Pain Physician, Volume 4, Number 4, pp 374-380
2001, American Society of Interventional Pain Physicians®
ISSN 1533-3159

Health Law Review

Beyond the Basics: Implementing the HIPAA Privacy Standards in Real Life Situations

William A. Sarraille, JD*, Anna Spencer, JD, Jerome T. Levy, JD**, Connie Raffa, JD**, Eileen Kahaner, JD**, and Kathleen Cheney, JD****

Although there is, at this point, a good deal of information available about the basic prohibitions and obligations imposed by the Privacy Standards (the Standards) under the Health Insurance Portability and Accountability Act (HIPAA), relatively little has been published on how the Standards will affect the day-to-day operations of various types of health care operations in specific situations, despite the almost universal acknowledgment that the Standards will, in fact, have a sweeping effect on those operations. In our presentations on the Standards for international pain practices, hospitals, ambulatory surgery centers, and others, we have noted the frustration of providers who have expressed a desire to "get beyond the basics" and to see, in tangible ways, how specific operations and recurrent issues will have to be confronted in light of the Standards. Accordingly, we have shifted many of our presentations to ones that focus on hypotheticals that deal with the difficult and quite specific issues which our clients are beginning to struggle with from a HIPAA compliance perspective. This article is designed to take some of the hypotheticals that we have discussed and present them to our readership. Our hope is that this discussion will begin to help international pain practices really understand the specific impact of HIPAA on their day-to-day operations.

Although the need to move forward quickly with changes designed to comply with the HIPAA Standards is clear, organizations, other than small health plans, will have until April 14, 2003 to comply with those Standards. Small health plans will have until April 14, 2004. As many international pain practices are realizing, the compliance deadline, despite being the better part of two years away, is frighteningly close in light of how much needs to be accomplished to ensure compliance.

The Department of Health and Human Services, acting with the Office of Civil Rights, has pledged to release a series of guidance documents over the next twelve months or so, which should measurably improve the difficult task of taking the Standards' often quite generalized language. In addition, there is the prospect that some not insignificant modifications to the Standards themselves will be made on consent, the minimum necessary, and other selected components of the Standards. Still, the need to press forward with implementation now is all too clear.

ARE YOU A COVERED ENTITY?

Pain Associates is a small practice that keeps its medical records on paper and in file drawers. It does not have any electronic medical records; it only uses its computer for accounting, scheduling and other fairly limited purposes.

Do the Standards apply to Pain Associates? What if the practice hires a billing company which files electronic health care claims on its behalf?

The Standards only apply to covered entities which is defined to include health plans, health care clearinghouse and those health care providers who engage in "electronic standard transactions" such as filing health care claims electronically. So, based on the facts presented here, Pain Associates is not a covered entity.

However, if Pain Associates were to hire a billing company to engage in standard transactions on its behalf, the Standards would apply to the practice. Having a billing company submit bills electronically for the practice would clearly convert Pain Associates into a covered entity. The practice may not escape the requirements of the rule by outsourcing the billing function. In addition, even though the practice itself only holds protected health information

From Arent Fox Klintner Plotkin and Khan, PLLC, Washington, DC. *Sarraille is a partner in the Health Law group of Arent Fox and general counsel to American Society of Interventional Pain Physicians. **Ms. Spencer, Mr. Levy, Ms. Raffa, Ms. Kahaner, and Ms. Cheney are Associates at Arent Fox. Address correspondence: William A. Sarraille, JD, 1050 Connecticut Avenue NW, Washington, DC 20036. Email: sarailw@arentfox.com

(PHI) in paper records, the Standards would protect the use and disclosure of PHI contained in those records, as well as the electronic records held by the billing company. This is because the definition of PHI includes any health information, in whatever form, which identifies an individual.

Additionally, if the practice submits one health care claim electronically itself, the Privacy Standards would apply to the practice. There is no minimum threshold for the number of claims submitted by a practice electronically for the requirements of the Standards to be triggered. So, hypothetically, if a covered entity engages in just one standard electronic transaction, it must meet the requirements of the Standards.

MISUSE OF PHI IN A GROUP HEALTH PLAN

The Angel City Physician Clinic, which has 250 employees, including three interventional pain physicians establishes a group health plan for the benefit of its employees. A couple of employees of the company perform administrative functions for the group health plan. They sometimes have access to PHI as a consequence. One of these employees learns that someone in the company has contracted hepatitis and tells her boss about the condition. The Clinic Administrator, fearful of the cost implications of the employee's condition, decides to include the employee in a reduction in force.

Would this disclosure by the group health plan violate the Standards?

Yes. It is often the case that ERISA group health plans do not have their own employees, so employees of the plan sponsor are named as fiduciaries to undertake administrative duties. This relationship poses the danger that information related to the health condition of employees will be improperly shared between the health plan and the plan sponsor. The rule permits group health plans to disclose PHI to plan sponsors for plan administration purposes, but not for employment-related actions. Thus, the disclosure by the employee working in plan administration to the boss for reasons other than plan administration would be a clear violation of the Standards. The consequences of such a violation to the company are enormous, given the criminal sanctions under the Standards.

IDENTIFYING BUSINESS ASSOCIATES

Comprehensive Pain Care, P.A. hires a law firm to defend it in a malpractice case. Ambulatory Surgery Centers, Inc. discloses PHI to a health plan for payment purposes.

Which of these entities, the law firm or the health plan, would be considered a business associate under the Standards such that a business associate contract would be required?

The law firm. A business associate is defined under the rule as an entity which (1) performs a function involving PHI *for or on behalf of* a covered entity or (2) provides specified services, such as legal and accounting services which involve the disclosure of PHI, *to* a covered entity. The law firm, because it would be defending the practice in a legal action and the practice would have to disclose PHI to the law firm to enable it to do that, is a business associate. Therefore, the law firm and the practice would have to enter into a contract which protects the use and disclosure of PHI by the law firm before disclosure is made. The health plan would not be a business associate of the ambulatory surgery center because it would not be performing a function for or on behalf of the ASC or providing one of the specified services to it. When it pays for services performed by the ASC, it is undertaking a task for its own business purposes, not as a contractor to the ASC.

COVERED ENTITY'S RESPONSIBILITY FOR BUSINESS ASSOCIATE'S MISUSE OF PHI

An interventional pain practice hires an accounting firm to provide it with on-going analysis of its operations to better improve its efficiency and profitability. The accounting firm issues a report to the practice. An employee of the accounting firm uses the PHI his employer gathered during the contract and faxes it to a number that he thinks is one used by the practice. Unfortunately, it is not. It is the fax number of the patient's brother, who was listed as a contact for the patient on the medical records in the event of an emergency.

Would the practice be subject to penalties under the rule for the actions of the accounting firm and its employee?

It depends. Clearly, the disclosure of PHI by the accounting firm would violate the terms of the business associate contract as the disclosure was not made for the purposes of improving the business operations of the hospital. Under the Standards, covered entities are not required to actively monitor their business associates, but they will be held responsible for business associate violations where they have knowledge of an improper use or disclosure by

the business associate, and fail to take appropriate corrective action. Assuming the practice was not aware of the disclosure of its PHI and took appropriate corrective action once (and if it became aware of the misuse of the PHI), the practice would not have violated the Standards.

DE-IDENTIFYING INFORMATION

A consulting company, We Have All the Answers, Inc., consults with an interventional pain practice on how it may improve its billings and collections. In order to do this, the consulting company must have access to practice bills and the medical information contained in the bills. If the practice discloses this information to the consulting company, it must have patient consent and a business associate contract which allows the disclosure. Further, it must ensure that it provides the minimum necessary PHI to accomplish the billing and collection review.

Does the practice have another option besides the above?

Yes. The practice could create de-identified information and provide only that information to the consulting company. The practice would need to remove the name, telephone number, fax number, address, social security number, medical record number, photographic image and any other identifier from the record which could be used to identify an individual. Or, it could remove fewer identifiers than is required to meet this safe harbor, if a person with appropriate statistical and scientific knowledge determines that the risk of identification would be small. The Standards do not apply to the use and disclosure of de-identified information. So, the practice could disclose the de-identified information to anyone for any purpose assuming that it did not also disclose the key to the information.

If the consulting company needed to be able to refer the practice to particular health records, the practice could assign dummy numbers for that purpose which the practice could later use to match information with a particular record. Covered entities may use codes and similar means of marking records so that they may be linked or later re-identified, if the code does not contain information about the subject of the individual (such as a code that is derivative of an individual's social security number). The covered entity is also prohibited from disclosing the mechanism for re-identification, such as tables, algorithms, or other tools that could be used to link the information.

The problem with the de-identification approach, of course, is that it can be so costly to employ. The cost grows with the number and volume of documents that must be "scrubbed."

DISCLOSURES TO OVERSIGHT AGENCIES

An insurance company acts as the Part B Carrier to Pain Consultants, P.A. The physician practice submits a large number of Medicare claims for a particular injection procedure so that the practice's utilization rates of this procedure appear aberrant, even though they are not. The Carrier suspects billing fraud and requests medical records from the practice as part of a post-payment audit.

May the practice disclose this information without permission from the patient under the Privacy Standards?

Yes. The Privacy Standards permit covered entities to disclose PHI to health oversight agencies, such as the OIG and those who act on behalf of such agencies for the purposes of oversight activities, without obtaining permission (consent, verbal agreement or authorization) from the individual who is the subject of the records. Therefore, the disclosure of PHI by the physician practice to the Carrier would not violate the Standards.

LEGAL REQUESTS FOR INFORMATION

A person injured in a car crash is treated at an ambulatory surgery center. The ASC receives a request for medical records from an attorney who represents the driver in the automobile accident. The request states that the attorney represents the driver who has been sued for negligence by the patient and to send the records to the lawyer within 15 days of receipt of the letter.

May the center disclose the patient's records to the attorney without an authorization from the patient?

No. Although there is a category of permissible uses and disclosure which permits the use and disclosure of PHI for judicial and administrative purposes without patient permission, the rule permits disclosure only upon (1) an order from a court or administrative tribunal OR (2) upon proof that the person seeking disclosure attempted to notify the individual who is the subject of the information and the individual did not object, or that a qualified protective order was obtained. It does not matter that state law might permit the disclosure under the theory that the patient waives his right to confidentiality by filing suit in a claim that puts his health condition at issue. To release the infor-

mation, the patient would have to sign a specific authorization for this purpose.

WHAT ABOUT MARKETING AND FUNDRAISING?

A large community hospital has recently established a new pain center. The hospital sends flyers announcing the new pain center to all persons who have been admitted to the hospital within the past six years. It also accesses it records to determine who has received pain treatments at the hospital in the past six years. These individuals receive solicitations to try and raise money for the development of the new pain center. The hospital also posts on its web site a positive testimonial from a patient who received injections at the center, but does not obtain the individual's authorization to do so.

Are these activities permitted under the Privacy Standards?

The Standards define marketing as a communication about a product or service designed to encourage the recipient of the communication to purchase or use the product or service. In response to significant comments to the Standards, the Standards permit numerous forms of marketing activities without the need for an individual authorization. For instance, a covered entity may use and disclose protected health information for marketing its health-related products and services if certain requirements are met. First, the communication must identify the covered entity, state if the covered entity will be paid for making the communication, and state that the individual may opt-out of future communications. Additionally, if the covered entity has used PHI to target individuals based upon their health status, the covered entity must make a determination that the service being advertised would be beneficial to the individual. It also must explain why the individual has been targeted to receive the flyers.

In order to be compliant with the rules, all flyers announcing the pain center must specifically identify the hospital. In addition, the flyers should indicate how the recipient of the flyer may opt out of future communications.

It would be inappropriate for the hospital to target past pain patients for pain center solicitations unless the patient had signed an individual authorization specific to the intended use. It is important to distinguish marketing from fundraising activities under these rules. Fundraising is a solicitation for the purpose of raising funds to benefit a covered entity. In comparison to marketing activities, fundraising activities are much more restricted under the Privacy Standards. According to the rules, general fundraising may not be targeted to an individual based upon the past health status of the individual. Instead, PHI used for fundraising, without a specific patient authorization, must be limited to demographic information and dates of treatment. Diagnosis or nature of the services received is not considered "demographic information." Demographic information includes name, address and other contact information, age, gender and insurance status.

Finally, under the new Standards, it is impermissible to post a patient testimonial without permission from the individual. This use requires a specific written authorization from the individual.

PARTICIPATION ON A PROVIDER COMMITTEE

One of the physicians with staff privileges at a community hospital is asked to participate in the hospital's quality assurance reviews.

May the physician participate in this review of PHI, even though the review does not involve the physician's own patients?

Yes. Under the Standards, providers in an organized health care arrangement may share information to support the health care operations of the enterprise, even though the sharing may not directly benefit a particular participant of the arrangement. Organized health care arrangements are arrangements which involve clinical or operational integration among legally separate covered entities. Individuals who obtain services from them have an expectation that operations are integrated and jointly managed.

The definition of health care operations includes quality assessment and improvement activities of a covered entity or of an organized health care arrangement in which a covered entity participates. Therefore, the physician on staff at the hospital may review information containing PHI for quality assurance purposes, even though the information does not relate to his own patients.

PICKING UP MEDICATIONS FOR A FRIEND

An elderly woman is bedridden and is unable to leave the house to pick up her pain medication. She calls a friend of hers and asks her to pick up her prescription for her. Her friend goes to the pharmacy and asks to pick up the

woman's medication.

May the pharmacist give the prescription medication to the friend?

Yes. One of the permissible disclosures under the Standards is for disclosures to persons assisting in a patient's care. If an individual is present, this type of disclosure may be made, where the covered entity simply obtains the affected individual's oral agreement. The agreement does not have to be written; it may even be inferred from the circumstances. If an individual is not present, or is incapacitated, a covered entity may release the information if it determines, in the exercise of its reasonable professional judgment, that the disclosure is in the best interests of the patient and it discloses only the PHI relevant to the person's involvement in the patient's care. So, the pharmacist in this example may disclose PHI to the patient's friend if it is in the patient's best interests, but it must restrict the amount of information given about the patient.

Of course, the rule leaves open exactly what information could be disclosed to a friend in this kind of situation. It is common today for pharmacists to attach on the outside of a bag containing the medication a sheet which describes what the medication is for, the instructions for its use and information about combining the medication with other medications the patient may be taking. In a case like the one presented here, the pharmacist might be under an obligation to place this sort of information within the bag.

What information could be disclosed to the friend would probably depend on the circumstances. If a friend or spouse had to assist the patient with taking the medication, the pharmacist could probably disclose more information regarding the recommended doses and need for the medication.

DISCLOSURES FOR LAW ENFORCEMENT PURPOSES

An interventional pain management physician prescribes narcotics for some of his patients that suffer from chronic pain. One day, an agent from the Drug Enforcement Agency (DEA) appears at the physician's office with a subpoena for some of the physician's medical records. The physician has been targeted for investigation because the physician allegedly has irregular patterns of prescribing controlling substances.

May the physician release PHI as requested by the DEA agent consistent with the Privacy Standards?

Under the Privacy Standards, disclosures to law enforcement agents are permissible without individual authorization only under certain circumstances. One circumstance where it is permissible for a provider to disclose PHI to law enforcement officials is where the disclosure is required by law. A covered entity may disclose PHI in compliance with a court order or a court-ordered warrant, or a subpoena or summons issued by a judicial officer, or a grand jury subpoena. So, it would clearly be permissible for the pain physician in our hypothetical to disclose the information requested by the DEA agent.

WHAT IS THE NOTICE OF PRIVATE PRACTICE?

Mr. Green, a 38-year-old man, is referred to Dr. Smith for evaluation of chronic pain. In addition to other elements of the plan, Dr. Smith assesses the medical management and finds the patient is not as compliant as he should be with his medications. Dr. Smith also learns that Mr. Green has a tendency to miss appointments. To improve Mr. Green's compliance, involving the lower back Dr. Smith's group has started mailing medication and appointment reminders to existing patients. Like other conscientious physician groups, Dr. Smith's practice also is concerned about its own compliance activities. As a result, the practice has decided to contract with an outside law firm to coordinate annual chart audits. The practice also has hired an external billing company to perform billing and collection services on behalf of the practice. When Mr. Green presents at the admission's window of Dr. Smith's practice, he is given a "Notice of Privacy Practices."

Why is he given this document and what is it?

The Privacy Standards require covered entities, such as physician practices, to develop a "Notice of Privacy Practices" that must be shared with any individual who provides PHI to the covered entity. It must be provided to a patient in writing no later than the first time that the practice sees the patient after the Privacy Standards implementation deadline of April 14, 2003.

The Notice of Privacy Practices is a complete, and detailed description of a covered entity's possible uses and disclosures of PHI. It explains how the provider will use and disclose PHI obtained from a patient. The Notice also explains the rights of individuals under the Privacy Standards and the legal obligations of the covered entity with

respect to PHI. In general, health care providers must post the Notice prominently, and must furnish a copy to each individual when the individual first receives care.

The detailed elements that must be contained within the Notice are specified in the Privacy Standards. While many of the elements appear generic, every covered entity must customize the Notice to its own behavior.

The Notice must include a description and at least one example of the types of uses and disclosures that the covered entity expects to make. Treatment, payment, and health care operations each require a separate example. Dr. Smith's Notice might reference the outside billing company or auditor as an expected recipient of Mr. Green's PHI.

Since the practice contacts patients with appointment reminders, Dr. Smith's Notice also will need a separate explanation about this intended use. Another separate statement also would be required if the practice intended to send individuals information about treatment alternatives, or other services that may be of interest.

The Notice also must include a general description of other permitted uses for which neither written consent nor an authorization are required. This includes disclosure to individuals involved in the patient's care or payment related to the individual's care, such as family members, relatives, or close personal friends. It also includes a general discussion of the public policy exceptions to the consent/agreement/authorization requirements.

Dr. Smith's practice, like all covered entities, must establish policies and procedures to implement the individual rights mandated under the Privacy Standards. The Notice must explain these rights and how an individual may exercise them.

Finally, the Notice must contain certain contact information about how to file a complaint with the Secretary of the Department of Health and Human Services and the health care provider, and must provide the name and telephone number of a person at the covered entity who may be contacted for more information about the Privacy Standards.

Covered entities should think carefully when developing their Notice. Making revisions may result in significant costs because covered entities must inform individuals when the Notice is amended and offer them a revised Notice. It is important to draft this document correctly in the first instance.

PSYCHOTHERAPY NOTES

A psychologist provides psychotherapy as part of Pain Consultants, P.A. One of the patients of the psychologist is a resident of a Nursing Facility. The Nursing Facility has requested copies of the psychotherapy records to substantiate the medical necessity of the services. The pain practice submits bills to Medicare electronically and is a covered entity under the Standards.

Is the psychologist permitted to disclose his or her psychotherapy notes to the Nursing Facility?

No, unless an authorization is obtained. In general, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes. There are limited exceptions to this rule, none of which are applicable here. Psychotherapy notes are notes kept by mental health professionals to document or analyze the contents of conversations during private, group, or family counseling sessions and are separated from the rest of an individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. Because the term psychotherapy notes is defined to exclude information necessary for treatment and payment, it was thought that there should be little need to use or disclose the notes of conversations between psychotherapists and their patients. In this way, the Privacy Standards provide special protections to psychotherapy notes.

A valid authorization to disclose psychotherapy notes must contain at least the following elements:

- a description of the notes to be disclosed;
- the name of the psychotherapist being authorized to make the requested disclosure;
- the name or identity of the person or class or persons to whom the disclosure is to be made;
- an expiration date or expiration event;
- a statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;
- a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be

protected by the privacy Standards;
- signature of the individual and date; and
- if the authorization is signed by a personal representative, a description of such representative's authority to act for the individual.

FAMILY MEMBERS INVOLVED IN CARE COMMUNICATIONS

Mrs. Johnson is 60 years old, has chronic pain, heart disease, diabetes, arthritis, depression, and some hearing loss. The patient's primary language is Spanish. Although the patient understands most English and can speak some English, the patient is most comfortable in her native language. The patient's daughter has always handled patient's affairs, including communicating with her mother's health care providers on symptoms, course of treatment, medication, tests, obtaining copies of medical records, and all medical decisions. The daughter also translates for the mother when appropriate during medical visits and about follow-up decisions.

How do the HIPAA Privacy standards impact the daughter's role in managing her mother's care?

The health care entities (insurance payors, nursing home, home health agencies, physicians, etc.) must make sure that there is appropriate permission from the patient for information to be shared with the daughter. In a case such as this, a verbal agreement from the patient should be sufficient. The consent may also be inferred by the circumstances. The minimum necessary restriction would still apply, however.

CONCLUSION

The Privacy Standards will pose many implementation challenges, but with more information about how to respond to specific situations, those implementation challenges may seem somewhat less daunting.