiable health information. *Fed Regist.* 1999; 64:59923 (codified at 45 C.F.R. parts 160-4).
16. *Ibid.* p 59924.
17. *Ibid.* p 59939.
18. *Ibid.* p 59967-71.
19. Health Insurance Portability and Accountability Act of 1996, Pub. L. no. 104-191, section 1176(a).
20. Standards for privacy of individually identifiable health information. *Fed Regist.* 1999; 64:60003 (codified at 45 C.F.R. parts 160-4).

Did you know that 6 million people worldwide are undergoing oral anticoagulation therapy? However, that number actually comes down to **one**...you.

Anticoagulation patients can find safety in numbers, starting with one.

The *Anticoagulation Management Module* helps you successfully manage a complete care program for your ambulatory patients on oral and more recent anticoagulant therapies. From your patients' individual diets to their lifestyles, you'll learn the intricacies of managing your patients' anticoagulation therapy, while mastering skills to:

- Develop collaborative patient relationships
- Design detailed therapeutic regimens and education plans
- Empower patients to provide appropriate self-care
- And, monitor the ambulatory care plan for your patients

Please visit the **ASHP Shopping Cart** at www.ashp.org, or call 301-657-4383. Order code P600

CE credit available!

The American Society of Health-System Pharmacists is approved by the American Council on Pharmaceutical Education as a provider of continuing pharmaceutical education. For more complete information, call 301-657-4383, ext. 1202.

American Society of Health-System Pharmacists®

©2001 American Society of Health-System Pharmacists®