*Pain Physician*, Volume 4, Number 3, pp 280-284
2001, American Society of Interventional Pain Physicians®
ISSN 1533-3159

Health Law Review

# HIPAA Privacy Regulations: Practical Information for Physicians

**Erin Brisbay McMahon, JD and Tracy Lee-Huber, JD**

After much debate and controversy, the Bush administration announced on April 12, 2001, that it would implement the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations issued by the Clinton administration in December of 2000. The privacy regulations became effective on April 14, 2001. Although the regulations are considered final, the Secretary of the Department of Health and Human Services has the power to modify the regulations at any time during the first year of implementation. These regulations affect how a patient's health information is used and disclosed, as well as how patients are informed of their privacy rights. As "covered entities," physicians have until April 14, 2003, to comply fully with the HIPAA privacy regulations, which are more than 1,500 pages in length. This article presents a basic overview of the new and complex regulations and highlights practical information about physicians' compliance with the regulations. However, this summary of the HIPAA privacy regulations should not be construed as legal advice or an opinion on specific situations. Please consult an attorney concerning your compliance with HIPAA and the regulations promulgated thereunder.

**Keywords:** HIPAA, federal privacy regulations, uses and disclosures, individually identifiable health information, covered entities, business associates

One of the main goals of the federal Health Insurance Portability and Accountability Act (HIPAA) was to protect the security and privacy of patient data. HIPAA gave Congress until August 21, 1999 to enact comprehensive health privacy legislation. Because Congress failed to act, however, HIPAA's provisions then gave the Department of Health and Human Services (DHHS) the authority to promulgate privacy regulations.

Final HIPAA privacy regulations were issued on December 28, 2000, and were to be effective February 26, 2001. Due to an administrative glitch delaying their effective date, however, the privacy regulations underwent another public comment period that ended March 30, 2001. Much to the dismay of the health care industry and to the surprise of everyone else, the Bush administration decided to forego further delays in implementing the comprehensive privacy regulations. Thus, the HIPAA privacy regulations that were issued in December became effective on April 14, 2001, and physicians' offices must be in compliance with them by April 14, 2003.

From the law firm of Wyatt, Tarrant & Combs, LLP, Lexington, Kentucky. Ms. McMahon and Ms. Lee-Huber are attorneys at Wyatt. Address correspondence: Erin Brisbay McMahon, Esq., Wyatt, Tarrant & Combs, LLP, 250 W. Main St., Suite 1700, Lexington, Kentucky 40507. E-mail: emcmahon@wyattfirm.com

The privacy regulations, as they exist currently, are more than 1,500 pages in length including the rules, comments, and the predicted impact of the regulations on the health care industry. The last comment period produced at lease 7,500 additional comments on the controversial regulations. This article is intended to highlight and simplify, to the extent possible, the practical aspects of the regulations for physicians.

## COVERED ENTITIES

The burden of complying with the HIPAA privacy regulations is placed squarely upon "covered entities." Covered entities are defined as health plans, health care clearinghouses, or health care providers. A health care provider is defined as a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Therefore, physicians have an obligation to implement the privacy regulations. As a covered entity, physicians may not use or disclose protected health information except as permitted or required by the regulations.

## PROTECTED INFORMATION

The privacy regulations are intended to protect *all medical records* and *individually identifiable health information* held, created, or disclosed by a physician. As the regulations exist currently, they broadly protect health infor-

mation communicated electronically, on paper or orally. The proposed regulations only covered electronic records or any paper records that had at some point been in electronic form. However, the final regulations were expanded to cover all mediums in which health information could be transmitted.

Opponents have heavily criticized the regulations for their restrictive nature on physician communications and for the burden that the regulations place on the provision of health care. For example, opponents argue that the regulations will inhibit physicians from speaking freely with one another, their staff, or even with the patient while rendering health services if someone unauthorized were present to hear protected health information. Providers unsuccessfully argued for the final regulations to cover only electronically transmitted health information.

Individually identifiable health information (IIHI) is a subset of health information, including demographic information collected from the individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse. Protected IIHI must relate 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. For IIHI to be protected, it must also identify the individual or give the physician a reasonable basis to believe that the information in question can be used to identify the individual. Given the above factors, it is hard to imagine any information that would be excluded from protection by the physician in his or her practice.

## MINIMUM NECESSARY INFORMATION

Not only does the physician have an obligation to protect a patient's health information, but that physician must limit the amount of information used, requested or disclosed to the "minimum necessary" to accomplish an intended use, disclosure, or request. This minimum necessary obligation also applies to a physician's workforce.

Under the regulations, a physician has a duty to limit the access of his/her workforce to certain designated protected health information. A physician must identify those classes of individuals in his/her workforce who need access to protected health information in order to carry out their duties. Also, a physician must identify the categories of protected health information to which workforce access is needed and set any conditions appropriate to such access.

In line with the minimum necessary requirements, a physician's office must implement policies and procedures for any type of disclosure that it makes on a *routine* basis so that it limits the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all non-routine disclosures, a physician must (a) develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to achieve the purpose for which disclosure is sought and (b) review requests for disclosure on an individual basis in accordance with such criteria. Obviously, a physician's workforce must be trained on the above policies and procedures in order for the members of the workforce to carry out their respective duties.

The minimum necessary requirement does not apply to disclosures to or requests by a health care provider for treatment; to disclosures to the individual who is the subject of the privacy information; to disclosures made to the Secretary of Health and Human Services pursuant to an investigation for violation of the privacy regulations; or to disclosures that are required by law or by the privacy regulations. Even with these exclusions, there remains a debate between proponents of the privacy regulations and health care providers as to whether or not the minimum necessary requirement will dangerously hinder the ability of health professionals to provide unrestrictive treatment to their patients.

## PERMITTED AND REQUIRED DISCLOSURES

The general rule under the HIPAA privacy regulations is that a physician is allowed to use or disclose protected health information if it is:

- disclosed to the individual who is the subject of the information;
- pursuant to a valid consent to carry out treatment, payment or health care operations;
- pursuant to a valid authorization;
- without consent, if consent is not required under the regulations; or
- without written consent, if the individual was informed in advance of the use or disclosure and had the opportunity to agree to or to prohibit the disclosure.

A physician will be confronted with the regulations most frequently in the circumstance where the physician must obtain the consent of the patient to use or disclose personal health information in order to carry out treatment,

payment, or health care operations. The regulations require the physician to obtain the individual's consent prior to using or disclosing such protected health information to carry out treatment, payment or health care operations.
A physician is not required to obtain the patient's consent in certain limited situations. For instance, a physician does not need a patient's consent to use or disclose health information if the physician has an "indirect treatment relationship" with the individual, such as where the physician is reading an x-ray on the orders of a second physician who will report the results of the x-ray to the patient. Nor does the physician need the patient's consent in emergency treatment situations if the physician attempts to obtain the consent as soon as reasonably practicable after the delivery of treatment. Also, if a physician is unable to obtain the consent of an individual because of language or other communication barriers, the physician may use or disclose the protected health information if the individual's consent is clearly inferred from the circumstances. However, a physician who fails to obtain consent, as required, must document his or her attempt to obtain consent and the reason why consent was not obtained.

Furthermore, a physician may condition treatment of a patient on the provision of consent. A consent to carry out treatment, payment or health care operations must be, among other things, visually and organizationally separate from other written legal permission; in plain language; separately signed and dated by the individual; and inform the individual of his or her rights in and to the protected information. If a physician receives any other consent or written legal permission from an individual for a disclosure of protected health information to carry out treatment, payment or health care operations, the physician must follow the more restrictive consent.
Another important part of the regulations is the physician's obligation to obtain the patient's authorization if he or she wants to use the patient's protected health information or disclose the protected health information for a purpose other than carrying out treatment, payment or health care operations. A physician may not use an individual's protected health information or make a disclosure of that information to a third party without a valid authorization.

A valid authorization consists of, among other things, a description of the information to be used or disclosed; the identification of the person or class of persons allowed to make the requested use or disclosure; a signature of the individual and the date; and a statement of the individual's right to revoke the authorization. An individual may revoke an authorization at any time provided that the revocation is in writing and the physician has not taken action in reliance on it. A physician must document and retain any authorizations as well as provide the individual with a copy of the signed authorization.

## PATIENTS' RIGHTS

As one would expect from the pro-patient nature of the privacy regulations, the patient has an array of rights with respect to the use or disclosure of his or her individual health information. With few exceptions, an individual has the right to adequate notice of the uses and disclosures of protected health information; to know his or her individual rights to the protected health information; and to know the physician's legal duties with respect to the protected health information. The patient's rights manifest themselves in the form of a comprehensive notice that must be given by the physician to his or her patients.

The physician must provide a notice to the patient that is written in plain language containing information as to how the patient's protected information may be used or disclosed. The notice must also contain a description, and at least one example, of the types and uses and disclosures that the physician is permitted to make for treatment, payment and health care operations. Furthermore, the notice must set forth a description of each scenario in which the physician is required or permitted to use or disclose protected health information without the individual's written consent or authorization. The physician must inform the patient that, other than the exceptions listed above, uses and disclosures will be made only with the individual's written authorization and that the individual may revoke that authorization.

A statement of the individual's rights with respect to protected health information, and a brief description of how the individual may exercise these rights, must also be contained in the notice. The following are individual rights of a patient that must be provided in the physician's notice:

- the right to request restrictions on certain uses and disclosures of protected health information;
- the right to receive confidential communications of protected health information;
- the right to inspect, copy, and amend protected health information;
- the right to receive an accounting of disclosures of protected health information; and
- the right to obtain a paper copy of the physician's notice upon request.

The physician's legal duties under the privacy regulations must also be placed in his or her notice to the patient. The notice must state that the physician reserves the right to change the terms of his or her notice and to make new provisions effective for all protected health information retained by the physician. However, the physician must promptly revise and distribute his or her notice whenever there is a material change. The notice must briefly describe how patients may file a complaint with the physician if they believe that their privacy rights have been violated. Correspondingly, the notice must state that the individual will not suffer retaliation for filing a complaint and designate the name, title, and telephone number of a person or office to contact with concerns.

## OBLIGATIONS OF THE PHYSICIAN

The notice requirements contained in the HIPAA privacy regulations are only one piece of the physician's obligation puzzle. The physician must implement and maintain various policies and procedures as well as have in place appropriate administrative, technical, and physical safeguards in the workplace to protect the privacy of health information from any intentional or unintentional use or disclosure that would violate the regulations.

The privacy regulations require that a physician designate a privacy official who is responsible for the development and implementation of the above policies and procedures, and a contact person responsible for receiving complaints and for providing information about matters covered by the notice. As part of the implementation process, the physician must train all members of his or her workforce on established policies and procedures as necessary and appropriate for all members to carry out their duties with respect to protected health information. The physician must accurately document personnel designations and any training conducted by the physician. Likewise, the physician must apply appropriate sanctions against members of the workforce who fail to comply with established policies and procedures.

The physician also has an obligation to provide a process for individuals to make complaints concerning the physician's policies or procedures or the physician's compliance with such policies and procedures. The physician must document all complaints. The physician may not intimidate, threaten, coerce, discriminate against, or take other retaliatory actions against any individual for the exercise of his or her rights under the privacy regulations.

The privacy regulations require the physician to mitigate, to the extent practicable, any harmful effect that is known to the physician of a use or disclosure of protected health information in violation of the physician's policies and procedures or the privacy regulations. This responsibility of mitigating harmful effects from uses or disclosures of health information also applies to the physician when he or she deals with business associates. The regulations define a business associate as a person who performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information. Examples of business associates include: claim processors, data analysts, attorneys, accountants, and consultants. A physician may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on the physician's behalf only if the physician obtains adequate assurances that the business associate will properly protect the information. To assure adequate protection, the physician must enter into a written contract with the business associate.

The contract must establish the permitted and required uses and disclosures of the health information by the business associate; must authorize termination of the contract if the business associate violates a material term of the contract; and must outline mandatory obligations of the business associate under the privacy regulations. A physician is noncompliant with the regulations if he or she knew of a pattern of activity or practice of the business associate that violated their agreement unless the physician took action to cure the breach. If actions by the physician to cure the business associate's breach are unsuccessful the physician must terminate the contract, if feasible, or if not, report the problem to the Secretary of Health and Human Services.

## INVESTIGATIONS AND REVIEWS

The Secretary of Health and Human Services may conduct compliance reviews of the physician's office to determine whether the physician is complying with the privacy regulations. Physicians are expected to keep records and to submit compliance reports to the Secretary so that he may determine whether a physician is complying with the privacy regulations. Furthermore, the physician must permit access to information during his or her normal business hours unless the Secretary determines that such information may be hidden or destroyed. If so, the physician must permit access by the Secretary at any time. If the Secretary receives a complaint about a physician, the Sec-

retary may investigate the complaint by reviewing the physician's policies and procedures. The physician must fully comply with the investigation.

## STEPS TOWARD COMPLIANCE

Now that the privacy regulations are finalized, there are several steps that physicians may take today to get their practices in compliance mode. Physicians should do a comprehensive study of their practices to determine how patient information flows in and out of their organizations. If a physician has not done so already, he or she should quickly designate a compliance officer in order to begin determining what policies and procedures are necessary for compliance. It may be prudent for physicians to consider hiring a compliance officer from outside his or her current staff.

Physicians should evaluate the capacity of their current software and review the technical requirements for implementation of the transaction and code set requirements found in a separate section of the HIPAA regulations. Moreover, physicians need to consider budgetary concerns that will arise from the implementation of the expansive privacy regulations.

Tommy Thompson, the Secretary of DHHS, announced that DHHS will issue guidelines in the coming months on how the rule should be implemented in order to help providers with compliance. Thompson has stated that the guidelines will clarify some of the confusion regarding the impact the regulations might have on health care delivery and access.

## PENALTIES

The stakes for noncompliance with the HIPAA privacy standards are high. A physician failing to comply with the regulations can be subject to civil or criminal liability. The civil monetary penalties are $100 per incident, up to $25,000 per person, per year, per standard. There will be federal criminal penalties for physicians that knowingly and improperly disclose protected health information or obtain protected health information under false pretenses. Penalties will be higher for actions designed to generate monetary gain. The criminal penalties range up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under false pretenses; or up to $250,000 and up to ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

## COMPLIANCE DEADLINE

Physicians will have two years in which to come into compliance with the privacy regulations. Thus, physicians must comply with the HIPAA regulations by April 14, 2003. Given the magnitude of these regulations, it is imperative that physicians begin drafting a compliance plan and begin practicing the implementation of that plan today in order to meet the 2003 deadline.