COMMENTARY

DANIEL E. NICKELSON
Director, Department of Government Affairs, The Cleveland Clinic

JOHN E. STEINER, JR, ESQ
Chief Compliance Officer and Privacy Official, The Cleveland Clinic Health System

NEIL MEHTA, MD
Director, Center for Online Medical Education and Training; Department of General Internal Medicine, The Cleveland Clinic

Privacy protection for your patients: Understanding the federal requirements

The compliance deadline is April 14, 2003

THIS YEAR, there is another important federal government deadline besides income tax. On April 14, 2003, almost every medical provider in the country—from small physician practices to large tertiary medical centers—must begin implementing new federal rules governing the privacy of patients and access to their medical records.

If you share any information electronically, such as with an insurance company or Medicare, every patient who visits your office will have to be provided a written statement about his or her privacy rights. Every patient has the right to request copies of his or her medical records, and you must provide those copies, at a reasonable cost, within a specified amount of time.

And if a patient with heart failure is organizing a research fund-raising event, you will need more than the patient's verbal approval before talking to a reporter about his case.

In this article we give you an overview of the law's requirements, especially as it relates to office-based physicians. We have tried to limit the use of legal terminology, but have included those terms that you will see in articles and training material on these new rules.

It is impossible in this short article to describe all the nuances of the federal rules. We have included in TABLE 1 some helpful sources on the World Wide Web.

A BRIEF HISTORY OF THE LAW

In August 1996, Congress passed and the President signed into law the Health Insurance Portability and Accountability Act (HIPAA). The primary purpose of the HIPAA was to make it easier for people to have health insurance when leaving or changing jobs. Title I of the act deals with this area.

Title II of the act simplifies some administrative matters with the aim of reducing fraud and abuse and gives the health care consumer specific rights, notably privacy protection for his or her medical information. The Congressional debate on this latter section was lengthy and intense.

Once HIPAA went into law, the Department of Health and Human Services (HHS) issued more detailed regulations, called the Privacy Rule, which specify how the law is to be carried out. All affected parties have to be in compliance with this regulation no later than April 14, 2003. On August 14, 2002, HHS issued its final rule. While clarifying the rule related to marketing and research issues, its most significant provision was to make the mandatory initial consent requirement optional.

HIGHLIGHTS OF THE HIPAA PRIVACY RULE

Who does it apply to?

The regulation applies to all health care providers (except those that have no electronic transactions), health plans, and health care clearinghouses. A provider who keeps only paper records and does not engage in any electronic transactions is exempt from all of these requirements.

What is protected?

The information subject to protection consists of all medical records and any other individually identifiable health information

The information within this article is for educational purposes. If legal or other expert advice is required, the services of a competent professional should be sought.

TABLE 1

Web sites with information on HIPAA

www.hhs.gov/ocr/hipaa
The site of the Office of Civil Rights, Department of Health and Human Services, which is administering the Privacy Rule.

www.massmed.org/search/results.asp?userneed=AtTheForefront-HIPAA
The HIPAA site of the Massachusetts Medical Society. For an easier link, go to **www.massmed.org**. In the search box, enter HIPAA. When the search results are displayed, click on "Help with HIPAA."

www.ama-assn.org/go/hipaa
The site of the American Medical Association, with free links and information about its formal training programs, for which there is a charge.

www.acponline.org/pmc/hipaa.htm
The site of the American College of Physicians-American Society of Internal Medicine. Access to most of the site requires users to be registered members of the ACP-ASIM.

www.emron.com/pathways
A free, sponsored site containing online information and sample forms. Online HIPAA training modules, with 3.5 hours of free CME credit, are available.

www.hcca-info.org/html/hipaa_library.html
A password-protected site on HIPAA available only to members of the Health Care Compliance Association.

www.ifebp.org/knowledge/hipaatoc.asp
Free HIPAA information compiled by the International Foundation of Employee Benefit Plans.

http://www.state.oh.us/hipaa/234hpm.htm
Site by the Ohio State Medical Association and the Ohio State Bar Association. It compares Ohio privacy requirements with the federal Privacy Rule.

used or disclosed by any of the organizations above in any form—electronic, paper, or oral.

Individually identifiable health information is defined very broadly to include information about:

- The past, present, or future physical or mental health (or condition) of an individual
- The provision of health care to an individual
- Past, present, or future payment for provision of health care to an individual.

Not only information that could *directly* identify the patient must be kept confidential, but also information *that could be used* to identify the patient. For instance, even if you do not disclose the name of the patient, disclosing the age, sex, race, and occupation of a patient might in some circumstances enable someone to identify the patient.

Each provider must have a written privacy policy

Every provider and health plan will be required to give every patient a clear, easy-to-understand, written explanation of the entity's privacy policy (called the Notice of Privacy Practices or NPP). In addition, providers and health plans must document that the patient (or the patient's representative) received a Notice of Privacy Practices. Among many requirements, the entity must:

- Assure the patient's right to see and copy his or her medical record, request and offer amendments, and see what types of nonroutine disclosures have happened with the record
- Obtain the patient's authorization for any nonroutine disclosure, ie, other than for payment, treatment, or health care operations (such as quality assessment and improvement; evaluation of physicians, nurses, trainees, and other workers; auditing; and business management purposes)—and the patient has the right to request that restrictions be placed on these possible disclosures
- Set up an internal process for handling patient complaints and documenting how they are resolved

Before sharing any information for treatment, payment, or health care operations, the health care provider *has the option* of requesting patient consent. A provider may disclose health information for other purposes without prior consent, under certain limited circumstances. These circumstances include emergencies, identification in case of death, public health purposes, research approved by an institutional review board, limited law enforcement activities, and activities related to national defense and security.

Penalties for violations

There are penalties if one violates the Privacy Rule. The law provides for civil penalties of $100 per violation, up to $25,000 per person per year for each violation. Additionally, there are criminal penalties for knowingly violating patient privacy. Criminal penalties are up to $50,000 and a year in prison for obtaining or disclosing protected health information; up to $100,000 and 5 years in prison for obtaining protected health information under false pretenses; and up to $250,000 and 10 years in prison for disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

The term "protected health information" is derived from the term "individually identifiable health information" and includes information that:

- Identifies or reasonably could identify the individual
- Is collected from the individual by the provider or someone else
- Is received by the provider, health plan, or employer
- Relates to the individual's health, health care, or health payments.

HIPAA does not supersede state requirements

An added complexity—this federal rule does not supersede state requirements. If the state has laws that are more strict in protecting medical records privacy, the state law prevails.

IMPLICATIONS FOR OFFICE-BASED PRACTICES: SIZE MATTERS

In developing the regulations, HHS recognized that there are many types of medical practices, ranging from highly complex health care systems to the individual physician office. Consequently, it developed a concept called "scalability," which means that large providers have to meet the full range of requirements while smaller-scale providers should reasonably attempt to comply with the Privacy Rule, given their resources and capabilities. In the introduction to the privacy regulations, HHS stated more than 200 times that providers should be "reasonable" in their interpretation and application of the regulations.

For example, the rules require that there be a privacy official responsible for the development and implementation of privacy policies and procedures. However, whether this privacy official must be full-time or part-time can vary. A small-scale physician practice might designate the office manager as the part-time privacy official, whereas a large, more complex entity would be expected to have a full-time privacy official.

The regulation emphasizes that small-scale providers should consider this scalability concept as they develop their plans to meet the requirements. In short, it is the *principle* of the requirement that must be met, not the *how* of its accomplishment. The most important thing a provider can do is to be able to show good faith efforts to comply with these regulations.

Document what you do!

As with all other interactions with government agencies, documentation that the regulatory requirements are being met is essential. The documentation requirements of the Privacy Rule will require additional resources not only to satisfy a government auditor, but to guarantee that a patient can discover what has happened with his or her health care information. Records and forms required under HIPAA, such as authorizations, must be maintained for at least 6 years after the date of their creation or the date they last are in effect, whichever is later.

Most importantly, be able to show good faith efforts to comply

EVERY PATIENT MUST RECEIVE A WRITTEN PRIVACY NOTICE

Every provider must provide a Notice of Privacy Practices written in plain language that contains:

- The following title: THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY

- A description, with at least one example, of the types of uses and disclosures permitted without prior authorization from the patient, and a statement that other uses and disclosures will be made only with the patient's written authorization, and that the patient has the right to revoke that authorization
- A statement of the patient's rights with respect to the protected health information and a brief description of how the individual may exercise those rights
- A statement that the provider is required by law to maintain the privacy of protected health information and to provide patients with notice of its legal duties and privacy practices
- A statement that patients may complain to the provider and to the Secretary of the Department of Health and Human Services if they believe that their privacy rights have been violated
- A brief description of how to file a complaint with the provider, and a statement that the patient will not face retaliation for having filed a complaint
- The name or title and telephone number of a person or office to contact for any further information
- The date on which the notice went into effect, which cannot be earlier than the date that the notice was printed or published.

Whenever there are material changes in the privacy policy, the notice must be revised promptly.

A Notice of Privacy Practices must be clearly posted in the office

When must the Notice of Privacy Practices be available?

Beginning on April 14, 2003, the Notice of Privacy Practices must be made available to patients no later than the date of first service delivery, including service delivered electronically, and as soon as reasonable or practicable in emergency treatment situations. A point to emphasize: providers *must* make a good faith effort to obtain from the patient written acknowledgment of receipt of the provider's Notice of Privacy Practices.

The Notice of Privacy Practices should be available at the service delivery site for patients to take with them and should be posted in a clear and prominent location where it is reasonable to expect that patients seeking service from the provider can read the notice, along with any revisions.

PERMISSION TO DISCLOSE INFORMATION

Patient consent for treatment, payment, and health care operations

A key element of the Privacy Rule is the option to obtain consent for use or disclosure of protected health information for the purposes of treatment, payment, and health care operations. The rule grants a provider the right to refuse treatment, except in emergency situations, if the patient refuses to consent to this.

Patient authorization for nonroutine disclosures of information

Providers *must* obtain authorization for nonroutine disclosures of information, that is, information not related to treatment, payment, or health care operations. In most instances, this will involve obtaining a signed patient authorization for use of their information for research, fundraising, marketing, or public relations activities. The authorization must be written in plain language, and a copy must be provided to the patient.

These authorizations require a description of:

- The information to be disclosed
- Who will be receiving it
- The purpose of the disclosure
- The expiration date of the disclosure authorization
- The signature of the patient and date it was signed.

Additionally, the authorization must contain statements adequate to place the individual on notice of all of the following:

- The patient's right to revoke the authorization in writing
- The provider cannot condition the patient's treatment, payment, enrollment, or eligibility for benefits on whether the patient signs the authorization form
- The potential for the information that the

authorization covers to be disclosed beyond the immediate recipient of the information since it is no longer covered by the Privacy Rule. For instance, if an authorization allows release of information to a newspaper reporter, that information may become known to the general community.

How all this will work in practice

Thus, at a minimum, providers must provide a Notice of Privacy Practices to the patient and get an acknowledgment from the patient that it was provided. Even if a patient refuses to acknowledge receipt of a Notice of Privacy Practices, the provider should document the attempt to obtain the acknowledgment. Providers also may obtain consent for disclosure of protected health information for purposes of treatment, payment, and health care operations. If consent is refused, care can be denied. Providers are required to put in place procedures and train employees so that patients' health information is protected.

A written authorization, signed by the patient or the patient's representative, is needed for information not related to treatment, payment, or health care operations, with certain exceptions such as public health or law enforcement (discussed above).

Disclose the least amount of information necessary

When protected health information is disclosed, care should be taken to disclose only the minimum necessary and to verify the authority and identity of the person to whom it is disclosed. HIPAA does allow incidental disclosure of protected health information which is required for normal operations and communications, eg, calling out a patient's name in the waiting room.

Patients can restrict access

The patient has the right to request restrictions on who can access their protected health information (eg, relatives), ask for alternative confidential methods of communication (eg, sending correspondence to a post office box instead of a home address), and ask for an accounting of anyone to whom their protected health information has been disclosed.

TABLE 2

Check your office for privacy violations

Potential violations
No posting of the Notice of Privacy Practices
Protected health information viewable in public areas
Staff discussing patient information in public areas (lobbies, elevators, etc)
Patient charts and reports left in public areas
Computers not logged off
Passwords posted on computers
Smart cards left in readers

PATIENT ACCESS TO THE MEDICAL RECORD

With some narrow exceptions, the patient has the right to inspect or to obtain a copy of the protected health information, ie, their medical records, maintained by the provider. The provider must respond to the request within 30 days. If the information is not maintained or accessible on-site, the provider may take up to 60 days to respond. The provider may require a written request, so long as that requirement is explained in the Notice of Privacy Practices that is initially given to the patient.

Additionally, the provider must make the information available in the form or format requested by the patient, if it is readily producible in that format, or in some form agreed to by the provider and the patient. The provider may provide a summary if the patient agrees.

Copying fees must be based on cost

What you can charge to copy or summarize medical records

A fee may be charged, but it must be based on costs and may include only the cost of copying, including supplies and labor, and postage. If the patient has agreed to receive a summary, the provider may also charge a fee for preparing the summary. The fee may

not include costs associated with searching for and retrieving the requested information.

Patient's right to request medical record amendments

The patient has the right to request that the provider amend his or her record. The provider may require patients to make this request in writing and provide a rationale, provided that it informs patients in advance of the requirement in the Notice of Privacy Practices initially given to the patient. The provider is required to act on the patient's request for an amendment no later than 60 days after receipt of the request. Under certain rules, a 30-day extension is possible. There are requirements dealing with both approvals and denials of a desired amendment by the individual.

Telling a patient who got their information

The patient has a right to receive an accounting of certain disclosures of protected health information made by a provider in the 6 years prior to the date on which the accounting is requested. The accounting does not have to include disclosures made for purposes of treatment, payment, or health care operations or most disclosures authorized by the patient.

As we noted earlier, the key to complying with these new rules is to show a good faith effort. That means having the forms and procedures, scaled to the size of your organization, in place by April 14, 2003. Periodically you need to examine your office and workplace to make sure there are no privacy violations, such as leaving patient charts in public areas or failure to prominently post your Notice of Privacy Practices (**TABLE 2**).

If a question is ever raised, your good faith efforts to comply will be your best defense.

ADDRESS: *Daniel E. Nickelson, Department of Government Affairs, W14, The Cleveland Clinic Foundation, 9500 Euclid Avenue, Cleveland, OH 44195.*