THE HIPAA PRIVACY RULE:

Answers to Frequently Asked Questions

How will the privacy rule affect your practice? We took that question and others to a health care attorney to find out.

Alice G. Gosfield, JD

Many physicians are so overwhelmed by decreasing reimbursement, increasing administrative burdens and demanding patient loads that they have yet to come to grips with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule. The Department of Health and Human Services Office of Civil Rights will begin to enforce the privacy rule on April 14, 2003, and there are penalties for noncompliance. This article will give you a better idea of what is now required of your practice.

What is the HIPAA privacy regulation?

Until Congress passed HIPAA in 1996, personal health information was protected by a patchwork of federal and state laws. Patients' health information could be distributed without their consent for reasons having nothing to do with their medical treatment or health care reimbursement. The HIPAA regulation provides the first comprehensive federal protection for the privacy of individually identifiable health information. The regulation increases consumer control over the use and disclosure of their medical information. It also establishes appropriate safeguards that must be followed to protect the privacy of patients' health information. What's provided here is basic information on the regulation. The resource box on page 40 provides sources for additional information.

Will the privacy regulation be changed or delayed?

No. Changes to the final privacy regulation were published on Aug. 14, 2002, and no further changes are likely. You must be ready to comply with the regulation by April 14, 2003.

Who must comply with HIPAA?

Any person or organization that stores or transmits individually identifiable health information electronically is considered a "covered entity" and is required by law to comply with HIPAA. For example, if you submit claims electronically or make referrals or obtain authorizations by sending e-mail messages that contain individually identifiable health information, you are a covered entity.

If your practice is paper based, don't automatically assume you're exempt from the

Alice Gosfield is an attorney and principal of Alice G. Gosfield & Associates, PC, in Philadelphia, chairman of the Board of Directors of the National Committee for Quality Assurance, and a member of the Family Practice Management *Panel of Consultants. Conflicts of interest: none reported.*

CME
Covered in *FPM* Quiz

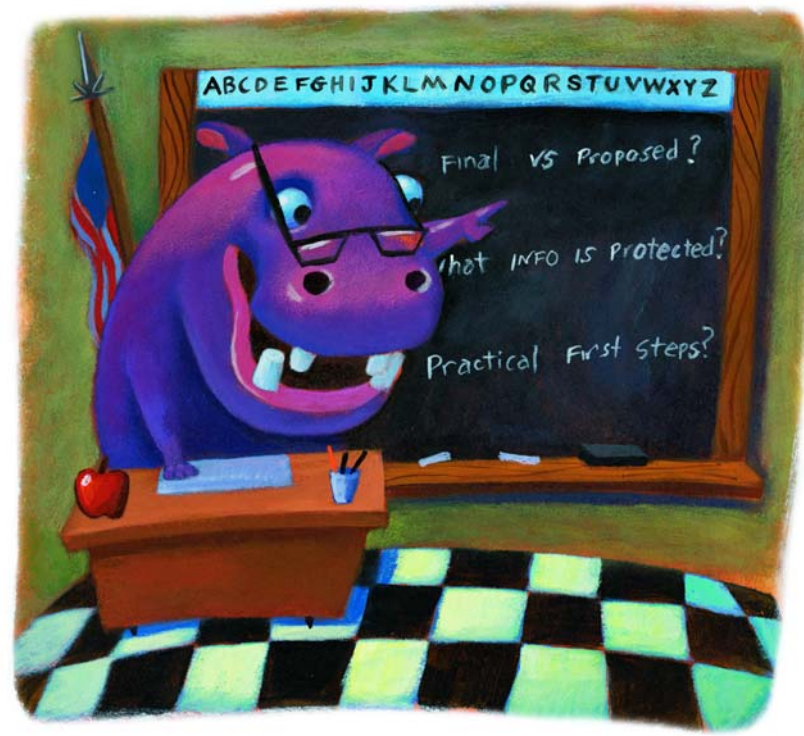

ILLUSTRATION BY WILL TERRY

SPEEDBAR®

The HIPAA privacy rule will be enforced beginning April 14, 2003.

It provides the first comprehensive federal protection for the privacy of individually identifiable health information.

Any health care entity that transmits individually identifiable health information electronically is considered a "covered entity" and must comply with HIPAA.

If you aren't considered a covered entity, the rule doesn't apply to you directly. However, you'll feel its impact if you deal with any organization that must comply.

regulation. For example, if you submit hard copies of claims to your billing company and it transmits them electronically to payers, the HIPAA rule applies to you. For help determining whether you are a covered entity under HIPAA, go to www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

If you aren't a covered entity, the law does not apply to you directly. However, you will feel its impact if you deal with any physician or organization that is a covered entity. For example, a covered entity may ask you to sign a business associate agreement to provide assurance that you will safeguard any individually identifiable health information to the same extent it does.

What if I don't comply with the regulation?

The government can impose civil penalties for noncompliance ranging from $100 to $250,000 and, in extreme cases, criminal penalties and imprisonment.

Can't I just follow state laws regarding physician-patient confidentiality?

No. The HIPAA privacy rule is much more formal than the patient confidentiality laws physicians have traditionally adhered to. State law should only be followed when it is more stringent than federal law. You will undoubtedly want to consult with your state medical society, if not a health care lawyer, to determine which rules are stronger.

How will the government even know if I'm complying?

Obviously the government doesn't have the money or the manpower to be certain that every covered entity complies with the HIPAA regulation. But the government does have the authority to launch its own compliance reviews, and while it's unlikely that it will initiate these reviews right away, patients can complain anytime. If, as a result, the government does investigate your practice, your good-faith effort to have privacy policies and procedures in place will be important.

What information is protected?

HIPAA defines protected health information (PHI) as individually identifiable health information held or disclosed by a covered entity. PHI is widely inclusive. It can include a patient's name, Social Security number or medical record number; specific dates such as birth, admission, discharge or death; or any other information that may be used to identify a patient. This may include information about past, present or future physical or mental conditions, the provision of health care to an individual, or the past, present or future payment for the provision of health care. Simply removing the patient's name is not enough to protect the information, and "de-identification" is an onerous task that most physician practices will not undertake.

KEY POINTS

- The HIPAA privacy rule formalizes many of the policies and procedures you may already use to safeguard patient information and maintain physician-patient confidentiality.
- The privacy rule doesn't require patient consent for routine uses or disclosures of medical information, such as for treatment or billing purposes.
- It will require you to give patients notice of your privacy policies, obtain authorization before using individually identifiable medical information for non-routine purposes and ask business associates to sign privacy agreements.

Do I only have to protect the PHI that my practice transmits electronically?

No. If you are a covered entity, all uses and disclosures of PHI are regulated. You must institute safeguards to protect PHI whether you disclose it verbally, in writing or electronically. The good news is that under the final rule, you do not need the patient's consent for most routine uses or disclosures of PHI related to treatment, payment and health care operations (TPO). Health care operations include but are not limited to fundraising activities; quality assessment and improvement activities; insurance activities; business planning, development and management activities; licensing and audits; evaluating health care professionals and plans; and training health care professionals.

What are the basic rules on disclosure of PHI?

The rules regarding the use of PHI pertain to disclosures as well. Essentially, your practice may use and disclose PHI for your own TPO activities. The regulation also requires that you put in place policies regarding use

and disclosure (e.g., who in your practice will be permitted to disclose PHI).

What kinds of safeguards are required?

You must establish appropriate administrative, technical and physical safeguards to protect the PHI in your practice from intentional or unintentional disclosure. For example, the regulation requires you to limit access to PHI but provides you with enough flexibility to determine for yourself who in your office needs access to PHI and how much information they need to do their jobs.

What are a patient's rights regarding PHI?

Patients have six fundamental rights:

1. The right to receive a notice about your privacy policies. This notice will be similar to the form credit card companies or banks currently send to customers, indicating specifically how they use their personal information. The notice must include information about patients' rights under HIPAA, including the right to access the information you maintain about them and the right to complain if they feel their rights have been violated. Although you do not have to obtain a patient's consent to use his or her PHI for treatment, you must at least make a good faith effort to acquire the patient's acknowledgement that he or she received notice of your privacy policies. A copy of the acknowledgment should be kept in the patient's file.

2. The right to access the medical information you maintain about him or her. On request, you may provide a summary of the patient records or the records themselves, but you must do so within a specified time period. If you provide a copy of records, you may charge the patient a reasonable price for reproducing them.

The government can impose civil penalties for noncompliance ranging from $100 to $250,000.

There are some exceptions under which you may deny patients access to their records. However, if you do this, your decision must be reviewed by another licensed professional whom you have designated in your privacy policies and procedures.

3. The right to limit the uses and disclosure of medical information. This includes limitations that can cause significant practical problems. For example, a patient may not want her diagnosis of cancer disclosed to a payer out of fear the information could reach her employer. If she is estranged from her family, she may not want any information (e.g., her phone number) disclosed to her siblings.

A patient could also refuse to allow you to report data to his health plan for quality assurance purposes (which is otherwise protected under the definition of "operations" for which you do not need consent). Although this is a patient's right under HIPAA, reporting such data is also a requirement of most managed care contracts and something you will have to take into account during future negotiations.

You are not obligated to agree to patients' restrictions, nor must you care for patients whose restrictions would interfere with their treatment. The real problem arises when a patient with whom you have an established relationship restricts use or disclosure. If you agree to the restrictions, you must document them and abide by them. If you don't agree to them, the patient will either have to relinquish the request or look elsewhere for care. If the patient chooses the latter, you will have to adhere to your basic common law responsibilities of non-abandonment.

4. The right to request amendments to the medical record. The privacy notice you give to patients must specify how they should make requests to amend their records (e.g., in writing). You may refuse such a request for several reasons, including that the patient's record is accurate and complete. However, the patient does have the right to appeal. If you agree to amend the patient's record, you must notify the individual and others to whom you have provided the information that it has been amended.

5. The right to revoke or limit authorization. If your practice uses or discloses PHI for any reason other than TPO, you must obtain a specific "authorization" from the patient. This is a form that states what information will be disclosed and how it will be done. Special rules apply for clinical trials or research data. Psychotherapy notes may only be disclosed subject to authorization. ➤

SPEEDBAR®

The government can impose civil penalties for noncompliance ranging from $100 to $250,000.

If your practice is investigated for noncompliance, a good-faith effort to have privacy policies and procedures in place will be important.

You will not need patient consent for most routine uses or disclosures of protected health information related to treatment, payment or health care operations.

You will need specific written authorization from patients to disclose their medical information for nonroutine purposes, such as marketing.

SPEEDBAR®

Patient rights include the right to access their medical information and the right to limit its use and disclosure.

The privacy rule requires adopting safeguards to protect the medical information you maintain, but allow you to determine what is reasonable.

Safeguards include developing privacy policies and procedures for your practice, educating staff and providing information to patients about their privacy rights.

You must also shore up systems in your office to limit access to patient health information to only those people who need it to do their jobs.

Parental access to minors' medical records will continue to be controlled by state law.

6. The right to an accounting of disclosures of PHI. According to the privacy rule, patients can ask to see what disclosures have been made during the past six years only.

What should I do to protect the PHI in my office?

Although the privacy regulation gives you some flexibility for determining what is reasonable for protecting PHI in your office, you will be required to do the following:

- Adopt clear privacy policies and procedures for your practice.
- Designate someone to be responsible for seeing that the privacy policies and procedures are followed.
- Train employees so that they understand the privacy policies and procedures.
- Secure patient records containing PHI so that they are not accessible to those who don't need them.
- Provide information to patients about their privacy rights and how their information can be used.

How you satisfy each of these requirements will vary according to the size of your practice. For example, every covered entity must have a privacy officer. In a large organization, this may be someone's sole job responsibility, but in a solo or small private practice, it may be a physician or office manager serving in a dual role. Staff training regarding privacy policies and procedures may also vary depending on the size of your organization. A small practice may satisfy this requirement by providing staff members with a privacy policies and procedures handbook and documenting that they have received and reviewed it. Larger organizations with bigger budgets may actually conduct HIPAA compliance classes.

You will need to develop a privacy notice informing patients of your policies and procedures.

What are some practical first steps?

Develop privacy policies and procedures. As I've already mentioned, you'll need to identify someone to serve as your privacy officer. The privacy officer will need to learn about HIPAA, develop privacy policies and procedures for the practice, educate staff, and make sure the privacy policies and procedures are being followed. HIPAA also requires that you have a process in place for staff to register complaints about your practice's policies and procedures as well as sanctions for staff who violate the privacy rule.

Identify business associates. You should also think about all the ways you use and disclose PHI to determine who meets the definition of a business associate. These people and organizations will need to sign business associate agreements.

Develop a privacy notice. Once you have thought about how you use PHI, you will need to develop a privacy notice informing patients of your policies and procedures. You may want to obtain some examples from other practices to guide you, but don't simply copy someone else's notice without carefully analyzing how it applies to you. If you think you need to, have a lawyer or consultant help you refine a notice so that it reflects the specifics of your practice. In the last analysis, though, only your practice will know all the ways in which it uses PHI.

Decide how you will give notice. Will the receptionist provide the notice to the patient when he or she checks in for an office visit? Will the acknowledgement that the patient received notice be signed then? And will the receptionist be equipped to answer questions the patient may have? These are just some of the things to consider.

Determine authorization needs. Does your practice use PHI for any purpose (e.g., marketing) that will require patients to sign a special authorization form? The privacy regulation gives patients the right to revoke or limit the authorization. You will need to determine how your practice will document these refusals or modifications.

Decide how you will handle requests for PHI. You will need to develop basic policies regarding the disclosure of PHI. For example, who will review denied requests for access? It's likely that as you begin to think about these issues your staff will have many questions that can help you determine how to proceed. For example, what information can be provided to a caller who asserts he or she is a family member or to a caller who

says he or she represents a provider or health plan? What information can be faxed and to whom? What types of messages can be left on patients' answering machines? How should billing information containing PHI be handled? Should clinical information be handled the same way? Who will be allowed to access the medical record?

Develop a system for managing restrictions on PHI. Think about how you will handle PHI when patients restrict its use and disclosure. How will you proceed if you don't agree to the patient's request for restrictions? For example, suppose a patient says, "Don't tell my husband anything about me." If you agree to the patient's request, you will have to make sure you abide by it. How will your staff know the restriction exists? Where will you document it? One solution may be to color-code charts that have restrictions associated with them so everyone is aware they should receive special handling.

Develop a procedure for logging disclosures. Under the privacy rule, you must be able to provide an accounting of disclosures (other than for TPO) to patients who request it. You will also have to decide how you will allow patients access to their information and establish a procedure for patients to request amendments to their records. If you refuse to provide a patient access to his or her PHI for the very limited and specific reasons identified in the regulation or refuse to make the amendment to the record, how will you handle the appeal process? When you agree to amend a patient's record, you'll also have to notify anyone else who has the information. This is a real dilemma.

What new forms are required?

No specific forms are mandated, but to comply with the privacy regulation, you will need a notice of privacy as well as an acknowledgement form, an authorization form and a business associate agreement. Consent forms are permitted, but are not required. The AMA provides sample authorization, consent and notice of privacy forms on its Web site at www.ama-assn.org/ama/pub/category/6698.html. A sample business

KEY HIPAA PRIVACY TERMS

The HIPAA privacy regulation contains at least 69 specifically defined terms. This abbreviated glossary is intended to explain the terms used in this article. For a more complete glossary, go to www.cms.hhs.gov/glossary.

Acknowledgment. The patient's written statement that he or she has received the notice of your privacy policies and procedures.

Authorization. The patient's written permission to disclose information for uses outside of treatment, payment and operations.

Business associate. A person or entity with access to health information that conducts activities on behalf of a covered entity, but is not part of the covered entity's work force.

Covered entity. A health care provider, health plan or health care clearinghouse that transmits any health information in electronic form in connection with a HIPAA transaction.

Disclosure. The release, transfer, provision of access to or divulging in any other manner of information outside the entity holding the information.

Health care operations. These include but are not limited to the following: fundraising activities; quality assessment and improvement activities; insurance activities; business planning, development and management activities; licensing and audits; evaluating health care professionals and plans; and training health care professionals.

Health information. Any information, regardless of its form, relating to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

Individually identifiable health information. A subset of health information, including demographic information, that identifies an individual or provides enough information that there is a reasonable basis to believe it could be used to identify the individual. Also referred to as "Protected Health Information" (PHI).

Use. The employment, application, utilization, examination analysis or sharing of individually identifiable health information with an entity that maintains such information.

Work force. Employees, volunteers, trainees and other persons whose conduct while performing work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity.

SPEEDBAR®

You will need to identify a privacy officer for your practice and develop a privacy notice informing patients of your privacy policies and procedures.

The privacy notice must reflect the specifics of your practice. You cannot simply use a generic form.

To comply with the privacy regulations you'll also need an authorization form, an acknowledgement form and a business associate agreement.

Some sample forms are available at www.ama-assn.org/ama/pub/category/6698.html.

SPEEDBAR®

One of the biggest challenges of the privacy rule will be identifying your business associates.

HIPAA defines a business associate as a person or entity that has access to your patients' medical information in order to do work on your behalf.

To comply with the privacy rule, you must have a written agreement with each business associate stating that it will safeguard patient information to the same extent you do.

However, you won't need a written agreement for providers to whom you refer for treatment, such as hospitals, labs or other physicians.

associate agreement is available at www.hhs.gov/ocr/hipaa/contractprov.html.

Can I continue to use a patient sign-in sheet?

Yes. The privacy rule won't require you to refer to patients by code names, retrofit your office or soundproof your examination or consultation rooms. It simply formalizes much of what you probably already do to protect patient privacy and maintain physician-patient confidentiality. Most improper disclosures of PHI occur because of human error. HIPAA will force you to shore up your systems. For example, you will have to be more careful about faxing lab results to patients, posting patient names outside exam rooms or leaving messages containing PHI on answering machines.

HIPAA is a new risk-management area that no one can afford to ignore.

What about the businesses that aren't covered entities?

The government has created the concept of "business associates" to address this. A business associate is a person or entity that has access to your patients' PHI in order to do work on your behalf that you might otherwise hire your own work force to do. Examples include billing companies, transcription services, practice management companies, financial managers, outside auditors who review your records for documentation compliance, mailing services that send bills to your patients, your software vendor, your medical records off-site storage company, even a lawyer who may review PHI in connection with a Medicare audit.

Unfortunately, the privacy rule does not include an exhaustive list of all possible business associates. One of your basic challenges will be to identify your business associates. Why does it matter? Because to comply with the privacy regulation, you must have a written contract with each business associate that basically says it will safeguard PHI to the same extent that you do as a covered entity. While a signed contract does not make you a guarantor of a business associate's performance, one that is not HIPAA compliant can create real liability for you. It will benefit you to deal with companies and vendors who understand HIPAA and have their own privacy policies and procedures in place.

HIPAA doesn't require you to have a business associate agreement with some providers to whom you refer for treatment, such as other physicians, a hospital, lab or pharmacy. However, if these providers also perform work-related functions for you (e.g., a hospital leases you a nurse or a typist on a part-time basis), they are considered your business associate as well as a provider to your patients. It is important to determine all the ways you use PHI, who has access to it within your practice, and to whom you disclose it outside your practice.

According to the privacy rule, you will have until April 14, 2003, to get agreements signed with new business associates and until April 14, 2004, for existing business associates.

What's ahead?

No one really knows how many patients will want to restrict disclosure of their PHI, make amendments to their medical records or seek access to their files. We'll have to wait and see. And until the privacy rule is breached, no one really knows how strongly it will be enforced. What we do know is that, unlike a lawsuit, HIPAA won't require patients to show damages. A penalty will pertain simply for a violation. HIPAA is a new risk-management arena that no one can afford to ignore. So welcome to the brave new world of privacy, and if you haven't done so already, it's time to start your engines at turbo speed. FPM

Send comments to fpmedit@aafp.org.

HIPAA RESOURCES

American Academy of Family Physicians (www.aafp.org/hipaa) offers tips and tools for HIPAA implementation as well as FAQs.

American Medical Association (www.ama-assn.org/ama/pub/category/4234.html) offers the following draft forms at no charge: consent, authorization and notice of privacy policies.

Department of Health and Human Services (www.hhs.gov/ocr/hipaa/whatsnew.html) offers the complete text of the final amended privacy regulation as well as FAQs.