AMERICAN SOCIETY OF INTERVENTIONAL PAIN PHYSICIANS

MODEL COMPLIANCE PROGRAM FOR THE HIPAA PRIVACY STANDARDS

September 25, 2002

PREPARED BY:
THE LAW FIRM OF
ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
WASHINGTON, DC

TABLE OF CONTENTS

Page

Introduction

Profound advances in technology have permitted the health care industry to increase steadily its use of electronic technology to store and transmit health information. In an era of cost containment, these developments offer significant opportunities for health care providers to achieve cost-savings, while improving service delivery. However, at the same time, public concern is growing about the role of technology in violations of the confidentiality of personal health information.

To address these issues, the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 (also known as "HIPAA") required the promulgation of a set of interlocking regulations that will change fundamentally the handling and processing of health information. HIPAA requires the federal government to adopt:

- uniform standards for the transfer of certain electronic transactions and associated code sets;
- national identifiers for health care providers, employers, health plans, and individuals;
- uniform standards for the use and disclosure of personal health information;
- new patient rights with respect to personal health information; and
- uniform standards for electronic security.

Almost every health care provider, regardless of size, will be required to comply with the HIPAA regulations. Understanding these new rules can be daunting. This Model Program for the HIPAA Privacy Standards is designed to assist your practice's compliance efforts. It does not address every topic governed by HIPAA. Rather, it focuses on compliance with the new Privacy Standards governing the use and disclosure of protected health information.

While HIPAA imposes the same general obligations on every covered health care provider, implementation must be tailored to the particular needs of your practice. This document provides examples of the components necessary to satisfy the obligations of HIPAA; but each practice must separately and independently evaluate its needs and the shape and content of its own program. Each practice should consult with an appropriate expert in this field. The American Society of Interventional Pain Physicians ("ASIPP") is not to be regarded as providing any advice or direction through this publication. All covered health care providers must be in compliance with the Privacy Standards by **April 14, 2003**. It is never too early (or too late) to begin. A glossary of key terms may be found at the end of this document and before the attachments.

ASIPP is pleased to offer this compliance program. ASIPP is grateful to William A. Sarraille, J.D., Eileen Kahaner, J.D., and Anna Spencer, J.D. of Arent Fox Kintner Plotkin & Kahn, PLLC, a law firm with offices in Washington, D.C. and New York, NY, and one of the leading health care practices in the country, for developing this document. Mr. Sarraille serves as ASIPP's National Regulatory Special Counsel.

The Privacy Standards

The Standards for Privacy of Individually Identifiable Health Information ("**the Privacy Standards**")[1] limit the use and disclosure of certain personally identifiable health information. The Standards are intended to facilitate the use and transfer of information within the health care delivery system and to increase the difficulty of transferring information outside of the system. The Privacy Standards are structured in three sections:

- Restriction of the use and disclosure of certain health information;
- Establishment of individual rights regarding health information; and
- Establishment of administrative requirements to ensure confidentiality and appropriate use of health information.

Most entities covered by the Privacy Standards have until April 14, 2003 to achieve compliance.[2]

I. Information Protected by the Privacy Standards

The Privacy Standards govern the use and disclosure of protected health information ("**PHI**"). PHI is broadly defined. PHI is individually identifiable information that relates to the health of an individual or the provision of health care to an individual. PHI may be maintained or transmitted in any format, including electronic, paper, or oral communications. Examples of PHI include information in paper and computer billing records, patient medical charts, discussions about a patient's health condition between a physician and a patient's family member, diagnostic test results, and the contents of a hospital patient directory. PHI excludes individually identifiable health information in employment records held by a Covered Entity in its role as an employer.

The Privacy Standards do not apply to "**de-identified information**." De-identified information is health information from which individual identifiers have been removed. De-identified information may be used and disclosed freely, so long as any key that could re-identify the data is protected.

Typically, PHI will be de-identified by removing an enumerated list of data elements, such as, but not limited to, name, address, birth date or age, telephone number, medical

---

[1] The full text of the Privacy Standards may be found at 65 Fed. Reg. 82,462-82,829 (Dec. 28, 2000). The Standards were revised on August 14, 2002 and may be found at 67 Fed. Reg. 53,182 (August 14, 2002).

[2] Congress recently enacted a law that permits providers to delay the implementation of the standard electronic transaction requirements for one year from the date of October 16, 2002, if a compliance plan meeting the requirements of the law is filed with the Department of Health and Human Services ("HHS") and certain other restrictions apply. This law does not, however, delay in any way the implementation of the Privacy Standards. For information about the law, please visit the Arent Fox website at www.arentfox.com, choose "Publications" and then choose "Alerts" and see Alert dated 12/28/01.

record number, biometric identifiers, and health plan number. The Privacy Standards also permit health information to be treated as de-identified if a person with appropriate statistical and scientific expertise determines that the risk of re-identification is very small. [3]

The Standards also permit a more limited data set to be used for research, public health purposes or health care operations purposes. The limited data set may not contain enumerated identifiers that directly identify an individual, but may contain certain patient specific information, such as admission, discharge and service dates, date of death, age and five-digit zip code. Disclosure of the limited data set is conditioned upon the covered provider obtaining a data use or similar agreement from the recipient. The data use agreement must require, among other things, that the recipient limit its use of the data to the original reasons for the disclosure and refrain from attempting to re-identify the information or use it to contact the subjects of the information.

II. Entities Covered by the Privacy Standards

A. Covered Entities and Other Organizations Recognized Under HIPAA

The Privacy Standards directly apply to "covered entities." A **Covered Entity** is defined as:

- a health plan,
- a health care clearing house, or
- a health care provider who transmits health information in electronic form in connection with a transaction for which there is a HIPAA standard form.

A health care provider includes individuals and entities such as physicians, ambulatory surgery centers, nurses, and hospitals. It also includes persons or entities that provide, bill for, or are paid for health care services in the normal course of business.

Health care providers who do not undertake electronic transactions for which there is a HIPAA standard are not covered by the Privacy Standards. The specific "**HIPAA Standard Transactions**" include: health care claims, health care payments and remittance advices, coordination of benefits, health care claims status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, and health claims attachments.

If for no other reason, most interventional pain practices will submit HIPAA Standard Transactions by engaging in electronic claims submissions. Submitting even one electronic claim will trigger application of the Privacy Standards for all patients and all

[3] Creating de-identified information could be useful if an interventional pain practice considered undertaking certain clinical research, coding audits, or the sale of clinical information to third parties, such as pharmaceutical or medical equipment companies. However, the requirements for de-identification are demanding enough that they are unlikely to be of use in many circumstances. The ease with which an interventional pain practice may create de-identified information will depend upon the sophistication of the practice's electronic record systems.

payers. Contracting with another entity (i.e., a billing company) to transmit electronic claims on your practice's behalf will not permit the practice to avoid the Privacy Standards.

The Privacy Standards recognize today's health care system is complex and no longer comprised solely of individual health care providers. There are special rules that apply, for instance, to "**organized health care arrangements**" and "**affiliated covered entities**."

An organized health care arrangement is comprised of multiple, separate Covered Entities. An organized health care arrangement is a (1) clinically integrated care setting in which individuals typically receive care from more than one health care provider or (2) an organized system of health care in which more than one Covered Entity participates. To be considered an organized system of health care, the entities must hold themselves out to the public as participating in a joint arrangement, and the entities must jointly participate in utilization review, quality assessment and improvement, or payment activities. An example of an organized health care arrangement includes a hospital or ambulatory surgery center and its medical staff.

The Privacy Standards allow Covered Entities in an organized health care arrangement to develop joint Notices of Privacy Practices[4] provided that each Covered Entity participating in the arrangement agrees to follow the terms of the notice with respect to PHI created or received by the Covered Entity as part of its participation in the arrangement. Additionally, a Covered Entity that participates in an organized health care arrangement may disclose PHI about an individual to another Covered Entity participating in the arrangement for health care operation activities of the arrangement.

For purposes of the Privacy Standards, affiliated covered entities may designate themselves as one Covered Entity. This means that the entities may enjoy operation efficiencies by developing common HIPAA forms. Additionally, designation of affiliated entities as one entity means that the entities may share PHI between one another freely for health care operations.

Affiliated covered entities are legally separate entities that elect to designate themselves as a single Covered Entity for purposes of the Privacy Standards. The entities must be under common ownership or common control. This means that (1) one entity has an ownership interest of five percent or more in another or (2) one entity has the power to significantly influence or direct the actions or policies of another entity. An example of affiliated covered entities includes a separately incorporated ambulatory surgery center owned by a physician practice.

B. Business Associates

The Privacy Standards also apply *indirectly* to a Covered Entity's **Business Associates**. A Business Associate is defined under the Privacy Standards as an entity which:

---

[4] Notices of Privacy Practices are documents required by the Privacy Standards which outline how a practice uses and discloses PHI. They are discussed in Section V(A).

- performs a function involving PHI for or on behalf of a Covered Entity, or
- provides specified services to a Covered Entity, such as legal, actuarial, accounting, consulting, data aggregation, management, accreditation, or financial services, which involve the disclosure of PHI.

Outside auditors, billing companies, practice management companies, billing and coding consultants, attorneys, insurance companies that perform risk management services, and medical directors all will be considered Business Associates, if their work requires the use or review of PHI.[5]

Business Associates do not include employees or independent contractors who are members of the Covered Entity's workforce. The term "workforce" includes employees, volunteers, trainees, independent contractors (including part-time sub-specialists) and other persons who perform work for the Covered Entity and whose conduct is under the direct control of the Covered Entity. Business Associates also do not include health care providers who receive PHI in connection with their own treatment of an individual patient. For example, the physicians on a medical staff of an ambulatory surgery center or a hospital are not considered Business Associates of the ambulatory surgery center or the hospital for this reason.

The regulations permit Covered Entities to share PHI with Business Associates so long as Business Associates are contractually bound to appropriately safeguard the information and the Covered Entity addresses situations where its Business Associates fail to comply with their privacy obligations. These requirements must be documented in a written agreement between the Covered Entity and the Business Associate, called a **Business Associate Agreement**. Exhibit 1 is a model Business Associate Agreement.

The particular elements that a Business Associate Agreement must contain are:

- The Agreement must identify the permitted and required uses and disclosures of PHI to and by the Business Associate. [6]

- The Agreement must prohibit the Business Associate from using or further disclosing the PHI, other than as permitted by the contract or as required by law. The Business Associate also must implement appropriate safeguards to protect against inappropriate disclosure or use. [7]

---

[5] At this time, entities that provide accreditation services are considered Business Associates. This characterization is being challenged and Covered Entities should follow developments in this area.

[6] This does not mean that every specific use or disclosure must be specified. Rather, the Agreement must discuss the general purposes for which the Business Associate may use and disclose PHI and the types of persons to whom it is anticipated that the Business Associate may make further disclosures (i.e., persons or entities to whom the Business Associate will likely, in turn, make disclosures).

[7] The Privacy Standards do not specify what qualifies as "appropriate safeguards." Interventional pain practices should inquire about the internal safeguards its potential Business Associates have implemented. Reasonable safeguards likely would include limiting access of personnel to hardcopy or electronic information, policies and procedures prohibiting disclosure to unapproved third parties, internal

- If a Business Associate becomes aware of any use or disclosure not provided for in the agreement, the Business Associate must report this violation to the Covered Entity.[8]

- The Business Associate must ensure that any of its agents and subcontractors that have access to the Covered Entity's PHI (such as a transcription company that subcontracts with independent contracts to furnish services) will agree to the same conditions and restrictions that apply to the Business Associate.

- The Business Associate must agree to provide copies of those records that the interventional pain practice identifies as a "designated record set." See, below, at page 15 for more discussion of this "access" requirement and the other HIPAA patient rights.

- The Business Associate also must agree to make requested amendments to inaccurate or incomplete information that it holds and to provide an "accounting" of certain uses and disclosures.

- For the purpose of determining whether or not a Covered Entity is complying with the Privacy Standards, a Business Associate must agree to make available to the Secretary of the Department of Health and Human Services its internal books, records, and practices relating to its use and disclosure of PHI.

- At the end of the engagement, the Privacy Standards require the Business Associate to agree to destroy or return, to the extent feasible, all PHI received from the Covered Entity. [9]

- The Covered Entity must be permitted to terminate the Agreement if the Covered Entity determines that the Business Associate violated a material term.

Although Covered Entities are not generally responsible for policing the activities of their Business Associates, Covered Entities must exercise some oversight. A Covered Entity will violate the Privacy Standards if (1) a Business Associate has materially breached the contract terms and (2) the Covered Entity knew of the violation, and (3) the Covered Entity did not take reasonable steps to correct the violation or minimize its consequences. If these efforts are unsuccessful or if the Business Associate continues to act inappropriately, the Business Associate Agreement generally must be terminated. [10]

---

computer security measures such as use of passwords or encryption, where appropriate, and training on the appropriate handling of confidential information.

[8] Business Associates should represent that they will train their employees about what would constitute violations and implement policies and procedures mandating internal reporting of violations.

[9] The Business Associate may retain information if the return or destruction of the information is not feasible. Any retained information must remain subject to the protections of the contract.

[10] In certain situations, however, terminating the contract may not feasible. For example, an interventional pain practice may have invested significant resources in an information system that only is serviced by the Business Associate. In this situation, the Privacy Standards say that the practice should report the violation to the Secretary of the Department of Health and Human Services.

III. Rules Governing the Handling of Protected Health Information

Under the Privacy Standards, Covered Entities must limit their use and disclosure of PHI in a variety of ways. Nevertheless, Covered Entities are required to disclose PHI in two situations. In addition, they are allowed under HIPAA, though not required by HIPAA, to use or disclose PHI without the individual's permission for certain public policy purposes, such as research, law enforcement, and disclosure to public health authorities. Additionally, with the exception of psychotherapy notes,[11] they may use and disclose PHI for treatment, payment and health care operation purposes without individual permission, unless permission is required by some law other than HIPAA. For all other purposes, a Covered Entity must have appropriate permission from the individual who is the subject of the data, in the form of a verbal agreement or a written authorization, as dictated by the circumstances.

A. Required Disclosures

With very limited exceptions, Covered Entities must release PHI to the individual who is the subject of the information or to the individual's appointed representative. Generally, the parent of a minor child is considered the child's representative. Limitations on these rights are governed by state law and the Privacy Standards defer to these determinations. Covered Entities also must release PHI to the U.S. Department of Health and Human Services, upon request, so that the Department can audit compliance with the Privacy Standards.

B. Uses and Disclosures Permitted Without Individual Permission

1. Public Policy

Provided that technical regulatory requirements specific to the particular situation are satisfied, Covered Entities may use or disclose PHI for a number of public policy purposes without an individual's permission. The Privacy Standards do not require, however, that a Covered Entity use or disclose information in this manner, though other provisions of law may do so.

The Privacy Standards establish requirements for public policy uses and disclosures related to:

- Disclosures required by state or federal law.
- Public health activities, such as vital statistics, communicable disease reporting, child abuse or neglect reporting, post-marketing surveillance or adverse event

[11] Psychotherapy notes are the notes taken by a mental health professional during a counseling session and are maintained separately from the rest of an individual's medical record. In general, an authorization is required to use or disclose psychotherapy notes. Some exceptions exist, however. For instance, the creator of the notes may use or disclose PHI contained within the notes for treatment, payment and health care operations.

reporting, department of motor vehicles visual acuity reporting, and certain OSHA-related workplace medical surveillance or work-related illness or injuries.

- Reports of adult abuse, neglect, or domestic violence. Disclosures are permissible if they are (i) required by law or (ii) expressly authorized by law and the disclosure is necessary to prevent serious harm to the individual or other potential victims, based upon the professional judgment of the Covered Entity or if the individual is unable to agree to the disclosure because of incapacity, a law enforcement or other public official represents that the information is not intended to be used against the individual, and that immediate enforcement activity would be materially and adversely affected by waiting until the individual would agree to the disclosure.[12]

- Health oversight activities, such as investigations, payor coding and billing audits,[13] licensure or disciplinary actions, or criminal, civil or administrative proceedings.

- Judicial and administrative proceedings pursuant to an order of a court or administrative tribunal, a subpoena, or a discovery request.[14]

- Law enforcement activities pursuant to a court order, warrant, subpoena, summons, or discovery request.[15] Additionally, these provisions allow disclosures (i) of limited information for identification and location purposes, (ii) in response to a law enforcement official's request about an individual who is, or is suspected to be, a victim of a crime, (iii) to alert law enforcement about an individual who has died, (iv) that the Covered Entity believes in good faith constitute evidence of criminal conduct that occurred on the premises of the Covered Entity and (v) to report crime occurring during emergencies.

- Law enforcement activities as required by law for the purposes of identifying a victim or locating a suspect, fugitive, missing person or witness.

---

[12] The individual (or his or her personal representative) must be informed that the PHI has been disclosed, unless the Covered Entity believes this would (i) place the individual at risk of serious harm or (ii) the personal representative is reasonably believed to be responsible for the abuse, neglect, or injury.

[13] Consequently, this exception permits a health care provider to produce patient medical records in connection with a government payment audit without obtaining patient permission.

[14] Before furnishing information not requested by a court or administrative order (i.e. in response to a subpoena, discovery request, or other similar request), the Covered Entity must receive assurances that the individual has received notice of the request or reasonable efforts have been made to notify the individual or the requesting party has obtained protective order from a court or administrative tribunal. In the alternative, the Covered Entity may make reasonable efforts to provide notice to the individual or to seek a qualified protective order. The Privacy Standards contain a detailed explanation of how these obligations may be satisfied. Due the complexities of this provision, interventional practices should consult with appropriate legal counsel before information is disclosed under this provision.

[15] If the material is requested pursuant to an administrative subpoena or civil investigative demand, the request must be relevant and material to a legitimate law enforcement inquiry, limited in scope, and de-identified information cannot reasonably be substituted. As it may be difficult for many health care providers to make these determinations, providers should consult with appropriate counsel before information is provided to law enforcement officials under this provision.

- Decedents and donated tissues and organs, including disclosures to coroners, medical examiners, funeral directors, organ procurement organizations, transplant centers, and eye or tissue banks.

- Research, including conducting epidemiological studies, evaluating outcomes, and other purposes, if an Institutional Review Board or Privacy Board determines, among other things, that the use or disclosure involves no more than a minimal risk to the privacy of individuals participating in the research.

- Serious threats to health or safety of the public at large. Information may only be disclosed if the Covered Entity believes the use or disclosure (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat, including the target of the threat, or (2) necessary for law enforcement authorities to identify or apprehend an individual. This exception is limited by other applicable laws and standards of ethical conduct. Providers in California, for example, should be aware of privacy constraints imposed by the state constitution.

- Specialized government functions, such as the military, Secret Service, or national security activities and correctional facilities operations.

- Workers' compensation, to the extent required by state law.

2. Use and Disclosures for Treatment, Payment and Health Care Operations

Under the Privacy Standards, Covered Entities may use or disclose PHI for treatment, payment or health care operations without obtaining individual permission, unless state or other law requires it. At the same time, Covered Entities are permitted to use consents if they desire. The terms treatment, payment and health care operations have the following meanings under the Privacy Standards:

> Treatment: treatment means the provision, coordination, and management of health care and related services.
>
> Payment: payment includes activities undertaken for billing and collection of claims, determination of plan eligibility, utilization review, pre-certification, and medical necessity reviews.
>
> Health care operations: health care operations include general business and administrative functions, quality assessment and improvement activities, peer review, accreditation, licensing, internal auditing, and certain fundraising activities.

These provisions of the Standards allow a Covered Entity to release PHI to another health care provider for treatment and payment purposes of the recipient, without regard to that

provider's status as a Covered Entity under the Privacy Rule. Similarly, PHI may be released to a covered health plan, for the recipient's use for payment purposes.

Additionally, a Covered Entity is permitted to disclose PHI to another Covered Entity for certain healthcare operations purposes of the receiving entity, including, but not limited to, conducting quality assessment and improvement activities, carrying out population-based analyses related to improving health, and reviewing the competence of health care providers. However, these disclosures are allowed only to the extent that the entity receiving the PHI has or had a relationship with the individual who is the subject of the information which is requested. Where the relationship has ended, a disclosure about the individual is permitted only if it relates to the past relationship.

Notwithstanding the above, except in emergency situations, the Privacy Standards require providers with a direct treatment relationship[16] to make a **good faith effort** to obtain a patient's **written acknowledgement of receipt of the provider's Notice of Privacy Practices** at the time of first service delivery.[17] The acknowledgement does not have to take a specific form. It may be as simple as the patient's initials on a cover sheet to the provider's privacy notice or a signature on a list or form. The acknowledgement also may be electronic. Providers faced with patients who refuse to sign or to return the acknowledgment must document in the patient's record their efforts to obtain the acknowledgment and the reasons for failure. Other covered entities, such as health plans and indirect treatment providers[18], are not required to obtain this acknowledgement, but may do so if they choose.

C. Uses and Disclosures Pursuant to Appropriate Permission

For a Covered Entity to use or disclose PHI in any situation that was not covered in the previous discussions, the Covered Entity must obtain appropriate permission from the individual who is the subject of the information. The type of permission required varies with the circumstances. There are two kinds of permission under the Privacy Standards - **verbal agreement and written authorization**.

1. Verbal Agreements

Covered Entities may rely upon verbal agreements from an individual to use or disclose PHI, in certain limited circumstances. Verbal agreements permit an interventional pain practice to communicate with patient family members, close relatives, personal friends, or others who may be assisting in a patient's care. For instance, after providing an

---

[16] A patient's relationship with an interventional pain practice typically qualifies as a direct treatment relationship.

[17] A model acknowledgement is found with the model Notice of Privacy Practices at Exhibit 4.

[18] An indirect treatment relationship exists when a healthcare practitioner or entity provides services to an individual based on the orders of another provider, and the results are reported back to the ordering provider. Examples of indirect healthcare providers include pathologists, radiologists, and specialists who consult with a patient's treating physician. Another example is when an interventional pain physician is asked to review a film and advise another physician whether or not the patient could potentially benefit from an interventional pain procedure.

epidural lysis of adhesions, an interventional pain physician may give follow-up care instructions to the patient's family member who meets the physician in the waiting area after the procedure. This is permitted under HIPAA as long as the patient has given his or her verbal agreement.[19] Should a patient give an interventional pain practice verbal agreement to share PHI in these kinds of circumstances, it is good practice, but not required, to document this permission in the patient's chart or other appropriate record.

2. Written Authorizations

Where individual permission is required for a use or disclosure, but consents or verbal agreement are not deemed sufficient, an authorization must be used. Uses or disclosures for almost any purpose other than treatment, payment, health care operations, the public police purposes outlined above, or to persons assisting in an individual's care will typically require an authorization.

Examples:

- An individual is applying for disability insurance and the disability insurance company requests the insured's medical record to make the underwriting decision.
- An interventional pain practice wants to sell nerve block outcomes data that includes patient identifiable information to pharmaceutical manufacturers.

Because authorizations permit sharing of PHI outside of the normal health care system, they must be time limited and written with specificity. In contrast to consents, Covered Entities usually may not condition treatment upon the granting of an authorization.[20]

The Privacy Standards identify specific requirements that must be met in order for an individual authorization to be valid. Exhibit 2 is a model authorization form. The minimum requirements of an authorization are listed below:

- A meaningful description of the information that will be used or disclosed.
- The name or specific identification of the person(s), or class of person(s), the individual will be authorizing to make the requested use or disclosure.
- The name or specific identification of the person(s), or class of person(s), who will use the information or to whom the information will be disclosed.
- A description of each purpose of the requested use or disclosure.[21]

---

[19] Where a patient is not present or a patient's agreement cannot be obtained because of an emergency or the patient's incapacity, an interventional pain practice may disclose PHI to persons assisting in the patient's care even without the patient's agreement if it determines that such disclosures are in the best interests of the patient.

[20] A health care provider may condition treatment or payment upon the completion of an authorization in two circumstances: (1) treatment furnished in connection with clinical research and (2) treatment done solely for the purpose of creating health information that is going to be disclosed to a third party (such as an employer mandated physical).

- An expiration date or the occurrence of a particular event that will act as the expiration date.

- Statement(s) adequate to put an individual on notice of the individual's right to revoke the authorization, the exceptions to the right and a description of how to exercise that right[22] or, if this information is contained in a Covered Entity's Notice of Privacy Practices, a reference to its Notice.

- Statement(s) adequate to put an individual on notice of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by the Privacy Standards. For example, once a health care provider is authorized to share certain PHI with an employer in the context of an employer mandated physical, the employer has no obligation to protect the confidentiality of the data. Of course, the parties may agree to impose such a restriction.

- Statement(s) adequate to put an individual on notice of the ability or inability of the Covered Entity to condition treatment, payment, enrollment or eligibility for benefits on an authorization by stating either (A) that the Covered Entity may not condition them on the signing of an authorization when the prohibition on conditioning of authorizations found in the Privacy Standards applies, or (B) the consequences to the individual of a refusal to sign the authorization, when such conditioning is permitted.

- The signature of the individual and the date the authorization was signed.

- If an authorization is signed by an individual's personal representative, an explanation of the representative's authority must be included.

3. Marketing

In general, the Privacy Standards require authorization in order to use or disclose PHI for marketing activities.[23] Marketing, under the Privacy Standards, means (i) a communication about a product or service to encourage recipients to purchase or use the product or service or (2) an arrangement between a Covered Entity and a third party where PHI is shared with the third party, for direct or indirect compensation, so the third party may make marketing communications about its own products and services.

---

[21] A statement that the use or disclosure of PHI is made "at the request of the individual" is a sufficient description of purpose when an individual initiates an authorization and does not explain the purpose for the disclosure.

[22] For example, it is reasonable to require the revocation to be in writing and sent to a particular individual at the interventional pain practice.

[23] The rules governing marketing are similar to the rules that apply to uses and disclosures for fundraising solicitations. However, demographic information may be used without individual authorization for the purposes of raising funds to benefit the Covered Entity. Demographic information does not include any information related to the individual's diagnosis or the type of services they received. Individuals must be instructed on how they may
opt-out of future fundraising communications.

Although Covered Entities must obtain an authorization to use or disclose PHI for marketing purposes, there are numerous exceptions to the definition of marketing. Marketing does not include communications made to an individual:

> (1) to describe the entities participating in a health care provider network, or to describe health-related products or services provided by the covered provider;
> (2) for treatment of that individual; or
> (3) for case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

Since disease management, wellness programs, prescription refill reminders and appointment notifications fit within the exclusions above, these activities would not require individual authorization. In fact, authorization would not be required to use or disclose PHI to market any health-related product or service of the Covered Entity **when marketed directly by the Covered Entity**. However, authorization is required to use or disclose PHI to market the health-related product or service of a third party. Finally, other exceptions permit Covered Entities to engage in face-to-face marketing communications and to distribute promotional materials of nominal value, such calendars, pens, and mugs with logos, without having to obtain an authorization.

In those situations where authorization is required, the authorization must state clearly whether the Covered Entity will receive remuneration from a third party for its efforts.

IV. The Minimum Necessary Standard

The Privacy Standards require Covered Entities to make reasonable efforts to limit the use of, disclosure of, and requests for PHI, to the minimum amount of information necessary to accomplish the task. In other words, as a general matter, even after an interventional pain practice determines that it can use or disclose information, it must determine that its use or disclosure is the minimum necessary to meet the purpose of the use or disclosure. This is one of the most controversial portions of the Privacy Standards.

Although the minimum necessary requirement underlies virtually every aspect of the Privacy Standards, there are a number of exceptions. These include:

- disclosures to or requests by a health care provider made for treatment purposes. In these situations, the entire medical record may be transferred.
- disclosures to the individual who is the subject of the information (i.e., disclosures to the patient);
- uses or disclosures made pursuant to an authorization;
- uses or disclosures required for compliance with the HIPAA Standards Transactions (for various electronic communications);

- disclosures to the Department of Health and Human Services when disclosure is required for enforcement with the Privacy Standards; and

- uses or disclosures required by other laws.

Compliance with the **minimum necessary** standard requires each Covered Entity to identify persons or classes of persons in its workforce who need access to PHI to carry out their duties. The Covered Entity must then define the category or categories of information that those individuals need, and establish workable procedures to restrict the PHI use accordingly. This standard is not intended to override professional judgment nor to sacrifice the quality of health care.

Examples of changes that may be necessary, depending on the circumstances, might include: isolating or locking file cabinets and records rooms, adding additional password security on certain computers, maintaining working charts in opaque rather than see-through holders, ensuring at least one private room is available for patients to discuss clinical or financial issues with Covered Entity staff and requiring the use of curtains in areas where oral communication often occur between doctors and patients or among other professionals treating patients.[24]

In the case of routine and recurring disclosures of or requests for PHI, a Covered Entity may implement policies and procedures that ensure compliance with the minimum necessary standard without making a case-by-case determination. For example, a provider could decide that any information requested by an accreditation organization consistent with that organization's protocol is the minimum necessary disclosure and draft a policy and procedure to establish that position. Non-routine disclosures of or requests for PHI will require a case-by-case review before the PHI may be used or disclosed. This means that interventional pain practices will need to educate their staff on what is a "non-routine" use or disclosure (like a request from a disability insurance company about a possible claim) and then develop a process so that a decision can be made about the extent to which information may be shared.

While the minimum necessary requirement is a difficult standard to meet, the Privacy Standards do permit some flexibility. Specifically, the Standards permit incidental uses and disclosures of PHI that cannot reasonably be prevented, that are limited in nature, and that occur as a by-product of an otherwise permitted or required use or disclosure under the Privacy Standards, so long as reasonable safeguards are taken to minimize the chance of incidental disclosure to others. If voices are kept appropriately low, for example, this permits the types of oral communications that occur when health care providers coordinate services at hospital nursing stations, review test results with patients in semi-private rooms, or discuss patients during rounds, even if those communications are overheard by others. They also would allow Covered Entities to call out patient names in waiting rooms and to continue using sign-in sheets, bedside charts, and X-ray light boards that may be visible to passers-by.

---

[24] These actions may overlap, to some extent, with the administrative safeguards that are discussed in Section VI.

Model practice policies and procedures may be found at Exhibit 3. Some of these policies and procedures deal with minimum necessary issues.

V. Individual Rights

The Privacy Standards afford individual significant rights concerning their PHI. These rights impose significant new obligations on interventional pain practices.

A. Notice of Privacy Practices

In most cases, interventional pain practices will be required to provide notice of their intended uses and disclosures of PHI, the rights of individuals, and the legal duties of the practices under the Privacy Standards.[25] This notice is known as the **Notice of Privacy Practices**. We have attached a model notice at Exhibit 4.

The Privacy Standards require posting the Notice in a prominent and clear location. In addition, except in emergency situations, the Notice must be provided (on paper or electronically) to an individual no later than the first time an interventional pain practice furnishes services to the individual after the compliance deadline in April 2003. In emergency situations, a Covered Entity must provide its Notice as soon as reasonable practicable after the emergency is over.

A Covered Entity that maintains a web site containing information about the Covered Entity's services or benefits must post the Notice of Privacy Practices prominently on the web site. The easiest mechanism to accomplish this may be for the patient registration or service order process to contain a screen posting the Notice and requiring an acknowledgment. Even when the Notice is furnished in an electronic format, however, individuals must be able to request that a paper copy be sent to them.

The Privacy Standards identify specific requirements that must be included in the Notice. These are listed below.

- The Notice must be written in "plain English."
- The following language must be prominently displayed: 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.

[25] As explained above, an organized health care arrangement and affiliated covered entity may elect to use a Notice of Privacy Practices that applies to all of the entities that are part of the organization or affiliated entity. This means that one comprehensive document may be used for all the entities. This also means that the Notice only needs to be distributed the first time the patient visits any of one of the entities.

- The Notice must include a description and at least one example of the types of uses and disclosures that the Covered Entity is permitted to make for treatment, payment, and health care operations .[26]

- A general description of other permitted or required uses and disclosures without the need for a written authorization also must be included.[27]

- If a use or disclosure otherwise permitted by HIPAA is limited by a stricter law, the Notice must reflect the stricter law.

- Certain uses or disclosures require separate explanatory statements. With respect to the typical interventional pain practice, these uses would likely include contacting the individual to provide appointment reminders.

- The Covered Entity must state that all other uses and disclosures will be made only with the individual's written authorization, which may be revoked, except to the extent that action was taken in reliance upon the authorization.

- The Notice must explain the Covered Entity's duties under the Privacy Standards, such as maintaining the privacy of PHI.

- If the Covered Entity wants to reserve the right to revise its Notice and apply changes in its policies and procedures to information created or received prior to issuing a revised Notice, the Notice must include a statement to this effect.

- The Notice must contain a statement of the individual rights permitted under the Privacy Standards and how an individual may exercise these rights.

- The Covered Entity must state that the Covered Entity is required to follow the terms of its Notice.

- The Notice must inform individuals how they may file a complaint with both the Secretary of the Department of Health and Human Services and the interventional pain practice if the individual believes his or her rights under the Privacy Standards have been violated. The Covered Entity must provide the name and telephone number of a person who may be contacted for more information about the Privacy Standards and their application to the Covered Entity. In addition, the Notice must contain a statement notifying the individual that the Covered Entity will not retaliate against the individual for filing a complaint.

---

[26] Treatment, payment, and health care operations each require a separate example. If the interventional pain practice agrees to limit the use or disclosure of certain information, this should be noted, as well.

[27] 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.

- The Notice must contain an effective date.

Interventional pain practices must document compliance with the Notice requirements by retaining copies of all notices issued by the practice for six (6) years from the date the Notice was last in effect. Since the operations of every health care provider are different, this document will need to be carefully tailored. Because Covered Entities must update and republish their Notice of Privacy Practices whenever they make material changes in their privacy policies, it is important that interventional pain practices take care to draft the Notice as correctly as possible the first time.

B. Access and Review of Medical Records

The Privacy Standards permit individuals the right to access and obtain a copy of their own PHI. Covered Entities must provide access to on-site records within thirty (30) days of a request, but have sixty (60) days to produce records stored off-site, unless the Covered Entity takes advantage of certain provisions n the Privacy Standards which allow the Covered Entity an additional thirty (30) days to act. This right of access includes information held by Business Associates. A Covered Entity may charge a reasonable copying fee for information provided to an individual. A copy charge at cost may be assessed by the practice, but the patient may not be charged a search fee.

Individuals are not entitled to access all PHI, only information held in "**designated record sets**." A designated record set is defined as a group of records maintained by a Covered Entity that are (1) medical or billing records about individuals maintained by or for a health care provider, (2) enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plan, or (3) records used, in whole or in part, by the Covered Entity to make decisions about individuals. By "record," the Privacy Standards mean any item, collection, or grouping that includes PHI that is maintained, collected, used, or disseminated by the Covered Entity.

A Covered Entity may deny an individual access to his or her PHI under certain circumstances. The denial must be in writing and, in certain circumstances, may be appealed by the individual for a review determination by the practice. Examples of circumstances in which access may be denied include (1) information compiled in reasonable anticipation of or use in civil criminal, or administrative proceedings, (2) information subject to, or exempt from, CLIA, (3) when, in the professional judgment of a health care provider, the information may endanger the life of the individual or another person, or (4) information makes reference to another person and, in the professional judgment health care provider, access would cause harm to such other person. The Privacy Standards also contain certain access exceptions in the context of correctional institutions, certain research programs, and other federal privacy protections.

C. Amending Medical Records

The Privacy Standards permit individuals to request that their medical records be amended. The Covered Entity and any Business Associate must honor any such request unless:

- the information was not created by the health care provider,
- the information was not part of a designated record set,
- the information is accurate and complete; or
- the individual does not have a right of access to the information because one of the exceptions to that right applies (and which are described immediately above in Section B).

A Covered Entity must act on an amendment request within sixty (60) days, unless the Covered Entity takes advantage of certain provisions in the Privacy Standards which allow the Covered Entity an additional thirty (30) days to act. Requests to amend PHI must be formally accepted or denied. If asked to do so, a Covered Entity denying an amendment request must add a statement to the record contesting the denial.

D. Use and Disclosure Accountings

The Privacy Standards also require Covered Entities to provide individuals with an accounting of disclosures of their PHI. There are some significant exceptions to this right. Covered Entities do not have to account for disclosures made for purposes of treatment, payment, or health care operations, to persons assisting in an individual's care, or those made pursuant to an authorization, among others.

Once the Privacy Standards have been in effect long enough, this accounting will have to detail releases for the prior six years or dating back to the compliance deadline date of April 14, 2003, if that is less than six (6) years.[28] Individuals have a right to receive one free accounting every twelve (12) months. An interventional pain practice may charge a reasonable fee for any accountings performed on a more frequent basis.

Although patients may request accountings infrequently, this individual right will require Covered Entities to develop new systems to track disclosure of PHI. At a minimum, this will require an interventional pain practice to note in its record (whether electronic or paper) what information was disclosed, when it was disclosed, and to whom. In addition, it must contain a brief statement of the purpose of the disclosure or, in lieu of such a statement, a copy of the authorization or written request for disclosure.

E. Accommodation Issues

Health care providers must accommodate an individual's reasonable requests to receive communications of PHI by alternative means or at alternative locations. For example, an individual may not wish to receive a postcard appointment reminder or may wish that laboratory results be communicated to him at work, not at home. To capture and track these limitations, Covered Entities also must entertain requests by an individual to limit

[28] Disclosures made regarding national security, intelligence, or certain law enforcement officials may be omitted from an accounting if inclusion would be reasonably likely to impede the officials' activities.

the uses and disclosures a Covered Entity is permitted to make for treatment, payment, health care operations, and to persons assisting in an individual's care, and disclosures for disaster relief purposes. Covered Entities are not required to agree to these special restrictions. But, if a Covered Entity does agree, then it is bound by them. Because of the existing complexity of the Privacy Standards, many providers will not be willing to accept any additional, voluntary restrictions.

VI. Administrative Requirements

To supplement the protections of the Privacy Standards, the regulations obligate Covered Entities to implement privacy compliance programs. While the regulations identify particular items that must be part of the administrative privacy program, the Privacy Standards contain few specifics about how they should be implemented. Instead, the Department of Health and Human Services has indicated that these administrative requirements are intended to be flexible and "scalable" to the capabilities of the particular Covered Entity.

The particular administrative requirements under the Privacy Standards are:

- Designation of a privacy officer to oversee the privacy compliance program and to accept complaints. There is no reason why this responsibility could not be assigned to the interventional pain practice's existing general compliance officer, if it has one.

- Develop up-to-date policies and procedures to ensure compliance with the Privacy Standards.

- Refrain from requiring individuals to waive their privacy rights to obtain treatment.

- Operate a privacy training program for existing and new workforce members.

- Implement reasonable administrative, technical, and physical safeguards to protect PHI from intentional or unintentional use or disclosure in violation of the Privacy Standards.

- Implement reasonable safeguards to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure as discussed in Section IV above.

- Apply appropriate sanctions against workforce members who fail to comply with privacy policies and procedures.

- Establish a privacy complaint procedure.

- Mitigate, to the extent practicable, any harm that results from a violation of privacy policies and procedures.

- Refrain from retaliatory acts against individuals who exercise their privacy rights.

- We have included a Model Compliance Plan at Exhibit 3.

VII. Relationship to State Laws

The Privacy Standards set a minimum floor of federal privacy protection for PHI and are not intended to supercede other applicable laws that provide greater privacy protections. As a general rule, any state law - whether it is a constitutional provision, statute, regulation, rule or common law - that is contrary to the requirements of the Privacy Standards is preempted, unless it relates to the privacy of individually identifiable health information and is more stringent (i.e., it provides patients more protections than the federal Privacy Standards) in which case the state provision must be followed. Other state laws are not preempted if the Secretary of Health and Human Services makes a determination that a state law is necessary to prevent fraud and abuse, to ensure state regulation of insurance, for state reporting on health care delivery costs, or for the purpose of serving a compelling need related to public health, safety or welfare.

VIII. Enforcement

Responsibility for enforcement of the Privacy Standards lies with the Office of Civil Rights ("OCR") at the Department of Health and Human Services. Any person, not just the person who is the subject of the allegedly mishandled PHI, may file a timely complaint with OCR. The preamble to the Privacy Standards suggests that one of OCR's primary functions will be to achieve voluntary compliance by providing technical assistance and responding to questions. Providers should periodically monitor the OCR web site for additional updates. The web site address is www.hhs.gov/ocr/hipaa. Where voluntary compliance cannot be achieved, OCR may seek civil money penalties and make referrals for criminal prosecution. According to the statute itself, violations are punishable by fines up to $250,000 and up to ten years imprisonment. In the future, the Department of Health and Human Services intends to issue a single Enforcement Rule applicable to all of the HIPAA Administrative Simplification provisions.

Glossary

Affiliated covered entities - legally separate Covered Entities that elect to designate themselves as a single Covered Entity for purposes of the Privacy Standards and that are under common ownership or common control

Authorization – a type of written permission that a Covered Entity must secure from an individual in certain circumstances to use and disclose the individual's PHI

Business Associate - an entity, that is not a member of the Covered Entity's workforce, that (1) performs a function involving PHI on behalf of a Covered Entity, or (2) provides specified services to a Covered Entity, such as legal, actuarial, accounting, consulting, data aggregation, management, accreditation, or financial services, which involve the disclosure of PHI

Business Associate Agreement - a written agreement between a Covered Entity and a Business Associate that contains satisfactory assurances from the Business Associate about how the Business Associate will use and disclose PHI from the Covered Entity

De-identified information – (1) health information from which specified individual identifiers have been removed or (2) health information from which all identifiers have not been removed but with respect to which a person with sufficient statistical and scientific knowledge has determined the risk of individual identification is small

Health care clearinghouse - public or private entities that convert health information from nonstandard formats into HIPAA standard formats, or *vice versa*

Health care operations - includes general business and administrative functions, quality assessment and improvement activities, peer review, training, accreditation, licensing, internal auditing, and certain fundraising activities

Health plan - individual or group plans that provide or pay for the cost of medical care

HIPAA Standard Transactions – activities covered by new federal Standards for Electronic Transactions, including health care claims, health care payments and remittance advices, coordination of benefits, health care claims status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, and health claims attachments

Notice of Privacy Practices - a written statement of a Covered Entity's intended uses and disclosures of PHI, the rights of individuals, and the legal duties of the Covered Entity under the Privacy Standards

Office of Civil Rights - the office at the U.S. Department of Health and Human Services responsible for enforcing the Privacy Standards

Organized health care arrangement - (1) clinically integrated care setting in which individuals typically receive care from more than one health care provider or (2) an organized system of health care in which more than one Covered Entity participates, the entities hold themselves out to the public as participating in a joint arrangement, and the entities jointly participate in utilization review, quality assessment and improvement, or payment activities

Payment - includes activities undertaken for billing and collection of claims, determination of plan eligibility, utilization review, pre-certification, and medical necessity reviews

Privacy Standards – the federal regulations governing the use and disclosure of individually identifiable health information

Protected Health Information (PHI) –individually identifiable information that relates to the health of an individual or the provision of health care to an individual

Standards for Electronic Transactions – the federal regulations standardizing the format and code sets for certain "standard transactions" conducted in an electronic form

Treatment - the provision, coordination, and management of health care and related services

Verbal agreement - verbal or implied permission from an individual permitting a Covered Entity to use the individual's PHI for the purposes a of using or disclosing for facility directory, and to persons assisting in a patient's care