



policy points

Protecting Patients' Privacy Health-care providers will need to comply with the Bush administration's privacy regulations by April 2003. Now is a good time to find out what you will—and will not—need to do.

BY JEFF ATKINSON



Will physicians and hospitals need to construct new soundproof rooms in hospitals and doctors' offices? Will sign-in sheets for patients be prohibited? Will family members no longer be able to pick up prescriptions for patients unless the patient has a signed consent form that is on file with the pharmacy? And will charts need to be kept in a secure area away from the patient's bedside?

These were among concerns voiced when the Bush administration approved new

health-care privacy regulations on April 13, 2001. If the regulations were being literally and strictly enforced, scenarios such as these could become true. [The U.S. Department of Health and Human Services](#), however, issued guidance materials in July to clarify the regulations and provide assurances that the regulations will be con-

strued reasonably and that providers will not be subject to inconveniences such as those described above.

Long path to adoption

The path to the federal privacy regulations has been a long one. Congress ordered creation of the regulations in 1996 with passage of the [Health Insurance Portability](#)

[and Accountability Act](#) (HIPAA). Under that law, Congress had three years to adopt privacy rules. If Congress did not meet that deadline—which it did not—the Department of Health and Human Services was directed to draft the rules—which it did. The proposed regulations were published in November 1999, and that was followed by an extended period for public comment.

When President George Bush assumed office, there was speculation that he would order modification of the regulations that had been drafted during the Clinton Administration. The Bush administration, however, decided to let the regulations take

Examples of reasonable measures to promote privacy include adopting rules about speaking quietly when discussing a patient's condition with family members or at nursing stations and avoiding using a patient's name in hallways and elevators.

POLICY POINTS

Continued from previous page

effect on April 13, 2001 and handle any problems that arose with the regulations by amending the regulations and publishing guidance materials. Since compliance with the rules is not required until April 2003 (or April 2004 for small health plans with annual receipts of \$5 million or less), fine-tuning of the rules can be done before the compliance date. Copies of the regulations and guidance materials are available on line at

www.hhs.gov/ocr/hipaa/. See sidebar “Where to send your suggestions,”

Reducing the “patchwork”

The privacy regulations were designed to provide added protection to patients, particularly regarding the use of electronic records, and to provide more uniformity in the law. The system in place before the new regulations was described by federal officials as “a patchwork of federal and state laws.” After the compliance date for the new regulations, physicians and other health-care providers will continue to be subject to both federal and state regulations, but the federal regulations will be more comprehensive than they were before, and states may feel less need to regulate the area.

The federal regulations will serve as a “floor” for patient protections. States can, if they wish, impose more stringent privacy requirements, but they may not allow more relaxed standards. In explaining the need for the rule, the federal guidance materials said: “Health-care providers have a strong tradition of safeguarding private health information. But in today’s world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the rules provide clear standards for all

parties regarding protection of personal health information.”

Someone in charge of privacy

One of the basic requirements of the new regulations is for health-care providers to designate someone to be in charge of privacy issues by seeing to it that privacy procedures are adopted and followed. The federal regulators say the nature and duties of this position will vary considerably according to the nature of the health-care provider. The guidance materials say: “The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.”

Similarly, the level of privacy training expected for a provider’s employees will vary with the size of the provider. In a small practice, it is likely to be sufficient for there to be a written privacy policy given to each new member of the work force coupled with a record documenting that new workers have reviewed the policy. At a larger institution, training might be more elaborate, perhaps involving live instruction, video presentations, or interactive soft-

Steps To Comply With the New Privacy Regulations

1. Designate a person to oversee the adoption of and compliance with privacy policies.
2. Consider modifications to facilities, equipment, and policies to promote privacy. (e.g., use of cubicles or privacy screens, passwords on computers, adoption of explicit policies to avoid discussing patients by name in public areas.)
3. Provide training, and document that training, for personnel. (The amount of training can vary with the size and type of health-care provider.)
4. Review contracts with business associates, such as billing services and consultants, to help ensure that the business associates will follow privacy policies.
5. Review consent forms for patients regarding treatment, payment, and health-care operations. (If a patient is being asked to agree to release information for something other than those three purposes, a separate “authorization” form usually will be necessary.) ■

ware programs. The federal regulations do not specify the precise level of training required. Rather the general rule for the regulations, is for the provider to have procedures that are reasonable under the circumstances.

Responsible business associates

“Business associates” is a key term under the regulations. Business associates are outside companies that a provider, such as a physician’s office, uses to perform certain functions including billing, accounting, marketing, or general consulting and which will have access to patient information. Although the [Department of Health and Human Services](#) does not directly regulate these outside companies, it does expect the provider to take steps to see that the outside companies protect patient privacy.

A common way for a provider to promote such protection is through a contract that requires the company to com-

POLICY POINTS

Continued from previous page

What You Do Not Need to Worry About

When the privacy regulations were issued, there was concern that many common and useful practices would be prohibited. In [guidance materials](#) issued in July 2001, the U.S. Department of Health and Human Services acknowledged that a strict or literal interpretation of the rules could have unintended consequences. The department said the following practices would *not* be required under rules with which health-care providers must comply by April 2003 (or April 2004 for small health plans):

1. **Construction of new soundproof rooms in hospitals and doctors' offices.**
2. **For hospitalized patients, use of private rooms only.**
3. **Keeping patient charts at bedside.**
4. **Having X-ray boards totally isolated from all other functions (although the privacy rules do "require covered entities to take reasonable precautions to protect X-rays from being accessible to the public").**
5. **Prohibition of use of sign-in sheets in providers' offices.**
6. **Prohibition of friends and family members from picking up a patient's prescription from a pharmacist unless the patient has a written consent on file at the pharmacist prior to pickup.**
7. **Prohibition of scheduling appointments, surgery, and other procedures for first-time patients before the patient's written consent is on file.**
8. **Mandatory use of encryption systems for telephone and wireless communications. ■**

ply with the privacy rules, including requiring that patient information be used only for the intended purpose. A provider is not liable for violations of its business associates, but the provider's contract with the business associate must obligate the business associate to tell the provider when violations have occurred. If the provider is aware of a pattern of violations by a business associate, the provider must take "reasonable steps" to remedy the situation.

Patient consent and authorization

The federal regulations codify the current practice of most providers of obtaining a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment, or health-care operations. (The acronym used by the regulators to describe "treatment, payment, or health-care operations" is "TPO.") There are three circumstances in which written consent is not required: (1) emergency situations; (2)

situations in which there is a substantial communications barrier; and (3) indirect treatment relationships, such as with laboratories and clearinghouses.

The rules for the written consent forms include the following:

- The consent form can be brief.
- It must be in plain language.
- A single consent form is sufficient.
- For purposes of TPO, the provider need not have the patient sign a new form periodically.
- Providers should retain consent forms for six years from the last time the form was used.
- The consent form can be paper or electronic.
- If a physician consults with another provider about a patient's case, a separate consent for that consultation is not necessary since the physician's consultation is considered part of the initial consent to "treatment."

The regulations differentiate between a patient's "consent" and "authorization." A "consent," as noted, is for purposes of TPO. An "authorization" is generally for purposes other than TPO, such as sale of the patient's name for a commercial product mailing list or disclosure of health information for the purpose of obtaining life insurance or making employment decisions. "Authorizations" are limited to the purposes specified, and the authorization documents, unlike consent forms, must have an expiration date.

The parent or guardian of a minor child is considered to be the child's "personal representative" under the regulations, and, therefore, has a right of access to medical information about the child. If, however, a state law gives children an added right to privacy (such as allowing an adolescent to seek mental health treatment without a parent's consent), then the state law will control.

Release only what is needed

The regulations have a general policy of allowing only the minimum disclosure necessary to accomplish the intended purpose. For example, when providing information for billing purposes, the regulations allow providing diagnostic and treatment information, but transmission of an entire patient file generally would not be necessary or appropriate.

The "minimum necessary" requirement does not apply to information provided in connection with treatment. The regulators recognized that effective treatment is usually advanced by providing more rather than less information about the patient's condition. The guidance materials to the regulations add that "the covered health-care entity can develop role-based access policies

POLICY POINTS

Continued from previous page

that allow its health-care providers and other employees, as appropriate, access to patient information, including the entire medical records, for treatment purposes.”

When medical students, medical residents, and nursing students have access to patient information for training purposes, that is considered appropriate under the umbrella of the patient’s consent to release of information for the purpose of “health-care operations.” Health-care providers should have written policies describing the amount of disclosure or use of medical records that is permitted in different circumstances.

Speak softly and shield the files

The federal privacy regulations require that health-care providers “reasonably safeguard protected health information (PHI) including oral information.” The guidance materials add: “We do not expect reasonable safeguards to guarantee the privacy of PHI from any and all potential risks.” For example, in a busy emergency room, it may be necessary for physicians or nurses to speak loudly in order to ensure appropriate treatment. It also is permissible for health-care staff to orally coordinate services at hospital nursing stations.

Examples of reasonable measures to promote privacy include adopting rules about speaking quietly when discussing a patient’s condition with family members or at nursing stations and avoiding using a patient’s name in hallways and elevators.

The regulations and the guidance materials do not specify the exact measures which must be taken to protect privacy of patients’ records. The general rule is reasonableness under the circumstances, including consideration of the type of facility involved. The guidance materials did reassure providers that re-

design of facilities, including installation of soundproof rooms, generally is not necessary. The regulators added: “However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords on computers maintaining personal information.”

If a provider is planning on remodel-

An obstetrician cannot turn over a list of pregnant women to companies that provide diaper services, baby formula, or magazines—at least not without patient authorization.

ing offices and service areas as part of general improvement of facilities, privacy considerations should be part of the planning.

Marketing and research

The rules seek to limit the circumstances in which patients can be solicited for “marketing” which is defined as “a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.” Patient lists cannot be sold to third parties without the patient’s authorization. Thus, for example, an obstetrician cannot turn over a list of pregnant women to companies that provide diaper services, baby formula, or magazines—at

least not without patient authorization. A physician also cannot provide a list of patients to pharmaceutical companies for the purpose of the drug companies’ own promotions.

The regulations and the guidance materials list a number of communications that are not considered “marketing” and, therefore, are permitted. Examples include: face-to-face recommendation of prescription or over-the-counter medication; information about what health-care providers or services are covered under a health plan; letters and telephone calls reminding a patient to schedule or come in for an appointment; and telemarketing that is done on behalf of the provider (not on behalf of a third party).

When it comes to patient information in connection with medical research, the regulations allow use of information without the patient’s consent in three circumstances: (1) when the waiver of patient authorization has been approved by an Institutional Review Board (IRB); (2) when the use of the information is solely to prepare a research protocol, such as to determine the feasibility of conducting a study; and (3) when the information is being sought solely for research on decedents. In each of these circumstances, it must be documented that the research would not be practical without the waiver of authorization and that the risks to individuals from loss of privacy is minimal compared to the anticipated benefits of the research. For many research projects, including clinical trials, written authorization of the participant for release of information is required.

Penalties for violations

When Congress adopted the Health Insurance Portability and

POLICY POINTS

Continued from previous page

Accountability Act of 1996, it provided civil and criminal penalties for misuse of personal health information. Civil penalties are \$100 per violation, up to \$25,000 per person per year. Criminal penalties for obtaining or disclosing protected patient information are up to a \$50,000 fine and one year in prison. The penalties are even more severe for obtaining protected health information under “false pretenses” or using the information for commercial advantage, personal gain, or malicious harm.

The federal government anticipates the private and public sectors will spend \$17.6 billion over ten years to implement the new privacy rules. On the other hand, the government also has said it expects the electronic transaction regulations issued in August 2000 to result in savings of \$29.9 billion.

Approximately 18 months remain before health-care providers are required to comply with the new regulations. Providers are advised to spend the time between now and April 2003 implementing privacy policies and monitoring their effectiveness, as well as perhaps recommending adjustments that will make the rules work better. ■

Jeff Atkinson teaches courses in health-care reform and health-care contracts at DePaul University College of Law in Chicago, where he graduated summa cum laude. He also writes on legal, medical, and ethical issues.

Where to send your suggestions

Comments on issues of general concern regarding the privacy regulations can be submitted to the U.S. Department of Health and Human Services in one of three ways:

1. By an e-mail to ocrprivacy@hhs.gov
2. By a posting through the department's privacy Web site at www.hhs.gov/ocr/hipaa/
3. By mail to: Office for Civil Rights, Attention: Privacy, U.S. Department of Health and Human Services, 200 Independence Avenue, Room 509-F, Washington, D.C. 20201.

The department will review comments, but will not make individual replies. At this time, the department is not accepting individual technical or implementation questions, but it will announce when it is ready to do so on its Web site. ■