What You Need to Know About HIPAA Now

Now that the final privacy rules have been published, your practice can't afford to ignore this legislation.

David C. Kibbe, MD, MBA

Dr. Kibbe is a family physician and CEO of Canopy Systems, Inc., an Internet clinical software application and services firm based in Chapel Hill, N.C. He is also a contributing editor to Family Practice Management.

CME
Covered in *FPM* Quiz

ILLUSTRATION BY KEN JOUDREY

Are you familiar with the Health Insurance Portability and Accountability Act (HIPAA)? If you aren't, you're not alone. Although HIPAA was signed into law in 1996, only the "portability" aspect of the law (which protects the ability of people with current or pre-existing medical conditions to get health insurance) has been fully implemented. Now the "accountability" aspects of the law are beginning to be addressed. Its many provisions include stringent codes for the uniform transfer of electronic data, including billing and other routine exchanges; and new patient rights regarding personal health information, including the right to access this information and to limit its disclosure. Also outlined are specific physical, procedural and technological security protections all health care organizations must take to ensure the confidentiality of patients' medical information. ➤

SPEEDBAR®

Physicians should begin to educate themselves about three aspects of the HIPAA regulations: privacy, security and transactions.

The final rules for transactions and privacy have been issued; the security rules are expected this spring.

Practices and health care organizations will have until the fall of 2002 to comply with the transactions regulations.

The compliance date for the privacy regulations is February 2003.

Taken together, the HIPAA standards will require major changes in how health care organizations handle all facets of information management, including reimbursement, coding, security, patient records and care management. Every practice in the United States will have to comply with these regulations, beginning with the transactions standards (i.e., the rules standardizing electronic data exchange of health-related information) in the fall of 2002. The privacy regulations will take effect in February 2003, and the security rules, while they've not yet been released, should be published shortly. I've studied the recently released regulations (all 1,000+ pages!) and suggest that you start doing what you can to educate yourself and prepare your practice for the changes ahead.

Transactions regulations

Currently, about 400 different formats exist for the online processing of health claims. The HIPAA transaction rules will require that everyone use the same format to transmit health-related information. Claims submission, claims status reporting, referral certification and authorization, and coordination of benefits will be affected. What does this mean for medical practices? Practices will have to ensure that their software vendors have implemented the required HIPAA changes so they can send and receive information using the standard formats. Because most software vendors already use the standard formats, this regulation shouldn't have much impact on daily practice, except perhaps to make electronic data interchange preferable to (i.e., less expensive than) paper processing for providers and health plans alike.

> **Every practice in the United States will have to comply with these regulations.**

Privacy and security regulations

Every practice in the country is going to feel the impact of HIPAA's privacy and security regulations. Instituted to provide greater protection of patient confidentiality, the regulations will require that you take a number of administrative measures to ensure that any patient-identifiable information, referred to by HIPAA as "protected health information" (PHI), in your practice is secure. (See "Key HIPAA terms" on page 45 for a complete definition of PHI.) Below are just a few of the ways you can expect the HIPAA privacy and security regulations to affect medical practices in the next 24 to 36 months.

Access control. Family physicians' offices are among the most active users of PHI in the health care community, routinely handling and transmitting many kinds of patient-identifiable information. HIPAA regulations will require that medical practices obtain explicit patient consent to use PHI for the purposes of health care delivery, payment and routine practice operations. Further, it requires patient authorization for any other use of PHI (e.g., research or marketing). Organizations will eventually have to determine which of the individuals and organizations they do business with can have access to PHI and build language into each contract to ensure that business associates will handle PHI in compliance with the law.

In my opinion, it will be almost impossible to control access to PHI using paper-based systems and processes. Why? Consider the haphazard treatment of paper documents in most offices. They are passed from one person to the next, photocopied, occasionally misplaced and often left out in public view. The intent of the HIPAA standard is to discourage this practice. I believe the unmistakable legacy of HIPAA will be to encourage computerization of all personal health information, regardless of who creates, stores or transmits it. How else can providers meet HIPAA's exhaustive requirements to document all releases of information, produce audit trails, and be able to inform patients about who has accessed their

KEY POINTS

Every practice regardless of its size will have to comply with the HIPAA security, privacy and transactions regulations.

Don't panic. There is a 24- to 36-month period between publication of the regulations and mandatory compliance with them.

Family physicians should start familiarizing themselves with HIPAA and consider performing a gap analysis to determine their organizational readiness.

medical information? The alternative to computerizing patients' medical information will be to maintain massive paper logs kept under lock and key.

Minimally necessary information. The HIPAA regulations not only require that health care organizations carefully

> **The unmistakable legacy of HIPAA will be to encourage computerization of all personal health information.**

define who has access to PHI, but also how much of the patient record front-office staff, utilization managers and others may view in the daily course of their work. Physicians will be able to continue to share a patient's entire medical record with colleagues for purposes of treatment; all other uses and disclosures must consist of only the minimal information necessary to achieve the purpose at hand. The intent of the HIPAA standard is to discourage the current practice of open access to medical records that may contain large stores of information regarding a patient's previous medical history.

Faxes. Faxing is the most common cause of confidential information ending up at the wrong place or in the wrong hands. Think about how often patient information in your office is left at the fax machine or sitting on a desktop for anyone to see. HIPAA security regulations will require faxes to be tracked carefully, especially those sent to parties outside the four walls of your organization. The regulations will require that you verify the identity of the party receiving the fax and provide ongoing monitoring of fax security practices.

Consent for sale of medical records. The HIPAA regulations also will prohibit medical records from being sold without patients'

KEY HIPAA TERMS

Understanding the HIPAA regulations will be a lot easier if you familiarize yourself with the following five terms:

Protected health information (PHI). HIPAA regulations apply to "protected health information," that is, medical information that contains any of a number of patient identifiers including name, Social Security number, telephone number, medical record number or ZIP code. The regulations protect all individually identifiable health information in *any* form (electronic, paper-based, oral) that is stored or transmitted by a covered entity.

Covered entities. Any health care providers, health plans or clearinghouses that electronically transmit medical information such as billing, claims, enrollment or eligibility verification must meet HIPAA regulations. Covered entities also include medical practices (including solo practices), employers, rehabilitation centers, nursing homes, public health authorities, life insurance agencies, billing agencies and some vendors, service organizations and universities.

Business associates. Covered entities cannot circumvent HIPAA regulations by using a "business associate," such as a billing service or other agency, to handle their electronic transactions. HIPAA requires covered entities to guarantee that their business associates and partners have security measures in place and technology sufficient to avoid accidental disclosure or mishandling of individually identifiable health information. This is known as a "chain of trust" relationship. Business associates must also abide by HIPAA regulations, for example, by ensuring that the individuals who are the subject of the information have access to it.

Privacy. HIPAA regulations protect an individual's right to the privacy of his or her medical information, that is, to keep it from falling into the hands of people who would use it for commercial advantage, personal gain or malicious harm. The HIPAA privacy regulations require providers to obtain a signed consent form in order to use and disclose PHI for activities related to treatment, payment and health care operations and to obtain a separate authorization to use or disclose PHI for any other purposes (e.g., marketing).

Security. Security refers to a covered entity's specific efforts to protect the integrity of the health information it holds and *prevent unauthorized breaches of privacy* such as might occur if data are lost or destroyed by accident, stolen by intent or sent to the wrong person in error. Security measures can be physical (e.g., locking rooms and storage facilities), administrative (e.g., policies and procedures covering access to information, user IDs and passwords, or punishments for violations of these) or technological (e.g., encryption of electronic data and use of digital signatures to authenticate users logging into a computer system).

SPEEDBAR®

The privacy regulations will require you to take a number of administrative measures to ensure that patient-identifiable information is protected.

The measures include documenting all releases of patient information, producing audit trails and informing patients about who has accessed their records.

The privacy regulations will also require you to define who can access a patient's record and how much of it they may view in the daily course of their work.

Physicians will still be able to share a patient's entire medical record with colleagues for purposes of treatment.

SPEEDBAR®

Although it may be the end of 2001 before HCFA recommends steps to take to comply with HIPAA, you can do three things now.

Begin familiarizing yourself with the basic components of the HIPAA regulations.

Consider assigning one person or a team of people in your practice to manage HIPAA compliance, and ask them to start learning all they can now.

Do an organizational risk assessment to determine where there may be gaps in your current confidentiality and security practices.

written consent. This could make the sale of some practices very difficult and affect physicians' retirement plans and negotiations with hospitals. It could also affect other parties involved in the transfer of patients' records from one provider to another.

Start preparing for HIPAA now

Remember that the enforcement date for complying with the HIPAA privacy regulations is February 2003. (The transactions regulations will begin to take effect in the fall of 2002 but will have less impact on the average physician practice.) You will have even more time to prepare for the security regulations, expected to be finalized this spring. So there is no need to panic, rush out and take a course, hire a consultant or attend a conference. In fact, it may be the end of 2001 or early 2002 before Health and Human Services makes recommendations for patient consent and authorization forms and before the checklists of recommended activities to do to comply with the security regulations are even available.

> **Fortunately, there are already a few excellent tools available for assessing organizational readiness.**

You should, however, take three important steps now:

- Begin familiarizing yourself with the basic components of the HIPAA regulations.
- Consider assigning a team to manage HIPAA compliance or, if your practice is small, appoint a privacy officer. Ask them to start learning all they can about HIPAA now.
- Do an organizational risk assessment. I'd suggest you begin by performing a "gap analysis" to determine where gaps may exist between your current confidentiality and security practices and what HIPAA privacy and security regulations are expected to require. Fortunately, there are already a few excellent tools available for assessing organizational readiness. HIPAA Early View (about $150; www.nchica.org), was developed by a non-profit group of leaders from the health care and information technology sectors and can be downloaded from the Internet. It guides users through a series of questions, generating a list and reports. Another good resource for HIPAA compliance is the American Health Information Management Association Web site (www.ahima.org/hot.topics). The site offers links to articles on HIPAA, a compliance checklist and answers to frequently asked questions. As the deadline for compliance gets closer, you can also expect to see more health care information services companies marketing their own HIPAA compliance solutions.

Not another Y2K

Preparing for Y2K made us all much more aware of our information systems and our dependence on them and the vendors who supply our hardware, software and network connectivity. HIPAA, however, will require more than an upgrade of current information systems, and the work can't be outsourced to software vendors and consultants. In the months ahead, providers will be forced to deal explicitly with privacy and confidentiality issues in many situations where disclosures have previously been implicit or a matter left up to the judgment of the physician and patient. Physicians will now have to consider more carefully than ever the decisions they make about sharing health information with their colleagues, co-workers or a patient's family, relatives or friends.

Each practice will have to carefully

HIPAA AT A GLANCE

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes three separate sets of rules that will affect your practice. They cover **transactions, security** and **privacy** of health care data. The transactions and privacy rules have been issued; the security rules are expected this spring.
- The regulations apply only to **information that identifies an individual** or "where there is a reasonable basis to believe that the information could be used to identify that individual."[1] The HIPAA regulations extend to all forms of individually identifiable information, even paper-based and oral communications. The regulations also list identifiers that, when removed from the data, create "de-identified" information not subject to HIPAA regulations.
- The HIPAA regulations do not preempt any state laws that are stronger or more protective of consumers' security and privacy than the federal standard.

1. Public Law 104-191. Health Insurance Portability and Accountability Act of 1996. *Federal Reg.* 1999; 64:60053.

consider how it handles and protects PHI; develop written policies and procedures tailored to the practice; train its employees; and evaluate its contracts with laboratories, medical suppliers, software vendors and others with an eye toward how the contracts may affect the privacy of patient information they transfer or share.

> **HIPAA carries severe civil and criminal penalties for noncompliance.**

And unlike Y2K, HIPAA carries severe civil and criminal penalties for noncompliance, including fines up to $25,000 for multiple violations of the same standard in a calendar year and fines up to $250,000 and/or 10 years in jail for knowing misuse of individually identifiable health information.

Final thoughts

HIPAA will force virtually every health care provider organization, from the largest health plan to the smallest practice, to put in place several layers of safeguards and protections that the majority do not now have. If your practice was affected financially by Y2K, it's a safe bet that HIPAA will cost you several times as much to implement over the next two or three years.

But ultimately, HIPAA will be a good thing for medicine. Patients will have greater trust that their personal health information is secure from accidental disclosure. Standardizing the forms and format for the electronic exchange of health-related data will bring down the cost of doing business for providers and other health organizations. And, finally, public health interests will benefit as computerization of PHI increases, making de-identified data more readily available for use in policy and public health decision making. FPM

Editor's note: After the final security regulations are released, Dr. Kibbe plans to write an article about specific HIPAA compliance steps. Look for it later this year.

SPEEDBAR®

HIPAA will force all of us to put in place several layers of safeguards and protections that the majority of us don't currently have.

Health care organizations that don't comply with HIPAA will face severe civil and criminal penalties.