Implementing the Federal Health Privacy Rule in California:

A Guide for Health Care Providers

Prepared for:

California HealthCare Foundation

Prepared by:

Health Privacy Project

Author:

Joy Pritts, J.D.

ihealthreports

February 2002

Acknowledgments

Health Privacy Project is a part of the Institute for Health Care Research and Policy at Georgetown University. The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. Additional background information on health privacy can be obtained by visiting **www.healthprivacy.org**.

The author would like to acknowledge the participation of a group of individuals whose expertise, industriousness, and guidance were essential to this report: Janlori Goldman, Director, Health Privacy Project; Sam Karp and Claudia Page, California HealthCare Foundation; and Scott Sanders, High Noon Communications. A special thank you also goes to the following professionals for taking time out of their busy schedules to review this guide; their input was invaluable: Catherine I. Hanson, Vice President and General Counsel, California Medical Association; Steven M. Fleisher, Vice President and General Counsel, MEDePass, Inc.; and Regina M. Boyle, J.D., Director of Legal Services, California Primary Care Association.

The **California HealthCare Foundation** (CHCF) is an independent philanthropy committed to improving California's health care delivery and financing systems. Our goal is to ensure that all Californians have access to affordable, quality health care. CHCF's work focuses on informing health policy decisions, advancing efficient business practices, improving the quality and efficiency of care delivery, and promoting informed health care and coverage decisions.

The iHealth Reports series focuses on emerging technology trends and applications and related policy and regulatory developments.

Additional copies of this report and other publications in the iHealth Report series can be obtained by calling the California HealthCare Foundation's publications line at 1-888-430-CHCF (2423) or visiting us online at **www.chcf.org**.

ISBN 1-929008-82-1

Contents

Overview

This guide is intended for those health care providers who are subject to two of the major health privacy statutes in California: the California Confidentiality of Medical Information Act[1] and the Patient Access to Medical Records Act.[2] These providers include the following licensed health care professionals and facilities:

- Physicians
- Osteopaths
- Surgeons
- Podiatrists
- Dentists
- Optometrists
- Psychologists
- Chiropractors
- Marriage, family, and child counselors
- Clinical social workers
- Hospitals
- Community clinics
- Outpatient clinics
- Home health agencies
- Others[3]

Pharmacists, acupuncturists, and other providers who are not subject to the Patient Access to Medical Records Act should consult *Implementing the Federal Health Privacy Rule in California: A Guide for Pharmacists*, a CHCF publication specifically designed for their needs.

Purpose

This guide is designed to help California health care providers to comply with the new Federal Health Privacy Rule, which was issued by the U.S. Department of Health and Human Services in December 2000. The guide is specific to holders of health information in California, which has its own state health privacy laws.

The guide is meant to serve as a general road map for implementing the Privacy Rule and will help providers begin the process of determining what steps they will need to take to come into compliance with the Privacy Rule in April 2003.

The guide, however, is not a step-by-step manual for bringing a health care practice or organization into compliance. It provides a thorough understanding of what will and will not be required under the Privacy Rule and will help individuals and organizations begin to think about how to best integrate those requirements into existing practices. As implementation draws near, it will be important to consult other resources, as appropriate, to ensure full compliance.

Specifically, the guide:

- Provides background on the value of health information and health privacy;
- Explains the Privacy Rule—how it came into being, who and what it covers, and its general framework;
- Discusses, in general, the preemption provisions of the Privacy Rule and explains the resulting relationship between the federal rule and California health privacy laws; and
- Analyzes how health care providers such as doctors, dentists, hospitals, and outpatient clinics will be required to implement the Privacy Rule and the rights it provides to patients to access and amend their health information in light of existing California law.

I. Background

The Value of Health Information

Health care providers are naturally aware of the value of health information. Its primary value is the key role it plays in the provision of high-quality care to the patient. Without information about a patient's condition, providers cannot offer adequate care, nor can payers cover the cost of that care.

Some other uses of health information also benefit patients and the larger community, while others primarily benefit the holder of the information. Some of the latter uses include:

- Managing disease;
- Ensuring quality and accountability;
- Investigating fraud and abuse;
- Monitoring public health;
- Insuring adequate government oversight; and
- Expanding commercial activities.

Why Health Privacy Matters

Given the numerous uses of health information and the number of people who have access to health information in today's complex health care system, many patients have concerns about the privacy of their own identifiable health information. Patients fear that their employers, family members, or friends may discover that they have a sensitive health condition that could negatively impact their job security, relationships, or personal safety. Among those with heightened concerns are adolescents, immigrants, mental health patients, people with HIV/AIDS, and victims of domestic violence. These concerns are magnified by the increased use of technology by health care organizations. While computerized records and use of the Internet can provide greater protections for information, they also open the door for broader access if confidentiality and security are breached. In fact, the media reports regularly on health privacy and security violations.

Many patients have developed a variety of "privacy-protective" behaviors to shield themselves from what they consider to be harmful and intrusive uses of their health information. A poll conducted for the California HealthCare Foundation in January 1999 found that:

- One in five American adults believes that a health care provider, insurance plan, government agency, or employer has improperly disclosed personal medical information. Half of these people say it resulted in personal embarrassment or harm.
- One in six American adults says he or she has done something out of the ordinary to keep personal medical information confidential. Among the actions reported are: going to another doctor; paying out-of-pocket for services; not seeking care; giving inaccurate or incomplete information on a medical history; and asking a doctor not to write down the health problem or record a less serious or embarrassing condition.
- Only a third of U.S. adults say they trust health plans and government programs like Medicare to maintain confidentiality all or most of the time.

Protecting Health Privacy

As a result of these fears and their negative impact on the quality of health care, many states—including California—and the Federal government have enacted protections for health information. These laws vary considerably as to the entities and types of specific information they cover and the strength of the protections that they provide.

II. The Federal Health Privacy Rule

In the broadest terms, the Privacy Rule does two things: (1) it imposes new restrictions on how covered entities can use and share health information; and (2) it creates new rights for individuals concerning their own health information.

Privacy Rule Updates

To receive email notification on changes to the Privacy Rule and other health privacy news sign on to the Health Privacy Project's listserv at: http://www.healthprivacy.org.

Introduction

In the last few years, health privacy has emerged as a prominent health care policy issue at the federal level. Although Congress has recognized the importance of protecting the confidentiality of health information, it has been unable to pass any comprehensive health privacy legislation. Congress did, however, give limited authority to the U.S. Department of Health and Human Services to issue regulations protecting the privacy of health information. Understanding the genesis of the Federal Health Privacy Rule is important for understanding the scope of the federal rule and how it operates.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes a major initiative intended to cut administrative health care costs by standardizing health care transactions. The provision, known as "Administrative Simplification," is aimed at facilitating the exchange, storage, and analysis of health information in uniform format across entities.

Prior to HIPAA's passage, this move towards standardization raised serious privacy concerns. To reconcile these competing priorities of safeguarding privacy and easing the flow of health data, Congress included in HIPAA a requirement that if it failed to pass comprehensive health privacy legislation by August 1999, the Secretary of the United States Department of Health and Human Services (HHS) would issue regulations. Despite the introduction of numerous proposals, Congress failed to meet its deadline, and the duty passed to HHS to promulgate health privacy regulations.

As required under HIPAA, the Secretary of HHS issued final health privacy regulations in December 2000[4] (see Timeline next page). After a short delay, the final regulation, known as the "Privacy Rule," became effective April 14, 2001. The Privacy Rule has the force of law. Compliance with the Privacy Rule is generally required by April 2003.

Although the Privacy Rule is "final," that does not mean that it will not be changed. HHS has made it clear that it intends to engage in additional rule-making to substantively change the rule in the near future.[5]

Timeline

November 3, 1999
Draft rule published in the *Federal Register*.

February 17, 2000
Public comment period closes. The Department of Health and Human Services received more than 52,000 comments on the draft.

December 28, 2000
The final privacy rule is published in the *Federal Register*.

April 14, 2001
The rule becomes *effective*, but covered entities do not yet have to comply with it.

July 6, 2001
HHS releases guidance, interpreting the final rule.

April 14, 2003
Covered health care providers and most health plans must be in compliance with the rule.

April 14, 2004
Small health plans must be in compliance.

Who Is Covered?

The Privacy Rule does not apply to everyone who receives or maintains health information. Congress authorized HHS to issue regulations only with respect to three specified types of entities that transfer or maintain health information. The Privacy Rule, therefore, directly applies only to:

- Health plans;
- Health care clearinghouses; and
- Health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions (such as claims for payment).[6]

These persons and organizations are referred to as "covered entities."[7] Any person or organization that provides or pays for health care should review these provisions carefully to determine whether or not they are covered by the Privacy Rule.

Health Plans

The definition of "health plan" is quite broad and generally includes any individual or group plan that provides or pays for medical care.[8] The term encompasses both private and governmental plans. It includes health insurance issuers and HMOs. High-risk pools are specifically covered, as are Medicaid and Medicare plans. Additionally, most employee health benefit plans are covered.

The Privacy Rule specifically *excludes* certain entities that provide or pay for health care. For example, small employee health benefit plans (fewer than 50 participants) that are self-administered are exempt. Likewise, workers' compensation carriers are excluded from the definition of health plan. Furthermore, government-funded programs that only incidentally provide or pay for the cost of health care are not health plans.[9]

Health Care Clearinghouses

"Health care clearinghouse" is a term of art under the Privacy Rule, and differs somewhat from the manner in which the term is generally used. Under the Privacy Rule, a health care clearinghouse is an entity that translates health information received from other entities either into or from the standard format that will be required for electronic transactions under HIPAA.[10] For instance, many health providers use the services of a health care clearinghouse to process their claims information into a standard format for submission to a health plan.

Health Care Providers Who Electronically Transmit Health Information

The Privacy Rule covers health care providers who transmit health information in electronic form in connection with HIPAA standard transactions.[11] A health care professional or facility must meet all three of the following criteria to be covered by HIPAA.

Health care provider. For purposes of the regulation, "health care provider" includes any person or entity that furnishes, bills, or is paid for health care in the normal course of business.[12] "Health care," in turn, is broadly defined as "care, services, or supplies related to the health of an individual."[13] Thus, the term health care provider includes both persons (such as dentists and podiatrists) and entities (such as hospitals and clinics). It includes mainstream practitioners (such as physicians, nurses, and psychotherapists), as well as providers of alternative care (such as homeopaths and acupuncturists). The Privacy Rule also covers both the providers of care and services (such as practitioners) and the providers of health supplies requiring a prescription (such as pharmacists and hearing aid dispensers). However, the Privacy Rule is not intended to encompass blood banks, sperm banks, organ banks, or similar organizations.[14]

Transmitting health information electronically.[15] To "transmit health information in electronic form," a provider must transfer personally identifiable health information via computer-based technology. Using the Internet, an Intranet, or private network system will bring a provider within the reach of the Privacy Rule. Similarly, information transferred from one location to another using magnetic tape or disk is covered by the Privacy Rule. In contrast, sending information via fax is not considered to be transmitting information electronically.

Standard transactions.[16] To come within the scope of the Privacy Rule, the health information must be transmitted in standard format in connection with one of the financial and administrative transactions listed in Section 1173 of HIPAA. These transactions include, but are not limited to, health claims, determining enrollment and eligibility in a health plan, and referral authorization.[17] Providers who submit health claims electronically will be required to transmit them in standard format by October 2003 at the latest.[18] In addition to covering those providers who directly engage in such transactions, the Privacy Rule also covers those who rely on third-party billing services to conduct such transactions on their behalf.[19] In contrast, providers who operate solely on an out-of-pocket basis and do not submit insurance claims probably will not be subject to the rule. For instance, an Internet pharmacy that only accepts credit card payments will not be covered by the Privacy Rule. If this Internet pharmacy also accepts insurance payments, however, then it may be covered by the rule.

What is Covered?

Generally, the Privacy Rule covers "protected health information" in any form that is created or received by a covered entity.[20] There are a number of elements that must be satisfied before health information is protected by the Privacy Rule. First, it must be "health information" as defined in the rule. Second, the health information must be individually identifiable. Finally, it must be created or received by a covered entity.[21]

Health Information

"Health information" is broadly defined as meaning any oral or recorded information relating to the past, present, or future physical or mental health of an individual, the provision of health care to the individual, or the payment for health care.[22] This definition is broad enough to encompass not only the traditional medical record but also physicians' personal notes and billing information.

Individually Identifiable Information

"Individually identifiable health information" is health information that identifies or reasonably can be used to identify the individual.[23] Health information that has been "de-identified" is not covered. A covered entity may de-identify health information by removing specific identifiers (including, but not limited to, name, social security number, medical record number, and address). Alternatively, a covered entity may treat information as de-identified if a qualified statistician, using accepted principles, determines that the risk that the individual could be identified is very small.[24]

Created or Received by a Covered Entity

Health information that is "created or received by a covered entity" is protected under the rule.[25] Any health information that a patient would divulge to his or her doctor would be covered. In contrast, health information that is created or received by others is not covered. For example, if an individual fills out a health assessment survey as part of donating blood to the Red Cross, that information would not be protected because the Red Cross is not a covered entity.

If health information meets these criteria, it is considered "protected health information" and is covered by the rule regardless of the media or form in which it is maintained or transmitted. This means that oral, written, and electronic information is protected health information.[26]

Because this guide focuses on implementing the Privacy Rule, the term "health information" as used in this guide refers only to "protected health information," i.e., individually identifiable health information created or received by a covered entity.

Requirements

In the broadest of terms, the Privacy Rule does two things: (1) it imposes new restrictions on how covered entities can use and share health information; and (2) it creates new rights for individuals concerning their own health information. A general overview of the requirements of the Privacy Rule follows. The specific implementation requirements will vary depending on existing California law and are discussed in the fourth section of this guide.

General Restrictions on Use and Disclosure

The Privacy Rule governs the "use" and "disclosure" of protected health information by covered entities. These two terms have specific meanings within the context of the Privacy Rule.[27]

Use. Protected health information is *used* when it is shared, examined, applied, or analyzed within a covered entity that receives or maintains the information.

Disclosure. Protected health information is *disclosed* when it is released, transferred, allowed to be accessed, or otherwise divulged outside the entity holding the information.

In general, the Privacy Rule prohibits covered entities from using or sharing protected health information without the individual's permission. The Privacy Rule then lists a number of exceptions where use and disclosure are permitted without the individual's written permission. When disclosure is permitted without the patient's permission, the Privacy Rule generally imposes conditions specific to the purpose for which the health information is being released. In order to use or disclose health information for a purpose that is not specified in the rule, the covered entity must first obtain a patient's written permission.

Key Restrictions on Use and Disclosure

Some of the major restrictions on using and disclosing health information include:

Consent

- Health care providers who provide direct treatment to patients must obtain an individual's written permission, a "consent," prior to using or disclosing health information for treatment, payment, or health care operations purposes.[28]
- Health plans are not required to obtain such a consent.

Consent forms generally advise patients that their health information may be used for treatment, payment, and health care operations purposes and inform them of their general rights with respect to this information. Consents do not contain specific details of the covered entities' use and disclosure of health information, but refer patients to the covered entities' notice of privacy practices for this information. (See "Patients' Rights," below.)

Authorization

- If the intended purpose of obtaining or using health information is not specifically permitted in the Privacy Rule, any covered entity must obtain an individual's signed written permission, an "authorization," prior to using or disclosing the health information.
- An authorization is generally used for purposes other than treatment, payment, or health care operations. Authorization forms are specifically required for many uses, such as disclosures of psychotherapy notes.
- In contrast to a consent, an authorization is a detailed form containing specifics about: (1) with whom information is being shared; (2) how it is to be used and disclosed; and (3) the length of time it is effective. These forms must be tailored to fit the particular purpose for which the health information is to be used or disclosed.

Minimum Necessary

- For most uses and disclosures, a covered entity is required to develop policies and practices reasonably assuring that the minimum amount of health information necessary is used or shared.
- This standard does not apply to requests by or disclosures to health care providers for treatment purposes.

Business Associates

In order to disclose protected health information to a third party who assists them with their business functions (business associates), covered entities are required to have contracts ensuring that the business associate will adequately safeguard the information.

Affording Patient Rights

The Privacy Rule also grants individuals a number of rights over their health information. The main rights include: (1) the right to receive a notice of information practices; (2) the right to see and copy their own health information; (3) the right to amend their health information, if it is inaccurate; and (4) the right to an accounting of disclosures.

Covered entities have the duty to ensure that individuals are able to exercise these rights with respect to protected health information that they maintain.

Administrative Requirements

The Privacy Rule requires covered entities to implement a number of administrative practices in order to ensure compliance. Among other things, covered entities are required to:

- Develop written privacy policies and procedures with respect to who has access to health information within an organization, how it will be used, and when the information may be disclosed;
- Put into place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information;
- Train personnel about the Privacy Rule;
- Designate a privacy officer, who will be in charge of implementing the Privacy Rule;
- Designate a contact person, whom people can contact with questions about privacy; and
- Maintain documentation of consents, authorizations, procedures and policies, training, and other activities undertaken in compliance with the Privacy Rule.

Compliance

Health care providers, health care clearinghouses, and most health plans that are covered by the Privacy Rule must comply with the new requirements by April 2003.[29] Small health plans (those with annual receipts of $5 million or less) have an additional 12 months to come into compliance[30] (see Timeline). It should be noted that these deadlines might change if HHS substantively alters the Privacy Rule through official rule-making procedures.[31]

The HHS Office for Civil Rights (OCR) is in charge of ensuring compliance with and enforcing the Privacy Rule.[32] In performing these functions, OCR's general philosophy is to provide a cooperative approach towards compliance, including use of technical assistance and informal means to resolve disputes.[33]

On July 6, 2001, OCR issued its first set of guidance to answer many common questions about the new Privacy Rule and to clarify some of the confusion regarding the Privacy Rule's potential impact on health care delivery and access.[34] Within its limited resources, OCR intends to continue to provide technical assistance to help covered entities implement the Privacy Rule.[35] The initial guidance and other information about the new rule are available on the Web at **http://www.hhs.gov/ocr/hipaa.**

Covered entities are not required to obtain prior approval from HHS for their compliance activities (such as developing privacy policies). Neither are they currently required to submit compliance reports, although this may change in the future.[36] Rather, compliance issues will come to the OCR's attention primarily through two different means:

- ***Complaints.*** Anyone who believes that a covered entity is in violation of the Privacy Rule may file a complaint with OCR.[37]
- ***Compliance reviews.*** OCR has the authority to conduct compliance reviews to determine whether covered entities are complying with the requirements of the Privacy Rule.[38]

The rule requires covered entities to cooperate with any resulting investigations.[39] In these proceedings, covered entities are required to document that they have undertaken the necessary steps to achieve compliance (e.g., establishing a privacy policy).[40] They are also required to provide access to such protected health information and other relevant information as necessary for compliance and investigation purposes.[41]

Remedies and Penalties

HIPAA establishes civil and criminal penalties for violations of the Privacy Rule. There is a $100 civil penalty up to a maximum of $25,000 per year for each standard violated.[42] For knowing, wrongful disclosures of health information, a criminal penalty may be imposed.[43] It is a graduated penalty that may escalate to a maximum of $250,000 for particularly egregious offenses.

HIPAA does not give individuals a federal right to sue for violations of the Act. Because the Privacy Rule creates a new "duty of care" with respect to health information, it is possible, however, that violations may be the grounds for state tort actions.

The Privacy Rule does not contain any provisions specifically addressing penalties. Rather, HHS plans at a future date to issue an Enforcement Rule governing penalties that will apply to all of the regulations issued under the Administrative Simplification provisions of HIPAA, including the Privacy Rule.[44]

III. The Interaction of the Federal Health Privacy Rule and California Privacy Laws

In a state like California, where there are strong, detailed health privacy standards in place, there effectively will be dual tracks of regulation, one state and one federal, whose requirements often intertwine.

State Reporting Laws

Q: Will the Federal Privacy Rule interfere with state reporting laws?

A: No. HIPAA expressly excludes from federal preemption state laws that provide for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health investigations.

See 45 C.F.R. § 160.203(d).

Introduction

The Federal Privacy Rule was not issued in a vacuum. Privacy protective laws already exist in many states. California, in particular, has been in the forefront of enacting laws that protect the privacy of health information.

The Federal Privacy Rule essentially sets a national "floor" of privacy standards that protect the health information of all Americans. It preempts or overrides state laws that are contrary to the Federal Privacy Rule and that are less protective.

State laws that are not contrary to the Federal Privacy Rule remain effective. A state law is "contrary to" the Federal Privacy Rule when:

- A covered entity would find it impossible to comply with both the state and federal requirements; or
- The provision of state law stands as an obstacle to the accomplishment and execution of the Federal Privacy Rule.[45]

Even if a state law is contrary to the Federal Privacy Rule, it will not be preempted if it is "more stringent." Generally, a state law is considered to be more stringent if:

- It is more restrictive than the Federal Privacy Rule with respect to a use or disclosure;
- It provides greater rights of access or amendment with respect to individuals' access to their own health information.[46]

In a state like California, where there are strong, detailed health privacy standards in place, there effectively will be dual tracks of regulation, one state and one federal, whose requirements often intertwine.

Complying with Both State and Federal Laws

A health care provider should first determine whether it is covered by the Federal Privacy Rule. It should then determine which health privacy laws it must already comply with under California law. Some of the major California health privacy statutes that may apply to a health care provider include:

- Confidentiality of Medical Information Act;[47]
- Patient Access to Medical Records Act; [48] and
- The Medi-Cal statute and regulations.[49]

Additionally, there are a number of state statutes that protect the privacy of health information associated with information gained through the treatment of certain medical conditions, including, but not limited to, the following:

- Mental health;[50]
- HIV/AIDS tests;[51] and
- Alcohol and drug dependency.[52]

Once health care providers have identified all the state laws that are particularly applicable to them, they will need to compare the provisions of the state laws to the requirements of the Federal Privacy Rule on an item-by-item basis. The following sections of this guide will discuss many of the provisions of the Federal Privacy Rule, California state laws, and how they interact.

Enforcing California Law

Q: Who will enforce the California health privacy laws after implementation of the Federal Privacy Rule?

A: California health privacy laws will continue to be enforced at the state level. Violation of a California law may result in the imposition of civil and/or criminal penalties by a California court, licensing body or regulating agency.

Q: Will patients have the right to sue?

A: Yes, in many cases. Many California health privacy statutes (e.g., Confidentiality of Medical Information Act) give patients the right to sue if their health information is improperly disclosed or if they are improperly denied access to their health information. Patients generally will retain these rights to sue for violations of their privacy rights under California law after implementation of the Federal Privacy Rule.

The Federal Privacy Rule has many standards that are similar to those in California privacy laws. When the standards are comparable, plans and providers should follow the "more stringent" standard. For example, the Federal Privacy Rule gives covered entities 30 days to respond to an individual's request to inspect his or her own health information, while California law requires a response within 5 business days. To comply with both laws, follow the strictest standard—in this case, provide access within 5 business days.

When the state and federal standards are not comparable, it will be necessary to determine if the state law is contrary to the Federal Privacy Rule and, if so, if it is more stringent. Making this determination will not always be a straightforward process. Using this guide should make it somewhat easier.

The purpose of this guide is to provide a general road map to the combined state and federal requirements that health care plans and health care providers will have to comply with upon implementation of the Federal Privacy Rule. From the state perspective, this guide focuses on the Confidentiality of Medical Information and the Patient Access to Medical Records Act. This guide does not identify or address all of the state health privacy laws that may be applicable to any given covered entity—it only highlights some of the major relevant state privacy laws.

The guide also only addresses *some* of the major changes in practice that the Federal Privacy Rule will require. The Federal Privacy Rule is lengthy and detailed, and careful reading of the entire rule will be necessary to ensure complete compliance.

IV. The California Medical Information Act and the Patient Access to Medical Records Act

Doctors, pharmacists, hospitals, clinics, counselors, physical therapists, and countless others… are subject to the same set of requirements under the Privacy Rule. In contrast, California law does not apply uniformly to all of these different providers.

Background

The Federal Privacy Rule applies to "health care providers" who engage in certain electronic transactions. The term "health care provider" is broadly defined in the Privacy Rule and encompasses just about anyone who furnishes, bills, or is paid for health care or health care supplies pursuant to prescription.[53] It includes doctors, pharmacists, hospitals, clinics, counselors, physical therapists, and countless others. All of these providers are subject to the same set of requirements under the Privacy Rule.

In contrast, California law does not apply uniformly to all of these different providers. Some providers, such as doctors, hospitals, and health clinics, are subject to both the Confidentiality of Medical Information Act (CMIA) and the Patient Access to Medical Records Act (PAMRA). Other providers, such as pharmacists and acupuncturists, are covered by the CMIA but are not covered by the PAMRA.[54]

Because large portions of the CMIA and the PAMRA will remain in place after the implementation of the Federal Privacy Rule, these differing groups of providers will continue to be governed by different rules. This guide only discusses those health care providers—listed at the beginning of the document—which are subject to both the CMIA and the PAMRA. A separate guide is available for those health care providers, such as pharmacists and acupuncturists, that are subject to the CMIA *but not* the PAMRA.

Existing Requirements in California Law

Doctors, hospitals, outpatient clinics, and many other health care providers in California should be familiar with state laws governing the disclosure of medical information, such as the CMIA, which restricts how health care providers may disclose "medical information."[55] The CMIA covers individually identifiable information regarding a patient's medical history, mental or physical condition, or treatment that is in the possession of or was derived from a provider of health care, a health care service plan, or a contractor. It protects information in electronic and physical form. Generally, the CMIA

prohibits a provider from disclosing medical information without a patient's written authorization.[56] It then specifically lists a number of exceptions where disclosure is permitted without the patient's permission. For each permitted disclosure, the CMIA generally imposes specific conditions dependent on the purpose of the disclosure. If a purpose is not enumerated in the CMIA, the health care provider must obtain a patient's authorization prior to disclosure. The CMIA sets out the form and substance for such authorizations.[57] In addition to the CMIA's restrictions on the disclosure of medical information, the PAMRA requires these health care providers to furnish a patient access to his or her own medical records. Under the PAMRA, patients have the right to see, copy, and append their own medical records that are maintained by certain health care providers.[58]

Similarities Between California Law and the Federal Privacy Rule

The Federal Privacy Rule's structure is fairly similar to California law: It prohibits the sharing of individually identifiable health information ("health information")[59] without the patient's permission unless the purpose of the disclosure is permitted by the rule. When disclosure is permitted without the patient's permission, the Privacy Rule generally imposes conditions specific to the purpose for which the health information is being released. If a purpose is not specified in the regulation, the provider must obtain a patient's authorization prior to using or disclosing the health information. And like California law, the Federal Privacy Rule gives patients the right to see, copy, and amend their health information.

Key Differences Between California Law and the Federal Privacy Rule

The Privacy Rule differs from California law in the following key areas:

- A patient's written consent generally must be obtained before a provider can use or disclose health information for the purposes of treatment, payment, and health care operations.
- Providers will be required to have contracts with those with whom they share information for administrative functions. These contracts must require those "business associates" to adequately safeguard the health information.
- In many circumstances, providers will be required to limit the health information they use and disclose to the minimum amount necessary to accomplish the intended purpose.
- Providers will be required to furnish a patient with a notice of privacy practices detailing how the provider may use and share health information, as well as informing the patient of his or her rights concerning his or her own health information.
- Providers will be required to undertake additional administrative duties to comply with the federal rule, such as implementing safeguards, training employees, designating a privacy official, and maintaining documentation of compliance with the regulation.

This implementation guide will focus on these major changes providers may have to implement under the Federal Privacy Rule. Providers should be aware, however, that there are also numerous other effects that the Privacy Rule will have on existing California law that are beyond the scope of this general guide.

As a practical matter, for ethical and professional reasons, many health care providers routinely obtain a patient's written permission to share their health information with others… The Privacy Rule builds upon these informal practices and makes them law.

Restrictions On Use and Disclosure of Health Information

Format of Health Information Protected

The Federal Privacy Rule expressly covers health information transmitted or maintained in any form or medium.[60] Although the Privacy Rule's restrictions on oral communications[61] generated much controversy,[62] this requirement should not substantively change the way health care providers practice in California. The inclusion of oral communications reflects many professional codes of ethics, which generally require that the health care professional maintain the confidentiality of medical information, and do not limit that requirement to information in physical form.[63] And although the CMIA does not cover oral information,[64] an individual's right to privacy under California's constitution would appear to be broad enough to prohibit inappropriate oral disclosures of personal medical information.[65]

Patient Consent: Treatment, Payment, and Health Care Operations

Health care providers, by the very nature of their occupations, receive and maintain vast quantities of identifiable health information. This information is primarily used for the "core" purposes of treatment of the patient, payment for the health care services, and for health care operations such as quality assessment and peer review. Currently, health care providers in California may use and disclose health information for these purposes without the patient's express written permission.[66] However, as a practical matter, for ethical and professional reasons, many health care providers routinely obtain a patient's written permission to share their health information with others, such as insurance companies.

HIV/AIDS

California law gives heightened protection to HIV/AIDS information. Generally, a provider must obtain a patient's written authorization specifically permitting the disclosure of the results of an HIV/AIDS test for each separate disclosure made. A patient's signing a consent form required by the Federal Privacy Rule is not enough. The federal consent form is too general, does not specifically address HIV/AIDS information, and is not required for every separate disclosure.

There are exceptions to this general rule. For example, providers may disclose HIV/AIDS test results as required under state reporting laws. Additionally, no specific authorization is required for disclosures to a provider (excluding health care service plans) for the direct purposes of diagnosis, care, or treatment of the patient.

The Privacy Rule builds upon these informal practices and makes them law. Under the Privacy Rule, health care providers are required to obtain their patients' consent prior to using or disclosing health information for treatment, payment, or health care operations.[67] However, providers who have an indirect treatment relationship with a patient (such as a radiologist in a hospital setting who does not interact with the patient) need not obtain a patient's consent.[68] The Privacy Rule also specifies some circumstances (such as in emergencies or when the provider is required by law to treat the patient) where no patient consent is required.[69]

The activities encompassed by the consent requirement are fairly broad. "Treatment" includes not only providing health care to a patient, but also coordinating or managing the patient's care with a third party, consulting with another provider, and referring a patient to another health care provider.

"Payment" includes: obtaining reimbursement for the provision of health care, billing, claims management, health care data processing, and other activities.

"Health care operations" includes: quality assessment (e.g., outcomes evaluation); case management and care coordination; peer review; accreditation and licensing; conducting or arranging for medical review, legal services, and auditing functions; customer service; business management; and other activities.

Consent Requirements

Although providers may be generally familiar with obtaining patients' written permission to share their health information, the specific requirements for obtaining and using such consents under the Federal Privacy Rule are new.

First, the Privacy Rule permits providers to refuse to treat patients who will not sign a consent permitting the use and disclosure of their health information for treatment, payment, or health care operations purposes.[70] The rule takes this approach in order to ensure that providers will be able to carry out their essential duties.

Additionally, it is not necessary for providers to obtain a new consent every time they see a patient. Rather, providers need to obtain consent from a patient for use or disclosure of health information for treatment, payment, and health care operations only once. This is true regardless of whether there is a connected course of treatment or treatment for unrelated conditions.[71]

Revoking Consent

Q: Can a patient revoke his consent?

A: Yes, a patient has the right to submit a written revocation at any time.

Q: What happens if a patient revokes his consent after receiving treatment, but before the provider has received payment?

A: The general rule is that a revocation is not effective to the extent a provider has acted in reliance on it. Since the provider in this example relied on the consent in providing treatment, it will still be able to use the consent to obtain payment for that treatment.

Format of Consent Form

Under the Federal Privacy Rule, a consent form may not be part of a notice of privacy practices. These are two distinct documents. The consent must be written in plain language. It can be brief and contain general terms. If a provider desires, it can combine a consent for the use and disclosure of health information with another type of written legal permission from the individual (e.g., an informed consent for treating the patient). However, the consent for using health information must be visually separate from the rest of the document and be signed separately by the individual.[72]

Content of the Consent Form

In order to be valid, the consent must:

- Inform the patient that his or her health information may be used and disclosed for treatment, payment, and health care operations.
- Advise the patient of his or her right to:

  Review the provider's privacy notice;

  Request restrictions on how information is used and disclosed for treatment, payment and health care operations purposes; and

  Revoke consent.
- Be signed and dated by the patient (or his or her personal representative).[73]

Providers are required to keep copies of consent forms (either in paper or electronic format) for six years.[74]

Consent in an Integrated Health Care Setting

How will consent work in a hospital setting? Will the patient have to sign a separate consent form for the hospital and for each provider they may come into contact with?

Providers who practice in a clinically integrated care setting (such as a hospital) have the option of reducing paperwork by using a single joint consent form, which applies to a number of different providers working in one setting. In order to use a joint consent form, the providers must first furnish patients with a joint notice of privacy practices. This notice must provide a description of the providers and the service delivery sites to which it applies, in addition to all of the information otherwise contained in a privacy notice. If the providers covered by the privacy notice intend to share health information with each other to carry out treatment, payment, and health care operations, they must advise patients of this arrangement.[75]

Patient Ability to Restrict Consents

In certain situations, patients have heightened concerns about the confidentiality of their health information. A patient may have friends or relatives who are employees of the health care organization. Perhaps a patient has a sensitive medical condition or is apprehensive about receiving mail or phone calls at home. Such concerns may be more frequently associated with certain services, such as family planning, mental health treatment, treatment for sexually transmitted diseases, or for injuries resulting from domestic violence. Many providers already informally accommodate these concerns by limiting the health information that they share or by restricting the method in which they communicate with the patient.

The Privacy Rule formalizes these practices by giving patients the right to request restrictions and the right to request confidential communications. Signing a consent form provides a prime opportunity for discussing these potential limitations on the use and disclosure of health information for treatment, payment, and health care operations.

Planning Consent Forms and Procedures

Providers who participate in organized health care arrangements should decide whether they want to use a joint consent with other participants.

Draft a standard consent form for future use. Consents contain only general information and their wording is not dependent on specific privacy practices and policies. When a provider is prepared to distribute its notice of privacy practice, the consent form will be ready to use.

Determine how consents will be processed and maintained.

Determine how revocations will be made effective.

Right to Request Restrictions

Under the Privacy Rule, a patient has the right to request that a provider restrict how his or her health information is used or to whom it is disclosed for treatment, payment, and health care operations purposes.[76] The provider does not have to agree to such a request. A provider is, however, bound by any restriction to which it does agree.[77] A written documentation of an agreed restriction must be kept for six years.[78]

Right to Request Confidential Communications

The Privacy Rule also creates a right to request that communications be made by specific means or at specific locations.[79] For instance, a patient could request that bills for health care services be sent to a relative's house, instead of to her home. Providers must accommodate such requests if they are reasonable. The Privacy Rule recognizes that there may be practical consequences to accommodating a request for confidential communications and permits a provider to impose certain conditions on fulfilling such a request. A provider may require the patient to put the request in writing, to provide information as to how payment will be handled, and to specify an alternative address or another method of contact.

Minimum Necessary vs. Transaction Standards

Under the HIPAA transaction standards, providers who submit health-claims information electronically will be required to use a set format that includes certain data elements. For example, providers will be required to submit health claims to insurers in a standard format.

Q: How will the minimum necessary standard affect these standard transactions?

A: It depends on the specific data element at issue. The minimum necessary rule does not apply to those data elements that are required under the transaction standards. These required data elements can be submitted without any minimum necessary analysis. However, to the extent providing information on a standard form is discretionary, providers will have to conduct the minimum necessary analysis to determine whether providing such optional information is necessary to accomplish the intended purpose.

Minimum Necessary Standard

Existing Requirements. The CMIA currently limits the amount of health information that a provider can disclose in certain circumstances. For example, a provider may disclose health information to those responsible for paying for the health care services rendered to the patient, but only to the extent necessary to allow responsibility to be determined and payment to be made.[80] Additionally, many providers have policies in place that limit the health information accessible to certain personnel. A hospital, for instance, may have a policy that allows staff pharmacists access only to prescription or medication information, as opposed to an entire medical record.

New Requirements. The Federal Privacy Rule builds on these existing rules and policies by generally requiring that covered entities, including providers, use and disclose the minimum amount of health information necessary to accomplish their goals. This is known as the "minimum necessary" standard. Providers should be aware that the "minimum necessary" standard generally applies to a broader range of circumstances than the limitations on disclosure imposed by California law.

Case-by-case Review Not Required. The Federal Privacy Rule is intended to make providers evaluate their privacy practices and improve them as needed to prevent unnecessary or inappropriate access to protected health information.[81] For most routine purposes, the rule requires that providers have policies and procedures to use and share the minimum amount of health information necessary to accomplish the intended purpose. As a general rule, providers are not required to conduct a case-by-case review.

Exceptions. There are a number of major exceptions to the minimum necessary requirement. Most significantly, the minimum necessary standard does not apply to disclosures to or requests by a health care provider for treatment purposes.[82]

Standard for Uses. For uses (i.e., using or sharing health information within a provider organization), a provider must identify those within its organization who need access to health information, the categories or type of information they need, and conditions appropriate to such access.[83] For instance, a hospital may develop a policy that a clerk who schedules medical procedures only needs access to limited relevant health information. The provider must develop policies and procedures that implement its analysis and must document them in written or electronic form.[84]

Privacy Rule Impact on Treatment

Q: Does the Privacy Rule preclude a provider from using a patient's entire medical record for treatment?

A: No. In fact, HHS anticipates that providers will have policies that allow a treating physician access to a patient's entire medical record. There must, however, be a written policy in place that supports this use.[85]

Standard for Disclosures and Requests for Disclosures. First and foremost, it is important to remember that the minimum necessary standard in the Federal Privacy Rule does not apply to any disclosure to or request by a health care provider for treatment purposes.[86] In contrast, the rule does apply for disclosures made for payment and health care operations purposes.

For other routine or recurring requests and disclosures, a provider's standard policies must limit the protected health information disclosed or requested to the minimum amount necessary for that particular type of disclosure or request.[87] These policies must also be maintained in written or electronic form.[88]

Requests from Other Covered Entities. Under the Privacy Rule, the requesting covered entity has the responsibility to request the minimum amount of health information necessary for the proposed purpose of obtaining the information. The covered entity releasing the information may (but is not required to) rely on the requesting covered entity.[89] For example, health plans routinely request health information from health care providers to support a claim for payment. In this circumstance, the burden is on the health plan to request the minimum amount of health information necessary. To comply with the minimum necessary standard, the provider can rely on the request. The provider does have the option, however, of making its own determination as to the amount and type of health information necessary.

Compliance will require identifying all of the privacy-related statutes… and doing a line-by-line comparison of these state requirements with those of the Privacy Rule. Providers will need to review their existing practices to see what changes they will need to make to come into compliance.

Preparing to Implement the Privacy Rule: Key Questions

Perform a "health information" audit of your organization or practice answering some of these key questions:

Who has access to health information within the organization or practice?

Who should have access to health information?

What type and amount of health information is reasonably necessary for employees to accomplish a specific job?

Should there be a limit on the time frame in which they have access?

Should there be other constraints on access, (e.g., information should not be removed from the premises)?

To whom does the provider disclose health information on a regular basis?

What types of health information are requested?

Is all the information requested necessary for the intended purpose?

Is the provider willing to rely on requests from other covered entities, such as health plans, to establish the boundaries of what information is needed?

Business Associates: Sharing Health Information for Administrative Purposes

Existing Requirements. Health care providers routinely hire other companies and consultants to perform a wide variety of functions for them. Providers, for example, may work with outside attorneys, bill collectors, or accreditation organizations. Under the CMIA, providers currently may freely disclose health information without patient permission for a variety of these administrative purposes, such as billing, claims management, and medical data processing. The CMIA then prohibits the recipient of this health information from further disclosing it in a way that would violate the Act.[90]

New Requirements. This practice will change with the implementation of the Federal Privacy Rule. Providers will be prohibited from disclosing health information to outside sources who perform these types of administrative functions ("business associates") unless they have entered into written contracts ensuring that the recipient of protected health information appropriately safeguards that information.[91] Entering into business associate contracts will be a major change for many providers.

Determining Who Is a Business Associate. Under the Privacy Rule, anyone who performs a function involving the use of health information on behalf of a provider or who furnishes certain services (such as legal, actuarial, or other administrative services) to the provider is a "business associate."[92] A key element of being a business associate is that the person or organization receives health information either from or on behalf of a provider. Under this standard, a billing agency would be a business associate, while a supplier of paper products would not. The Privacy Rule is not intended to cover those who merely act as a conduit of protected health information, like the U.S. Postal Service.[93]

The Necessary Elements of a Business Associate Contract. The Privacy Rule contains a fairly lengthy, detailed list of provisions that must be included in a business associate contract. Among other things, the contract must provide that the business associate will:[94]

- Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
- Ensure that subcontractors who receive protected health information from a business associate agree to the same restrictions and conditions as in the contract; and
- Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

Violation of Contracts

Q: Can a health care provider be held responsible if a business associate violates a contract?

A: Only if the provider knew the business associate was materially violating its contractual duty to safeguard health information and did nothing about it. A plan that knows that its business associate engages in a pattern of activity or a practice that materially violates the privacy provisions of its contract must take reasonable steps to correct the situation. If these steps are unsuccessful, the plan is required to either: (1) terminate the contract if feasible; or (2) if termination of the contract is not feasible, report the problem to HHS.

45 C.F.R. § 164.504(e).

Sharing Health Information with Friends and Family of the Patient

As a matter of practice, providers often share health information with family members and close friends of the patient, particularly with those who are involved with the patient's care. The Federal Privacy Rule does not prevent this practice, so long as the patient is given a chance to object. If the individual objects, the provider is prohibited from sharing health information with a patient's family or friends.[95]

Facility Directories

Some providers, such as hospitals, maintain a public directory of individuals at their facility. California statute currently restricts how this information may be collected and shared, permitting providers to use their discretion within the specified parameters.[96] The Federal Privacy Rule has more stringent requirements for including health information in a facility directory. Therefore, by following the standards of the Federal Privacy Rule, providers should be able to comply with both state and federal law.

Under the Privacy Rule, providers will be required to inform patients that their health information may be included in a directory and generally identify to whom the information may be disclosed.[97] Both the notice and any objection to inclusion in the directory may be made orally. Even if a patient does not object, the provider may only disclose the health information to a person who asks for the patient by name.[98] And the information that may be released is limited to the individual's name, location in the facility, and condition described in general terms that do not include specific medical information about the individual.[99]

The Difference Between a "Consent" and an "Authorization"

Both are written permission forms that allow a provider to use and/or disclose health information. They substantially differ, however, in both substance and form.

A consent:

- Is ongoing. It is obtained one time, and is good until the patient revokes it;
- Is used only in relation to treatment, payment, and health care operations; and
- Contains only general information and refers a patient to a notice of privacy practices for details; can be a standard form.

An authorization:

- Is limited;
- Expires upon a specified date or event;
- Is used in relation to uses and disclosures of health information for purposes other than treatment, payment, or health care operations that are not otherwise permitted by the Privacy Rule; and
- Is detailed, providing specifics about who may receive information and how it is to be used.

Uses and Disclosures That Do Not Require Authorization or Consent

Both the CMIA and the Federal Privacy Rule allow a provider to use and disclose health information without the patient's consent or authorization in a number of circumstances.[100] The laws generally impose conditions specific to the particular purpose for which the health information is to be used or disclosed. Due to the number of circumstances under which use and disclosure is permitted without any patient permission and the details of the related conditions, only a few of these purposes are discussed.

Law Enforcement. Under the CMIA and the Federal Privacy Rule, a health care provider may disclose health information pursuant to a search warrant lawfully issued to a governmental law enforcement agency.[101] However, California's Penal Code imposes more stringent restrictions on responding to search warrants for medical records when the target of the investigation is not the provider.[102] For instance, the records may be released only to a "special master" (an attorney appointed by the court) rather than the law enforcement agent, and if the provider states that the items sought should not be disclosed, the items are to be sealed and taken to the court for a hearing. There are additional procedural requirements as well.[103]

Civil Discovery. A provider may disclose a patient's health information in response to a subpoena issued in a civil proceeding only if the party requesting the information follows either of two specified procedures. The requesting party must either: (1) furnish the patient's written authorization to release the records, signed by the patient or his attorney; or (2) furnish proof that it has served on the patient (at a very minimum 10 days prior to the specified production date) a copy of the subpoena and the affidavit supporting the issuance of the subpoena.[104]

Research. Both the CMIA and the Federal Privacy Rule permit providers to disclose health information for research purposes without the permission of the patient.[105] Providers should be aware, however, that the conditions under which health information can be disclosed for research purposes are substantially altered by the Federal Privacy Rule. In the most general terms, in order to disclose health information to researchers, a provider will be required to obtain documentation that a waiver of authorization for the use and disclosure of health information was approved by either an Institutional Review Board (IRB), which reviews federally funded research; or a "privacy board," a new board that will review privately funded research using the same principles as an IRB.[106] The specific conditions under which health information can be used and disclosed for research purposes are quite detailed and should be reviewed closely.

Authorizations

Currently, under the CMIA, if a disclosure is not specifically permitted or required by the statute, a provider must obtain a patient's authorization prior to disclosing medical information.[107] The Federal Privacy Rule takes a similar approach. For purposes that are not expressly addressed in the Privacy Rule, a provider will be required to obtain a patient's authorization prior to using or disclosing his or her protected health information.[108] For example, a provider would be required to obtain a patient's authorization prior to disclosing his or her health information to a health insurer for initial enrollment purposes.[109]

Essential Elements of Authorization Forms That Will Meet State and Federal Requirements.

Because the authorization required by the Privacy Rule is quite similar to that provided for in the CMIA,[110] most plans will probably prefer that requesters of information use a single authorization form that conforms to both federal and state requirements. In order to comply with both the CMIA and the Federal Privacy Rule, an authorization form must, at a minimum:

- Be written in plain language;[111]
- Be handwritten by the person who signs it or be in 8-point typeface or larger;[112]
- Be separate (with some exceptions);[113]
- Be signed and dated;[114]
- Specifically describe the health information to be used or disclosed;[115]
- State the specific limitations on the type of information to be disclosed;[116]
- State the name or function of person (organization) authorized to make the disclosure;[117]
- State the specific date after which the provider is no longer authorized to disclose the information;[118]
- State the name or functions of persons (organization) authorized to use or receive the information;[119]
- State the specific uses and limitations on the use of medical information by the persons authorized to receive the information;[120]
- Advise the individual of his or her right to receive a copy of the authorization;[121]
- Inform the individual of his or her right to revoke the authorization under the Federal Privacy Rule; and[122]
- Include a statement that information used or disclosed under the authorization may be subject to redisclosure by the recipient and may no longer be protected by the Federal Privacy Rule.[123]

When a health care provider seeks an authorization to use or disclose health information that it maintains, the authorization form must include additional elements. Among other things, such an authorization must:[124]

- If applicable, state that the provider will not condition treatment, payment, enrollment in the health plan, or eligibility of benefits on the individual's providing the requested authorization; and
- State that the individual has the right to refuse to sign the form.

A provider that obtains an authorization for its own uses or disclosures must furnish the individual a copy of the signed authorization.[125]

Information Related to Mental Health Treatment

Information related to mental health treatment is given heightened protection by both California law and the Federal Privacy Rule. The rules vary depending on the specific type of mental health information at issue. The CMIA contains some restrictions on mental health information generated in an outpatient setting with private therapists. The Lanterman-Petris-Short Act imposes more extensive restrictive conditions on mental health information obtained in an institutional setting (either voluntary or involuntary) or pursuant to certain publicly funded community mental health treatment programs.

Mental Health Information Covered by the CMIA. A provider is required to comply with provisions of both the Privacy Rule and the CMIA in order to disclose psychotherapy-related information. Both laws have discrete rules governing psychotherapy-related information. The Privacy Rule has particularly stringent rules pertaining to psychotherapy notes.

When a third party requests health information related to psychotherapy (other than psychotherapy notes) a provider may disclose the information only if they have obtained: A signed general consent to use and disclose health information for treatment, payment, and health care operations (under the Federal Privacy Rule); and detailed written request from the person seeking the information (under the CMIA).[126]

For example, if a health insurer requests information about a diagnosis related to psychotherapy, a provider would need both a signed consent form (generally authorizing the provider to use or disclose health information for treatment, payment, and health care operations) and a written request from the insurer specifically detailing the information they require.

The request must include specific information related to psychotherapy treatment that is being requested; the specific intended use of the information; how long the information will be used; and other information. The patient's signature is not required on the request; however, a copy must be provided. The patient may waive notification of the request by submitting a letter to this effect to the provider.[127]

The heightened restrictions of the Federal Privacy Rule will govern the disclosure of psychotherapy notes (i.e., notes documenting or analyzing the contents of conversations taking place during therapy that are maintained separately from the rest of a patient's medical record).[128] A consent and a request under the CMIA will not be sufficient for disclosing these notes. Rather, a detailed authorization signed by the patient that specifically permits the use or disclosure of psychotherapy notes is required for their release.[129] Perhaps most importantly, health plans are prohibited from making enrollment or payment of claims conditional on a patient's signing such an authorization to disclose psychotherapy notes.[130]

Information Subject to the Lanterman-Petris-Short Act

Certain mental health information is governed by California's Lanterman-Petris-Short Act[131] (LPSA) in lieu of the CMIA.[132] The LPSA imposes strict restrictions on the disclosure of information obtained in the course of providing mental health services:

- To patients who are either voluntarily or involuntarily treated in an institutional setting;[133]
- Pursuant to a community mental health treatment program (funded under the Bronzan-McCorquodale Act); or
- In the course of providing intake, assessment, or services to persons with developmental disabilities by or on behalf of a regional or state developmental center.

Providers who are subject to the LPSA will need to comply with both the Federal Privacy Rule and state law. Many of the limitations on disclosure contained in the LPSA are more stringent than those contained in the Privacy Rule. For example, under the LPSA, when a patient is unable to authorize the release of his or her health information to family members, the provider may only disclose that the patient is present in the facility.[134] Because this standard is more stringent than that contained in the Privacy Rule, the state law should be followed. Similarly, the LPSA provides that a researcher must sign an oath of confidentiality as a condition of receiving mental health information for research purposes, a requirement not found in the Privacy Rule.[135]

The Privacy Rule does, however, provide additional protection for *psychotherapy notes* (i.e., notes documenting or analyzing the contents of conversations taking place during therapy that are maintained separately from the rest of a patient's medical record).[136] A detailed authorization signed by the patient that specifically permits the use or disclosure of psychotherapy notes is required for the release of this material for most purposes.[137] Perhaps most importantly, health plans are prohibited from conditioning enrollment or payment of claims on a patient's signing such an authorization to disclose psychotheraphy notes.[138]

Marketing

Among the more controversial aspects of the Federal Privacy Rule are the "marketing provisions." Under these provisions, providers are permitted to use health information for marketing health-related products or services (their own or those of a third party), so long as the marketing material identifies the provider as the source and gives the patient the opportunity to "opt out" of receiving further materials.[139] This gives the provider "one free shot" at sending the patient marketing materials before the patient is even given the opportunity to object.

Providers in California, however, should be aware that the CMIA appears to require a patient's written authorization before engaging in many marketing activities.[140] Because this standard is more consumer-protective than the federal regulation, the state law will remain in effect. This means that providers should get patients' written authorization before using or sharing their health information for marketing.

Patient Rights

In addition to imposing restrictions on how providers can use and disclose protected health information, both California law and the Federal Privacy Rule grant patients rights with respect to their own health information. These rights are based in fair information practice principles, which give patients the right to know how their information is being used and who it is being shared with; to see and copy their own health information; and to amend it, if necessary.

Notice of Privacy Practices

Under the Federal Privacy Rule, covered health care providers will be required to give patients a written notice describing their privacy practices.[141] This will be a new requirement for California providers, which currently are not required to furnish such notices under state law.

Providers should furnish these privacy notices to patients on or before the first time they provide health care after April 14, 2003 (the compliance date for the regulation). In addition to giving the patients a copy of the notice, providers must post the notice on their premises.

The Federal Privacy Rule is quite detailed in the content requirements for a notice of privacy practices. Providers will need to consult the rule to determine the exact language that a notice requires in order to be in compliance. In general, a notice of privacy practice must:[142]

- Be written in plain language;
- Contain a prominent statement about how health information may be used and disclosed;
- Describe how the provider protects health information under the Privacy Rule;
- Specify when health information may be used or released without the individual's prior written consent or authorization;
- Describe, including at least one example, the types of uses and disclosures that a health care provider is permitted to make for treatment, payment, and health care operations purposes under the Privacy Rule;
- Describe individuals' rights with respect to their protected health information (such as their right to revoke an authorization and their right to amend their health information) and describe how to exercise those rights;
- Notify individuals how they may obtain access to their health information, including obtaining copies;
- Include information about how an individual can file complaints about privacy matters with both their provider and the U.S. Department of Health and Human Services; and
- Provide the name of a contact person for additional information.

Giving Patients Access to Their Own Health Information

Existing Requirements. The PAMRA provides patients a right of access to "patient records" maintained by specified health care providers including doctors; dentists; psychologists; optometrists; clinical social workers; home health agencies; marriage, family and child counselors; and hospitals and other health care facilities. It generally requires health care providers to permit patients to see and copy their own "patient records," a term defined as "records in any form… maintained by… a health care provider relating to the health history, diagnosis, or condition of a patient, or relating to treatment provided or proposed to be provided to the patient."[143] By recent amendments, it also grants many patients the right to submit a written addendum to their medical record with respect to any item or statement that they believe to be incomplete or incorrect.[144]

Providing Laboratory Tests Results Electronically

California requires providers to furnish the results of lab tests to patients in oral or written form.[145] Under recent amendments, health care providers may also deliver laboratory test results in electronic form if they obtain a patient's written authorization to do so. Patients may not be charged for electing to receive their laboratory results in another format.[146]

New Requirements. The Federal Privacy Rule has a similar regulatory scheme. It requires covered providers to permit patients to see and copy their health information that is in a "designated record set," a term that includes (with respect to providers) medical records, billing records, and any other group of health information that is used to make decisions about the individual.[147] The Privacy Rule also grants patients the right to request amendments to their health information if it is incorrect or inaccurate. Generally, the "floor" set by the Federal Privacy Rule is less detailed and protective than that contained in PAMRA.

Complying with both Federal and State Requirements

The net result of the interplay between the PAMRA and federal law is that, for the most part, providers who already comply with the state statute will not be required to substantially change their practices with the implementation of the Federal Privacy Rule. The combined requirements of the state and federal law are discussed below.

Scope. Patients in California have the right to see and copy their health information that is maintained by a health care provider. This right extends to medical records and billing records maintained by a covered provider.[148]

Requests. Under state law, a patient's request to inspect or copy his or her health information must be in writing.[149] The Federal Privacy Rule will allow this practice to continue so long as the provider has given the patient notice that it only accepts written requests.[150] The provider should require the patient to provide reasonable verification of identity before responding to the request.[151]

Time Limits. A provider must allow a patient to review his or her health information within five working days of receiving a request.[152] If a patient requests a copy of this information, the provider must furnish the copy within 15 days of receiving the request.[153]

Format. A provider may prepare a summary of the requested health information, rather than allowing access to the entire medical record, if the patient agrees to this format and to pay the fees associated with preparing the summary.[154]

Fees. In order to offset the costs of providing access to health information, a provider may charge copying fees, which are set at 25 cents per page for a photocopy and 50 cents per page for microfilm.[155] In addition, providers may charge for the labor cost of copying the documents, as well as for postage.[156] HHS takes the position that providers may not charge for retrieving and handling the information or for processing the request.[157] It is unclear whether a provider that utilizes a third party record keeper that imposes a charge to retrieve records may pass such a change on to the patient. A provider can also charge a reasonable cost-based fee for explaining or summarizing health information, where a patient has agreed to this format.[158]

Denying Patients Access. In some circumstances, a provider is reluctant to provide a patient access to his own medical records for fear of the impact it may have on the patient. Under PAMRA, a provider may deny access to only a narrow category of health information based on this premise—mental health records (i.e., information that relates to the evaluation or treatment of a mental disorder).[159]

Although state law determines the category of information that may be denied, the Federal Privacy Rule will set the standard under which access may be denied.[160] Under the federal regulation, a provider may deny a patient access based on potential endangerment only when granting access is reasonably likely to endanger the life or physical safety of the patient or another person.[161]

The Federal Privacy Rule also creates a new framework for reviewing denials of access to health information.[162] A provider must furnish a patient a written denial in plain language that generally explains the basis of the denial. This notice must also advise the individual of his or her right to have this decision reviewed. If the patient requests a review, the provider must promptly refer the material to a licensed health care professional who did not participate in the original decision. The designated reviewer, who is selected by the provider, makes the final determination whether the patient should be furnished with access to the records.[163]

Even if access is denied at this point, the patient retains the right under California law to designate another provider to review his or her health information.[164] At the patient's request, the holder of the records must furnish the health information to the designated provider for his or her review. That designated provider, however, is prohibited from allowing the patient to see or copy the records.

Accounting of Disclosures

The Federal Privacy Rule grants patients the right to receive an accounting of prior disclosures of health information.[165] This will impose a new duty on providers, who are not currently required to furnish such an accounting under the PAMRA.

Within 60 days of receiving a request, a provider is required to furnish the patient with a list of disclosures made within the past six years.[166] This accounting is not as broad as it first appears. First, it only applies to "disclosures," i.e., information shared with third parties. It does not apply to "uses," i.e., information utilized or shared within a provider's organization. Additionally, the accounting provisions do not apply to any disclosures that are made for treatment, payment, or health care operations purposes.[167]

Providers will, however, be required to account for other disclosures that they may routinely make, such as those made to public health authorities, to researchers, and to health oversight agencies.

Patients' Right to Amend Health Information

Patients in California will have two methods of amending their health information after the Federal Privacy Rules are implemented—one based in state law, the other grounded in the Federal Privacy Rule. This results from the fact that the state requirements, while different from the federal requirements, do not conflict with them. Because each method has its own advantages, providers should expect to encounter and respond to both types of requests to amend.

State Procedure. California statutes provide a fairly simple method for requesting amendments of health information. Under recent amendments to the PAMRA, adult patients have the right to submit to their health care provider a written statement, no more than 250 words long, regarding any information contained in their medical records that they believe to be incomplete or inaccurate.[168] The statement becomes part of the medical record and must be included whenever the provider discloses the contested information. Although this procedure is simple, it does not require any input or review by any health care provider and, therefore, may lack credibility.

Federal Procedure. Under the Privacy Rule patients will have the right to request that their provider amend their health information.[169] Although the procedure for amendment under the federal regulation is more complex than under state law, it may be used by patients who believe that a change made by their provider will be more credible than a statement merely submitted on their own.

Providers may require patients to submit their requests in writing and to provide reasons supporting their request, so long as patients are informed of these procedural requirements in advance. The provider must act on the request for amendment within 60 days of receiving it.[170]

Accepting Requests for Amendment. If the provider accepts the request it must (1) make the appropriate amendment, and (2) inform the patient in a timely fashion that the amendment is accepted. The provider must then furnish the amendment to both entities identified by the individual and other entities known to have received the erroneous information.[171]

Denying Requests for Amendment. A provider may deny a patient's request for amendment if the provider determines that the information or record (1) was not created by the covered entity, unless the originator of the protected health information is no longer available to make the amendment; (2) is not a part of a designated record set; (3) would not be available for inspection (see summary of right of access above); or (4) is accurate and complete.[172]

If the provider denies a patient's request, it must give the individual a timely, written denial that includes (1) the basis for the denial, (2) the individual's right to submit a written statement disagreeing with the denial and how to exercise that right, (3) a statement that the individual can request the covered entity to include the individual's request and the denial with any future disclosures of the information (if the individual does not file a statement of disagreement), and (4) a description of how the individual can file a complaint with the covered entity or the Secretary of HHS.[173]

If the patient files a statement of disagreement, the provider can include a rebuttal to the patient's statement in the record. The provider must also give a copy of the rebuttal to the patient. The request for amendment, the denial, the statement of disagreement (if submitted), and rebuttal (if any), or a summary of such information must be provided with any subsequent disclosure of the protected health information.[174]

It should be noted that even if a patient initiates a request to amend under the federal regulations, he or she do not give up their right under state law to submit their own 250-word addendum.

Administrative Requirements

The Federal Privacy Rule will impose a number of administrative requirements on all covered health care providers. For the most part, these requirements are fairly general. HHS, recognizing that there are vast differences in the nature, size, and organization of health care providers, decided that a "one-size-fits-all" set of administrative requirements would not be workable. Rather, the administrative requirements are intended to be *flexible* and *scalable*, depending on the particular provider's circumstances.[175] Some of the major administrative requirements are listed below.

Policies and Procedures

Providers must develop and implement policies and procedures for using and maintaining health information in compliance with the Privacy Rule.[176] These policies and procedures should address, at a minimum, who has access to health information within the organization; how health information will be used within the organization; and when, to whom, and under what conditions the information may be disclosed.

Safeguards

A covered provider must have appropriate administrative, technical, and physical safeguards in place to protect the privacy of protected health information, and reasonably safeguard the information from intentional or unintentional use or disclosure.[177] Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring file cabinets containing such records to be locked.[178]

HHS has emphasized that this rule requires only "reasonable efforts" to protect health information. The rule does not require hospitals or doctors' offices to be retrofitted to provide private rooms or soundproofed walls, or otherwise restructured.[179] Rather, providers are urged to take a common sense approach.[180]

Sign-in sheets are somewhat problematic since by their very nature they disclose protected health information to others who are signing in for health care service. HHS expects to issue modifications to the Privacy Rule to clarify that sign-in sheets and similar practices will remain permissible.[181]

Training

A covered provider will be required to train all members of its workforce on the policies and procedures regarding protected health information required by the regulation no later than its compliance date. New members of the workforce should receive training within a reasonable period of time after they begin working.[182]

Again, training requirements are flexible and scalable. For example, in a small physician practice, the training requirement could be satisfied by providing each new member of the workforce with a copy of the practice's privacy policies and requiring these members to acknowledge that they have reviewed them.[183]

Privacy Officer and Contact Person

The Federal Privacy Rule requires a covered provider to designate a privacy official for the development and implementation of its policies and procedures.[184] In addition, a provider will be required to identify a contact person who is responsible for receiving complaints.[185] At its option, the provider can designate one person for both functions.[186]

The implementation of these requirements will depend on the size and organization of the provider's office. For example, a small physician's practice might designate the office manager to assume these roles along with other administrative duties.[187]

Complaint Procedure

Providers must establish a process for individuals to file complaints about the provider's health privacy policies and practices and its compliance with the Federal Rule.[188]

Documentation

Providers will be required to maintain documentation in a variety of areas including, but not limited to, the following:

- Consents;[189]
- Agreed restrictions on using or disclosing health information for treatment, payment and health care operations;[190]
- Authorizations;[191]
- Disclosures for purposes other than treatment, payment and health care operations;[192]
- Minimum necessary policies for use and disclosure of health information;[193] and
- Training of personnel.[194]

This documentation must be kept for six years from the date of its creation or the date it was last in effect, whichever is later.[195]

Looking Ahead

Clearly, the new Privacy Rule will require health care providers to make significant changes to their operations in order to comply with both the Privacy Rule and existing California laws. Understanding how the various laws interact and what practices will be required will be challenging. Compliance will require identifying all of the privacy-related statutes that apply to a particular provider and doing a line-by-line comparison of these state requirements with those of the Privacy Rule. Providers will need to review their existing practices to see what changes they will need to make to come into compliance. Hopefully, this guide has helped to begin that process. There is not a substantial amount of time for providers to complete the changes they will need to make and it is incumbent upon providers to use this period wisely.

Health Information for Minors

The Federal Privacy Rule will not change how the health information of minors is treated. Under both the Patient Access to Medical Records Act and the Federal Privacy Rule, generally it is the parent (not the minor) who has the right of access to the minor's health information. Both laws make an exception, however, when the information relates to medical treatment for which a minor is authorized by law to consent. For example, in certain circumstances, a minor in California has the right to consent to reproductive services and mental health services. In these situations, the minor, not the parent, has the right of access to the related health information.

Appendix A: Key Resources for Implementation Assistance

Department of Health and Human Services (HHS)
Information on all the Administrative Simplification requirements (including, but not limited to, the Privacy Rule): http://aspe.hhs.gov/admnsimp/index.htm.

Office of Civil Rights (OCR), HHS
Information on the Privacy Rule, including the text of the rule and technical guidance: http://www.hhs.gov/ocr/hipaa.

Massachusetts Medical Society HIPAA Resources
Useful links, questions/answers, and HIPAA implementation tips: http://www.mass.med.org.

American Health Information Management Association
Association that represents health information management professionals who work throughout the health care industry. HIPAA related articles, frequently asked questions, practice briefs, and links to other Web sites: http://www.ahima.org/hot.topics.

Health Privacy Project
Information about protecting the privacy of health information, including the Federal Privacy Rule, state health privacy laws, and current developments: http://www.healthprivacy.org.

Appendix B: Checklist of Key Items for Implementation

1. Adopt written privacy procedures, specifying:
   - who has access to health information,
   - how health information will be used within the provider's organization, and
   - when the information may be disclosed.

   (New under HIPAA)

2. Draft Notice of Information Practices.

   (New under HIPAA)

3. Draft Consent Forms.

   (New under HIPAA)

4. Revise or draft Authorization Forms.

   (CMIA and HIPAA)

5. Revise or draft Contracts with Business Associates.

   (New under HIPAA)

6. Designate:
   - contact person for receiving complaints, and
   - privacy officer (can be same person).

   (New under HIPAA)

7. Train personnel about protecting privacy and requirements of Privacy Rule.

   (New under HIPAA)

Endnotes

1. Cal. Civ. Code § 56-§ 56.37.
2. Cal. Health & Safety Code § 123100 - § 123149.5.
3. The Patient Access to Medical Records Act applies to all health facilities licensed pursuant to Cal. Health & Safety Code, Div. 2, Chap. 2 (commencing with Section 1250), as well as all clinics licensed pursuant to Cal. Health & Safety Code, Div. 2, Chap. 8 (commencing with Section 1725). Cal. Health & Safety Code § 123105.
4. *Standards for Privacy of Individually Identifiable Health Information: Final Rule*, vol. 65, Federal Register ("65 Fed. Reg.") pp. 82462-82829 (Dec. 28, 2000). This rule is codified in title 45, Code of Federal Regulations (45 C.F.R.).
5. *Standards for Privacy of Individually Identifiable Health Information: Guidance* (hereinafter "HHS Guidance") (July 6, 2001). Available online at *http://www.hhs.gov/ocr/hipaa/*.
6. 45 C.F.R. § 160.102 and § 164.104.
7. 45 C.F.R. § 160.103 (defining "covered entity").
8. 45 C.F.R. § 160.103 (defining "health plan").
9. 45 C.F.R. § 160.103 (defining "health plan").
10. 45 C.F.R. § 160.103 (defining "health care clearinghouse").
11. 45 C.F.R. § 160.102 and § 164.104 (explaining "applicability").
12. 45 C.F.R. § 160.103 (defining "health care provider").
13. 45 C.F.R. § 160.103 (defining "health care").
14. 65 Fed. Reg. 82477.
15. *See Standards for Privacy of Individually Identifiable Health Information: Proposed Rule, Preamble* ("Preamble to Proposed Privacy Rule"), 64 Fed. Reg. 59937 (November 3, 1999).
16. There is some controversy concerning whether a provider must actually use the required format to become a "covered entity" or whether it may become "covered" by merely electronically conducting one of the transactions listed in HIPAA.
17. *See* 42 U.S.C. Sec. 1320d-2(a) for the full list of electronic transactions that will trigger coverage of the privacy regulation.
18. Congress recently passed the Administrative Simplification Compliance Act, Pub. Law 107-105, that permits covered entities that cannot meet the October 2002 deadline for complying with the transactions regulations to obtain a one year delay. In order to qualify for the one-year delay, a covered entity must submit a compliance plan no later than October 2002. The date for complying with the Privacy Rule is not delayed or effected by this Act. *See* 147 Congressional Record S13077 (daily ed. December 12, 2001) (statement of Senator Dorgan).
19. *See Standards for Privacy of Individually Identifiable Health Information: Final Rule, Preamble* ("Preamble to Privacy Rule") 65 Fed. Reg. 82477.
20. 45 C.F.R. § 164.500.
21. 45 C.F.R. § 164.501 (defining "protected health information" and "individually identifiable health information") and § 160.103 (defining "health information").
22. 45 C.F.R. § 160.103 (defining "health information").
23. 45 C.F.R. § 164.501 (defining "individually identifiable health information").
24. 45 C.F.R. § 164.502 and § 164.514.
25. 45 C.F.R. § 164.501 (defining "individually identifiable health information").
26. There is some controversy over the scope of information that may be protected by HHS in the Privacy Rule. Some parties have challenged the constitutionality of the rule, contending that HHS only had the authority to regulate claims-related health information in electronic format. *See South Carolina Medical Association v. HHS,* No. 01-CV-2965 (U.S.D.Ct. S. Car.) (filed 7/16/01).
27. *See* 45 C.F.R. § 164.501 (defining "use" and "disclosure").
28. Providers who have only an indirect treatment relationship with patients are not required to obtain consent. *See* 45 C.F.R. § 164.506(a)(2). An indirect treatment relationship is one where the health care provider does not directly interact with patients, such as many radiologists in hospital settings. *See* 45 C.F.R. § 164.501 (defining "indirect treatment relationship").
29. Even if a covered entity obtains a delay for complying with the transaction standards, it still must comply with the Pirvacy Rule by April 2003. *See* note 18 above.

30. 45 C.F.R. § 160.103 (defining "small health plan") and § 164.534 (specifying compliance dates).
31. *See HHS Guidance* at 6-7, stating that HHS intends to alter the rule.
32. *Statement of Delegation of Authority*, 65 Fed. Reg. 82381 (Dec. 28, 2000).
33. *Preamble to Proposed Privacy Rule*, 64 Fed. Reg. 6002.
34. *See HHS Guidance*, note 5.
35. *See* HHS Guidance, note 5, at 3; 45 C.F.R. § 160.304 and 65 Fed. Reg. 82603.
36. *See* 45 C.F.R. § 160.310.
37. 45 C.F.R. § 160.306.
38. 45 C.F.R. § 160.308.
39. 45 C.F.R. § 160.310.
40. *See* discussion of documentation requirements in "Administrative Requirements," above.
41. 45 C.F.R. § 160.310.
42. 42 U.S.C. § 1320d-5.
43. 42 U.S.C. § 1320d-6.
44. *Preamble to Privacy Rule*, 65 Fed. Reg. 82488.
45. 45 C.F.R. § 160.202.
46. 45 C.F.R. § 160.202.
47. Cal. Civ. Code § 56-§ 56.37.
48. Cal. Health & Safety Code § 123100 - § 123149.5.
49. Cal. Welf. & Inst. Code § 14100.2.
50. The Lanterman-Petris-Short Act, codified at Cal. Wef. & Inst. Code § 5328 et seq.
51. Cal. Health & Safety Code § 120775, § 120975 - § 121020.
52. Cal. Welf. & Inst. Code § 11970.5 - § 11977.
53. *See* 45 C.F.R. § 160.102 (defining "health care" and "health care provider").
54. Both the CMIA and the Patient Access to Health Records Act apply to providers of health care. *See* Cal Civ. Code § 56.10 and Cal. Health & Safety Code § 123110. However, due to differing definitions of the term "health care provider," the Patient Access to Health Records Act applies to a narrower category of providers than the CMIA. *Compare* Cal. Civ. Code § 56.05(h) (defining "provider of health care") *with* Cal. Health & Safety Code § 123105 (defining "health care provider").
55. The CMIA applies to licensed health care providers, health care service plans licensed under the Knox-Keene Act, and contractors (medical groups that do not technically fall within the other categories). Cal. Civ. Code § 56.10.
56. Cal. Civ. Code § 56.10.
57. Cal. Civ. Code § 56.11.
58. Cal. Health & Safety Code § 123100 et. seq.
59. The definition of "health information" under the Privacy Rule appears to be broader than "medical information" under the CMIA.
60. *See* 45 C.F.R. § 164.501 (defining "protected health information").
61. Oral communications do not have to be recorded. Since patients only have access to health information in "designated record sets," as a practical matter they do not have access rights to oral information. However, if oral communications are recorded and used to make decisions about a person, oral information may become part of a designated record set and then must be made available to the patient upon request. *Standards for Privacy of Individually Identifiable Health Information: Guidance* at 28 (July 6, 2001) (hereinafter "Guidance").
62. *See* Robert Pear, White House Plans to Revise New Medical Privacy Rules, N.Y. Times, April 8, 2001 at 22.
63. *See* American Medical Association Canon 5.05.
64. Cal. Civ. Code § 56.10 and § 56.05(f) (defining "medical information.").
65. *See* Cal Const, art I § 1; Jeffrey H. v. Imai, Tadlock & Keeney, 100 Cal. Rptr.2d 916 (2000) (state constitutional right to privacy extends to the details of a person's medical history).
66. Cal. Civ. Code § 56.10.
67. 45 C.F.R. § 164.506.
68. 45 C.F.R. § 164.506.
69. 45 C.F.R. § 164.506
70. 45 C.F.R. § 164.506(b)(1).
71. HHS Guidance at 9.
72. 45 C.F.R. § 164.506(b)(3) and (4).
73. 45 C.F.R. § 164.506(c).

74. 45 C.F.R. . § 164.506(b)(6) and § 164.530(j).
75. 45 C.F.R. § 164.506(f); § 164.520(d) and § 164.501 (defining "organized health care arrangement").
76. 45 C.F.R. § 164.522.
77. 45 C.F.R. § 164.522.
78. 45 C.F.R. § 164.530(j).
79. 45 C.F.R. § 164.522(b).
80. Cal. Civ. Code § 56.10(c)(2).
81. *Guidance* at 20.
82. 45 C.F.R. § 164.502(b) (explaining when minimum necessary standard applies).
83. 45 C.F.R. § 164.514(d)(2).
84. 45 C.F.R. § 164.530(j).
85. 45 C.F.R. § 164.514(d)(5); 65 Fed. Reg. 52544 ("[W]e expect that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed").
86. 45 C.F.R. § 164.502(b)(2).
87. 45 C.F.R. § 164.514(d)(3) and (4).
88. 45 C.F.R. § 164.530(j).
89. *See* 45 C.F.R. § 164.514(d)(3) and (4).
90. Cal. Civ. Code § 56.10(c)(3).
91. 45 C.F.R. § 164.502(e).
92. 45 C.F.R. § 160.103 (defining "business associate").
93. 65 Fed. Reg. 82476.
94. 45 C.F.R. § 164.504(e)(2).
95. Of course, if the family member is responsible for payment of the health care services, disclosure is permitted to the extent necessary to obtain payment pursuant to the patient's signed consent form. 45 C.F.R. § 164.506.
96. Under California law, upon an inquiry concerning a specific patient, a provider is allowed to disclose certain health information unless the patient has made a written request to the contrary. If the patient has not made such a request, the provider may, at its discretion, release any of the following medical information: the patient's name, address, age, and sex; a general description of the reason for treatment (such as a burn or poisoning); the general nature of the medical condition; and the general condition of the patient. Cal. Civ. Code § 56.16.
97. 45 C.F.R. § 164.510(a).
98. Providers may also disclose health information to clergy who do not ask for patients by name. 45 C.F.R. § 164.510(a).
99. 45 C.F.R. § 164.510(a).
100. *See generally* Cal. Civ. Code § 56.10 and 45 C.F.R. § 164.512.
101. Cal. Civ. Code § 56.10(b) and 45 C.F.R. § 164.512.
102. *See* Cal. Penal Code § 1524, which generally applies when medical records are sought from a provider who is not the target of a criminal investigation.
103. Cal. Penal Code § 1524.
104. Cal. Civ. Code § 56.10(b) Cal. Code of Civ. Pro. § 1985.3 and 45 C.F.R. § 164.512(f).
105. Cal Civ. Code § 56.10 (c)(7) and 45 C.F.R. § 164.512(i).
106. 45 C.F.R. § 164.512(i).
107. Cal. Civ. Code § 56.10.
108. 45 C.F.R. § 164.
109. *See* 65 Fed. Reg. 82490 (explaining that an authorization is required to release health information for purposes of pre-enrollment underwriting).
110. *See* Cal. Civ. Code § 56.11.
111. 45 C.F.R. § 164.508(c)(2).
112. Cal. Civ. Code § 56.11.
113. *See* 45 C.F.R. § 164.508(b)(2). An authorization can be combined with other authorizations to use or disclose health information. This rule does not apply to authorizations to use or disclose psychotherapy notes, which must always be separate. It also does not apply where a covered entity has conditioned the provision of treatment, payment or enrollment in a health plan, or the eligibility of benefits on the provision of an authorization.
114. Cal. Civ. Code § 56.11 and 45 C.F.R. § 164.508(c)(1).
115. 45 C.F.R. § 164.508(c).
116. Cal. Civ. Code § 56.11.
117. Cal. Civ. Code § 56.11 and 45 C.F.R. § 164.508(c).
118. Cal. Civ. Code § 56.11 and 45 C.F.R. § 164.508(c) (the Federal Privacy Rule also allows a person to specify an event that would terminate the authorization).

119. Cal. Civ. Code § 56.11 and 45 C.F.R. § 164.508(c).

120. Cal. Civ. Code § 56.11.

121. Cal. Civ. Code §56.11.

122. 45 C.F.R. § 164.508(c).

123. 45 C.F.R. § 164.508(c). The Federal Privacy Rule does not directly regulate the recipients of health information, and therefore requires this notice. It should be noted, however, that the CMIA often directly prohibits these recipients from re-disclosing health information. In these circumstances, patients will be protected by state, rather than federal, law.

124. 45 C.F.R. § 164.508(d).

125. 45 C.F.R. § 45 C.F.R. § 164.508(d)(2).

126. Cal. Civ. Code § 56.104. The heightened protection afforded by California law appears to apply only when the third party *requests* information. It does not appear to apply when a provider initiates the transfer of information. For example, when a provider submits to an insurer a claim for payment related to psychotherapy no specific request under Section 56.104 is required. However, if an insurer wants to obtain additional information in support of the claim, it would need to submit such a request.

127. Cal. Civ. Code § 56.104.

128. 45 C.F.R. § 164.508(a)(2).

129. 45 C.F.R. § 164.508(a)(2).

130. *See* 45 C.F.R. § 164.508(b)(4).

131. Cal. Welf. & Inst. Code § 5328 et seq.

132. *See* Cal. Civ. Code § 56.30.

133. Institutional settings include any private institution, hospital, clinic, or sanitrium which conducts care and treatment for the mentally disordered.

134. *Compare* Cal. Welf. & Inst. Code § 5328.1 (limiting such information to the fact that the patient is present in the facility) *with* 45 C.F.R. § 164.510(b) (which allows the provider to use its professional judgment).

135. Welf. & Inst. Code § 5328(e).

136. *See* 45 C.F.R. § 164.508(a)(2) and § 164.501 (defining "psychotherapy notes").

137. *See* 45 C.F.R. § 164.508(a)(2).

138. *See* 45 C.F.R. § 164.508(b)(4).

139. 45 C.F.R. § 164.514(e).

140. Cal. Civ. Code § 56.10(d) specifies that a provider may not share, sell, or otherwise use any medical information for any purpose not necessary to provide health care services to the patient.

141. 45 C.F.R. § 164.520.

142. 45 C.F.R. § 164.520(b). This list is not exhaustive because the requirements of the Federal Privacy Rule are so detailed in this area. Please see the regulation itself for all of the required elements of a notice of privacy practices.

143. Cal. Health & Safety Code § 123105 (defining "patient records") and § 123110.

144. Cal. Health & Safety Code § 123111.

145. Ca. Health & Safety Code § 123148.

146. Ca. Health & Safety Code § 123148.

147. *See* 45 C.F.R. § 164.524 (giving patients access to information in a "designated record set") and 45 C.F.R. § 164.501 (defining "designated record set" as including "medical records and billing records about individuals maintained by or for a covered health care provider.")

148. A California appellate court has ruled that the "patient records" covered by the Patient Access to Medical Records Act include billing records. *See Person v. Farmers Insurance Group*, 61 Cal. Rep.2d 30 (1997). The Federal Privacy Rule also clearly grants patients access to information related to the payment of health care. *See* 45 C.F.R. § 164.524 (giving patients access to information in a "designated record set") and 45 C.F.R. § 164.501 (defining "designated record set" as including "medical records and billing records about individuals maintained by or for a covered health care provider.")

149. Cal. Health & Safety Code § 123110(a).

150. 45 C.F.R. § 164.524(a).

151. Cal. Health & Safety Code § 123110(a) and 45 C.F.R. §164.514(h).

152. Cal Health & Safety Code § 123110(a).

153. Cal. Health & Safety Code § 123110(b).

154. 45 C.F. R. § 164.524 (c).

155. Cal. Health & Safety Code § 123110(b).

156. 45 C.F.R. § 164.524(c).

157. *See* 45 C.F.R. § 164.524 and 65 Fed. Reg. 82557 (explaining HHS's position on the fees acceptable under the rule).

158. 45 C.F.R. § 164.524(c).

159. Cal. Health & Safety Code §§ 123115 and 123105 (defining "mental health records"). Providers should note that although the Lanterman-Petris-Short Act (LPSA) governs the disclosure of mental health information generated through treatment obtained at institutions and certain community clinics, the PAMRA governs a patient's access to that information. *See* Section V B xi above (discussing disclosure requirements under the LPSA) and Cal. Health & Safety Code, §. 23110, the PAMRA, (stating that it applies "notwithstanding" provisions of the LPSA).

160. The interplay between the Federal Privacy Rule and California law is complex in this area. The state law permits denials with respect to a narrow category of information whereas the federal rule permits access to be denied to any health information. However, the standard for denial is generally stricter under federal law than it is under state law. But the federal regulation would allow a denial of access to be based on endangerment to others, while California limits denial to where the access would endanger the patient. We have attempted to analyze this complicated interaction of state and federal law with an eye towards giving a patient the most access to their own health information, but advise providers to exercise caution in denying patients' access to their own information based on potential endangerment.

161. 45 C.F.R. § 164.524(a).

162. 45 C.F.R. § 164.524(d).

163. 45 C.F.R. § 164.524(d).

164. Cal. Health & Safety Code § 123115.

165. 45 C.F.R. § 164.528.

166. 45 C.F.R. § 164.528.

167. 45 C.F.R. § 164.528.

168. Cal. Health & Safety Code § 123111.

169. 45 C.F.R. § 164.526.

170. 45 C.F.R. § 164.526(b).

171. 45 C.F.R. § 164.526(c).

172. 45 C.F.R. § 164.526(d).

173. 45 C.F.R. § 164.526 (d).

174. 45 C.F.R. § 164.526 (d).

175. 65 Fed. Reg. 82471.

176. 45 C.F.R. § 164.530.

177. 45 C.F.R. § 164.530(c) and Cal. Civ. Code § 56.101 (requiring providers to preserve the confidentiality of medical information if they create, maintain, preserve, store, abandon, destroy, or dispose of such information). Additionally, HHS is to issue more detailed final HIPAA-mandated security regulations.

178. 65 Fed. Reg, 82562.

179. *Guidance* at 23.

180. 65 Fed. Reg, 82562.

181. *Guidance* at 23.

182. 45 C.F.R. § 164.530(b).

183. *Preamble to Proposed Standard for Privacy of Individually Identifiable Health Information*, 64 Fed. Reg. 59989 (Nov. 3, 1999).

184. 45 C.F.R. § 164.530(a).

185. 45 C.F.R. § 164.530(a).

186. Preamble to Proposed Rule, 64 Fed. Reg. 59988.

187. Preamble to Proposed Rule, 64 Fed. Reg. 59988.

188. 45 C.F.R. § 164.506(d).

189. 45 C.F.R. § 164.506(b).

190. 45 C.F.R. § 164.522(a).

191. 45 C.F.R. § 164.508(b)(6).

192. 45 C.F.R. § 164.528(d)(1).

193. 45 C.F.R. § 164.514 and § § 164.530(i) and 164.530(j).

194. 45 C.F.R. § 164.530(b) and § 164.530(j)(1).

195. 45 C.F.R. § 164.530(j)(2).

Related Publications in the iHealthReports series include:

- *HIPAA Administrative Simplification: Tool Kit for Small Group and Safety-Net Providers*
- *Comparing eHealth Privacy Initiatives*
- *E-Encounters*
- *E-Disease Management*
- *E-Prescribing*
- *Wireless and Mobile Computing*

These reports can be obtained by visiting the CHCF Web site at **www.chcf.org** or by calling the Publications line at **1-888-430-CHCF (2423)**.

CALIFORNIA
HEALTHCARE
FOUNDATION

476 Ninth Street
Oakland, California 94607
Tel: 510.238.1040
Fax: 510.238.1388
www.chcf.org