Implementing the Federal Health Privacy Rule in California:

A Guide for Health Insurers and Health Care Service Plans

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. Additionally, a special thank you goes to Dani Collier, Project Manager, Regulatory Compliance, PacifiCare of California and the staff of the Department of Managed Health Care for taking time out of their busy schedules to review this guide. Their input was invaluable.

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 1-929008-84-8

Contents

Overview

THIS GUIDE IS INTENDED FOR HEALTH INSURERS (subject to the Insurance Information and Privacy Protection Act) and health care service plans (subject to the Knox-Keene Health Care Service Plan Act).

Health care providers should consult either *Implementing the Federal Health Privacy Rule in California: A Guide for Providers,* or *Implementing the Federal Health Privacy Rule in California: A Guide for Pharmacists, Physical Therapists and Others,* CHCF publications specifically designed for their needs.

Purpose

THIS GUIDE IS DESIGNED TO HELP CALIFORNIA health insurers and health care service plans 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 health insurers and plans 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 an insurer or health care service plan 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 insurers and health care service plans 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.

Because health insurers and health care service plans are subject to different requirements under California law, the implementation requirements for each of these categories is addressed in a separate section. Each of these sections stands alone and may be read individually.

I. Background

The Value of Health Information

Health insurers and health care service plans 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 heath 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

Although Congress has recognized the importance of protecting the confidentiality of health information, it has been unable to pass any comprehensive health privacy legislation.

Privacy Rule Updates

To receive email notification on changes to the Privacy Rule and other health privacy news sign up 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, known as the "administrative simplification provisions," intended to cut administrative health care costs by standardizing electronic health care transactions. 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[1] (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.[2]

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).[3]

These persons and organizations are referred to as "covered entities."[4] 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.[5] 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.[6]

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.[7] 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.[8] 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.[9] "Health care," in turn, is broadly defined as "care, services, or supplies related to the health of an individual."[10] 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.[11]

Transmitting health information electronically.[12] 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 a 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.[13] 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.[14] Providers who submit health claims electronically will be required to transmit them in standard format by October 2003 at the latest.[15]

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.[16] 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.[17] 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.[18]

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.[19] This definition is broad enough to encompass not only the traditional medical record but also physicians' personal notes and billing information.

Individually Identifiable

Individually identifiable health information" is health information that identifies or reasonably can be used to identify the individual.[20] 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.[21]

Created or Received by a Covered Entity

Health information that is "created or received by a covered entity" is protected under the rule.[22] 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.[23]

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 Sections IV and V 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.[24]

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 treatment or health care products directly 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.[25]
- 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: with whom information is being shared; how it is to be used and disclosed; and 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.[26] Small health plans (those with annual receipts of $5 million or less) have an additional 12 months to come into compliance[27] (see Timeline). It should be noted that these deadlines might change if HHS substantively alters the Privacy Rule through official rule-making procedures.[28]

The HHS Office for Civil Rights (OCR) is in charge of ensuring compliance with and enforcing the Privacy Rule.[29] 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.[30]

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.[31] Within its limited resources, OCR intends to continue to provide technical assistance to help covered entities implement the Privacy Rule.[32] 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.[33] 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.[34]
- ***Compliance reviews.*** OCR has the authority to conduct compliance reviews to determine whether covered entities are complying with the requirements of the Privacy Rule.[35]

The rule requires covered entities to cooperate with any resulting investigations.[36] 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).[37] They are also required to provide access to such protected health information and other relevant information as necessary for compliance and investigation purposes.[38]

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. [39] For knowing, wrongful disclosures of health information, a criminal penalty may be imposed.[40] 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 Administrative Simplification provisions of HIPAA, including the Privacy Rule.[41]

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.

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.[42]

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,; or
- It provides greater rights of access or amendment with respect to individuals' access to their own health information.[43]

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 require health plans to report (or to provide access to) information for: management audits; financial audits; program monitoring and evaluation; and licensure or certification for facilities or individuals.

See 45 C.F.R. § 160.203(d).

Complying with Both State and Federal Laws

A health insurer or health care service plan 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 insurers and plans include:

- Confidentiality of Medical Information Act;[44]
- Insurance Information and Privacy Protection Act.[45]
- Knox-Keene Health Care Service Plan Act;[46] and
- Medi-Cal statute and regulations.[47]

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;[48]
- HIV/AIDS tests;[49] and
- Alcohol and drug dependency.[50]

Once a health plan has identified all the state laws that are particularly applicable to it, it 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.

The Federal Privacy Rule has many standards that are similar to those in California privacy laws. When the standards are comparable, plans should follow the "more stringent" standard. For example, under California law, an individual's request for a copy of his health information must be in writing. The Federal Rule permits insurers to have a policy of accepting only written requests for copies so long as the plan gives advance notice of this policy. To comply with both laws, follow the strictest standard—in this case, give notice that only written requests for copies will be accepted.

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.

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 by a California court, licensing body or regulating agency of civil and/or criminal penalties.

Q: Will patients have the right to sue?

A: Yes, in many cases. Many California health privacy statutes (e.g., Insurance Information and Privacy Protection 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 purpose of this guide is to provide a general road map to the combined state and federal requirements that health care plans will have to comply with upon implementation of the Federal Privacy Rule. From the state perspective, this guide focuses on the Insurance Information and Privacy Protection Act, the Confidentiality of Medical Information Act, and the Knox-Keene Health Care Service Plan 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 Insurance Information and Privacy Protection Act

Under the IIPPA, health insurers currently may disclose health information to a third party if the recipient agrees not to further disclose the information. The Federal Privacy Rule takes this requirement one step further, [requiring health insurers] to enter into written contracts.

Background

Existing Requirements in California Law

The Insurance Information and Privacy Protection Act (IIPPA) applies (with some exceptions) to anyone engaged in the business of insurance. Among others, it covers commercial health insurers as well as fraternal benefit society plans.[51] In general terms, the IIPPA regulates the collection, use, and disclosure of a broad range of "personal information," including health information, gathered in connection with insurance transactions.[52] It generally prohibits disclosing health information unless the insurer either has the individual's written authorization or the disclosure is for a purpose specifically permitted by the statute. In addition to restricting disclosures, the IIPPA gives individuals rights with respect to their health information, including the right to see, copy, and amend their own information. It also requires health insurers to provide individuals with a notice describing how their information may be collected and shared.

Similarities between California Law and the Federal Privacy Rule

The framework of the Federal Privacy Rule is fairly similar to the IIPPA, although it applies to a narrower category of information—individually identifiable *health* information.[53] It generally prohibits using or sharing health information without the individual's permission unless the purpose for the disclosure is specifically permitted by the rule. When disclosure is permitted without the individual's permission, the Privacy Rule generally imposes conditions specific to the purpose for which the health information is being used or released. If a purpose is not specified in the regulation, the insurer must obtain an individual's authorization prior to using or disclosing the health information. And like California law, the Federal Privacy Rule gives individuals the right to see, copy, and amend their health information.

Key Differences between California Law and the Federal Privacy Rule

The Federal Privacy Rule, however, does significantly differ from California law in the following key areas:

- Health insurers will be required to have contracts with those they share information with for administrative or business functions that will require those "business associates" to adequately safeguard the health information;
- In many circumstances, health insurers will be required to limit the health information they request, use, or disclose to the minimum amount necessary to accomplish the intended purpose;
- Health insurers will be prohibited from requiring patients to provide access to psychotherapy notes as a condition of enrollment or payment of a claim.
- Health insurers will be required to undertake additional administrative duties to comply with the Privacy Rule, such as training, designating a privacy official, and designing new notice and authorization forms.

These key differences, as well as the regulations that govern obtaining, using, and disclosing health information for particular purposes, are discussed below.

Restrictions on Use and Disclosure of Health Information

The Federal Privacy Rule establishes some use and disclosure restrictions that are generally applicable in most circumstances. It also establishes rules that apply when health information is used or shared for specific purposes.

Minimum Necessary Standard

The IIPPA generally limits the amount of health information that a health insurer can disclose to what is "reasonably necessary" for the specified purpose.[54] Health insurers will be required to adhere to a stricter standard under the Federal Privacy Rule. The Privacy Rule requires covered entities, including health insurers, to request, use, and disclose the minimum amount of health information necessary to accomplish their goals. This is known as the "minimum necessary" standard. This standard does *not* apply to disclosures to or requests by a health care provider for treatment purposes.[55]

Minimum Necessary vs. HIPAA Transaction Standards

Under the HIPAA transaction standards, covered entities who process health claims-type information electronically will be required to use a set format that includes certain data elements. For example, health insurers will be required to accept health claims that are electronically submitted in the standard format.

Q: How will the minimum necessary standards 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. However, to the extent providing information on a standard form is *discretionary,* a covered entity may conduct a minimum necessary analysis to determine whether providing such optional information is necessary to accomplish the intended purpose. *See* HHS Guidance.

The Privacy Rule is intended to make health insurers evaluate their privacy practices and improve them as needed to prevent unnecessary or inappropriate access to protected health information.[56] For most routine purposes, the Privacy Rule requires that health plans have policies and procedures to request, use, and share the minimum amount of health information necessary to accomplish the intended purpose. As a general rule, health insurers are not required to conduct a case-by-case review.

Uses. For uses (i.e., utilizing or sharing health information within an entity), a health insurer must identify those within the organization who need access to health information, the categories or type of information they need, and conditions appropriate to such access.[57] The health insurer must develop policies and procedures that implement this analysis and must document them in written or electronic form.[58]

Disclosures and requests for disclosures. For routine or recurring requests and disclosures, a health insurer's policies must limit the protected health information disclosed or requested to the minimum amount necessary for that particular type of disclosure or request.[59] These policies must also be maintained in written or electronic form.[60]

A health insurer is limited in the type and amount of information it can request for payment purposes? This limitation, however, should not interfere with normal business practices. The minimum necessary standard *does* apply to requests for payment purposes. "Payment," however, is broadly defined in the Privacy Rule and, among other things, includes:

- Determination of eligibility or coverage (including coordination of benefits or the determination of cost-sharing amounts);
- Risk-adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and
- Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services.

Preparing to Implement the Privacy Rule: Key Questions

Perform a "health information" audit, answering some of these key questions:

Who has access to health information within the organization?

Who should have access to this information?

What type and amount of health information are reasonably necessary for them to accomplish their 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)?

From whom does the health insurer request health information on a regular basis?

What types of health information are requested?

Is all the requested information necessary for the intended purpose of the information?

Business Associates: Sharing Health Information for Administrative Purposes

Health insurers may routinely hire other companies and consultants to perform a wide variety of functions for them. Insurers, for example, may work with outside attorneys and accountants. Under the IIPPA, health insurers currently may disclose health information to a third party to enable it to perform a business, professional or insurance function on the insurer's behalf, if the recipient agrees not to further disclose the information.[61]

The Federal Privacy Rule takes this requirement one step further. Health insurers that wish to use outside sources to perform these types of administrative functions will be required to enter into written contracts ensuring that the recipient of the information (a "business associate") appropriately safeguards the health information.[62]

Definition of "business associate." Under the Privacy Rule, anyone who performs a function involving the use of health information on behalf of a covered entity, including a health insurer, or who furnishes certain services (such as legal, actuarial, or other administrative services) to the insurer is a "business associate."[63]

A key element of being a business associate is that the person or organization receives health information either from or on behalf of a health insurer. Under this standard, a billing agency would be a business associate, while a supplier of paper products would not. The rule is not intended to cover those who merely act as a conduit for protected health information, like the U.S. Postal Service or FedEx.[64]

A health insurer can be a business associate of another covered entity. When the health insurer performs functions or provides services in addition to or not directly related to the provision of insurance, the insurer is a business associate with respect to those additional functions or services.[65] For example, when an insurer acts as a third party administrator for a self-funded group health plan, it is a business associate of the group health plan.

Violation of Contracts

Q: Can a health insurer be held responsible if a business associate violates its contract?

A: Only if the health insurer knew the business associate was materially violating its contractual duty to safeguard health information and did nothing about it. An insurer 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 health insurer is required to either: (1) terminate the contract if feasible; or (2) if termination of the contract is not feasible, report the problem to the U.S. Department of Health and Human Services.

45 C.F.R. § 164.504(e).

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 business associate contract must provide that the business associate will:[66]

- 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.

Information Obtained for Underwriting

Often a health plan will receive health information for the purpose of underwriting, premium rating, or other similar activity related to creating or renewing a health insurance contract without the individual's authorization.

Q: What happens to this information if the insurance contract is never placed? Can the health plan still use or share the health information?

A: No. This information generally may not be used for any other purpose without the individual's authorization.

45 C.F.R. § 164.514.

Uses and Disclosures That Do Not Require an Individual's Written Permission

Both the IIPPA and the Federal Privacy Rule allow a health insurer to use and disclose health information without the individual's written permission in a number of circumstances.[67] 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 are permitted without any patient permission and the details of the related conditions, only a few of these purposes are discussed.[68]

Treatment, payment and health care operations. The IIPPA allows health plans to disclose health information without the individual's written authorization for a number of purposes, including:[69]

- To determine an individual's eligibility for an insurance benefit or payment;
- To a medical care institution or medical professional for the purpose of verifying insurance coverage or benefits;
- To a medical care institution for the purpose of informing the individual of a medical problem of which the individual might not be aware;
- To other insurance institutions to allow either the disclosing or receiving institution to perform its function in connection with an insurance transaction;
- To detect or prevent fraud;
- To provide customer service;[70]
- To carry out business planning and development; [71] and
- To conduct legal services.[72]

After implementing the Federal Privacy Rule, health insurers will still be able to disclose health information without the individual's written permission for these purposes. The Federal Rule allows health plans, including health insurers, to use and disclose protected health information without the individual's written permission for purposes of treatment, payment, or health care operations.[73] All of the above purposes are considered to be treatment, payment, or health care operations functions under the Federal Rule.[74] (It should be noted that even though a health insurer can disclose health information without the individual's permission for these purposes, it may only do so in certain circumstances if a business associate contract is in place. See discussion about business associates above.)

In contrast, health care *providers* must obtain a patient's consent prior to using health information for treatment, payment, or health care operations purposes, under the Federal Privacy Rule.[75]

Web Sites

A health insurer that has a website that provides information about its customer services must post its notice of privacy practices on its site in such a manner that people are able to download it.

45 C.F.R. § 164.520(c).

Restrictions on Use of Social Security Numbers

Health insurers and health care service plans should be aware of a recently-enacted California law that restricts the use of social security numbers. Under the state law, health insurers, health care service plans, and others may not engage in any of the following activities:

- Publicly posting or publicly displaying an individual's social security number;
- Printing the individual's social security number on any card required for the individual to access products or services (such as a health plan identification card);
- Requiring the individual to transmit his or her social security number over the Internet unless the connection is secure or the social security number is encrypted;
- Requiring an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number is also required to access the Web site; and
- Printing an individual's social security number on any materials (such as explanation of benefits forms), unless required by state or federal law.

The use of social security numbers for internal verification or administrative purposes is permitted. There are staggered compliance dates for these various requirements, the earliest being January 1, 2003. *See* Cal. Stats. 2001 ch 720, adding Section 1798.85 to the Civil Code.

Right to request heightened protections in the context of treatment, payment, and health care operations. Although health insurers are not required to obtain written permission to use or disclose an individual's health information for treatment, payment, or health care operations purposes, this does not mean that the individual has no right whatsoever over the information. The Federal Privacy Rule gives individuals the right to request heightened protections in two manners: (1) by asking that a health insurer restrict its uses and disclosures, and (2) by asking that an insurer send communications by specific means.[76] These rights were crafted, at least partially, in response to requests from advocacy groups representing those with sensitive medical conditions.

- ***Right to request restrictions.***[77] Individuals have the right to request that covered entities, including health insurers, restrict how they use or share protected health information for the purposes of treatment, payment, and health care operations. Health insurers are not required to agree to requests to restrict, but are bound by any agreements to which they agree.
- ***Right to Request Confidential Communications.***[78] Some individuals are concerned about receiving information about their health treatment or payment at home. Under the Federal Privacy Rule, they will have the right to request that covered entities, including health insurers, contact them only in a specified manner (such as telephoning them only at work) or sending communications only to a specific location. A health insurer must agree to such a request if the individual clearly states that the disclosure of the protected health information could endanger him or her.

Law enforcement. The IIPPA permits a health insurer to disclose health information "as required by law."[79] The Federal Privacy Rule does not change this standard but does specifically limit permitted disclosures to the health information that is relevant to the requirements of the law.[80]

Civil discovery. A health insurer may disclose protected health information in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order without the individual's authorization only when the insurer has received certain assurances.[81] In particular, the party seeking the information must provide a written statement that it has made reasonable efforts to ensure that the individual who is the subject of the information has been given notice of the request and a chance to object to it. Alternatively, the requester must present documentation that it has sought a protective order.

Marketing[82]

A health insurer may use or disclose health information for marketing purposes without the individual's written permission depending on who is actually performing the marketing activities. The Federal Privacy Rule requires a health plan to obtain an individual's authorization prior to:

- Selling protected health information to a third party for its use and re-use; and
- Disclosing protected health information to a third party for the third party's own, independent marketing use.

However, the Privacy Rule permits a health insurer to use or disclose health information for marketing purposes without the individual's authorization if the following conditions are met:

- The health insurer uses or discloses health information only to market health-related products and services on its own or a third party's behalf;
- The information is only disclosed to a business partner that assists the insurer with such communications; and
- The marketing communication contains required information, including details on how the individual may opt out of receiving future marketing communications.

Authorizations

Currently, under the IIPPA, if a disclosure is not specifically permitted or required by the statute, a health insurer must obtain a patient's authorization prior to disclosing his or her health information.[83] The Federal Privacy Rule takes a similar approach. For purposes that are not expressly addressed in the Federal Privacy Rule, covered entities, including health insurers, will be required to obtain a patient's authorization prior to using or disclosing his or her protected health information.[84]

For example, the Federal Privacy Rule permits providers to disclose protected health information to a health insurer for enrollment purposes only pursuant to a written authorization of the individual.[85] An insurer may, however, condition enrollment on the enrollee's providing such an authorization form.[86]

Existing requirements for authorizations under IIPPA. The IIPPA provides for two different types of authorization forms. A detailed authorization form is used when disclosure is sought by an insurer, agent, or insurance support organization, and an abbreviated form is used when disclosure of information is sought by parties other than insurers, agents, or insurance support organizations. The abbreviated form, which had minimal requirements, will no longer be acceptable upon implementation of the Federal Privacy Rule.[87] Rather, the authorization will have to comply with the detailed elements of an authorization form as required by the Federal Privacy Rule, plus any additional requirements of the IIPPA.

Essential elements of authorization submitted by those other than insurance organizations (IIPPA and Federal Privacy Rule). In order to comply with *both* the IIPPA and the Federal Privacy Rule, an authorization form that is submitted by someone other than an insurer, insurance agent, or insurance support organization must, at a minimum:

- Be written in plain language;[88]
- Be separate (with some exceptions);[89]
- Be signed and dated;[90]
- Specifically describe the health information to be used or disclosed;[91]
- State the name or function of the person (organization) authorized to make the disclosure;[92]
- State the specific date or event after which the insurer is no longer authorized to disclose the information; this date may not exceed one year after the date the authorization was originally obtained;[93]

- State the names or functions of persons (organizations) authorized to use or receive the information;[94]
- Inform the individual of his or her right to revoke the authorization under the Federal Privacy Rule; and[95]
- 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.[96]

Authorizations submitted by insurers, insurance agents, or insurance support organizations. Authorizations submitted by insurers, insurance agents or insurance support organizations must have all the above elements. In addition they must:[97]

- Specify the purpose for which the information is being disclosed;
- State that they are effective for the term of the coverage (in lieu of expiring in one year); and
- Advise the individual of his or her right to receive a copy of the authorization.

If an authorization is requested by a health insurer for its own use or disclosure of health information that it maintains, the authorization form must include additional elements. Among other things, such an authorization must:[98]

- If applicable, state that the covered entity 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 health insurer that obtains an authorization for its own uses or disclosures must give the individual a copy of the signed authorization.[99]

Revocation of authorizations.[100] An individual has the right to submit a written revocation of his or her authorization at any time. A revocation is not effective, however, to the extent that a covered entity has taken action in reliance on it. Neither is a revocation effective with respect to authorizations that were obtained as a condition of providing insurance coverage when other laws provide the insurer with the right to contest a claim under the policy.

Disclosures to Sponsors of Group Health Plans

Under California law, health insurers that issue coverage to group health plans generally are prohibited from sharing identifiable health information with the sponsors of the plan without the individual's authorization.[101] Since this standard is more stringent than the Federal Privacy Rule, it will remain in place.[102] Health insurers may, however, disclose "summary health information" to a plan sponsor to permit the plan sponsor to solicit premium bids for providing health insurance coverage under the group health plan or for the purpose of modifying, amending, or terminating the group health plan.[103] "Summary health information" is information that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan from which certain identifiers (such as name, social security number, birth date [except year] and others) have been removed.[104]

Health insurers that act as third party administrators for self-insured group health plans will be constrained in disclosing health information to plan sponsors through general restrictions in the business associate contracts they have with group health plans.[105]

Information Related to Psychotherapy

Information related to psychotherapy is given heightened protection by both California law and the Federal Privacy Rule. The rules vary depending on the specific type of psychotherapy-related information being sought.

Psychotherapy-related information other than notes of a therapy session. If a health insurer wishes to obtain psychotherapy-related information (other than psychotherapy notes) from a provider, under the CMIA the insurer must submit a detailed, written request to that provider.[106] The request must include: (1) the specific information related to psychotherapy treatment that is being requested; (2) the specific intended use of the information; (3) how long the information will be used; and (4) other information. The patient's signature is not required on the request, but he or she must be provided with a copy.[107] For example, a health insurer desiring information about a diagnosis related to psychotherapy would need to submit to the provider a written request specifically detailing the information it desires.

Psychotherapy notes. The Federal Privacy Rule imposes even more restrictions on the disclosure of psychotherapy notes (i.e., notes documenting or analyzing the contents of conversations taking place during therapy).[108] A request under the CMIA will not be sufficient for obtaining these notes. Rather, a health insurer wishing to obtain this information must submit to the provider a detailed authorization form signed by the patient that specifically permits the use or disclosure of psychotherapy notes. Perhaps most importantly, health insurers are prohibited from conditioning enrollment or payment of claims on a patient's signing such an authorization to disclose psychotherapy notes.[109]

Patient Rights

In addition to imposing restrictions on how health insurers 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, and essentially give patients the right: (1) to know how their information is being used; (2) to know with whom it is being shared; (3) to review their information, and (4) to amend it, if necessary.

Notice of Privacy Practices

Those subject to the IIPPA should already be familiar with furnishing notices of information practices to applicants and policyholders with respect to their personal information.[110] A notice of information practice under the IIPPA must specify the source and type of information an insurer collects about an individual. Additionally, the notice must inform individuals of disclosures that the insurer is permitted to make without the individual's written authorization. It must also advise individuals of their rights to see, copy, and correct their personal information.

The Federal Privacy Rule will require health insurers to provide similar notices specifically describing their privacy practices with respect to protected health information. We anticipate that most health insurers will use separate notices to fulfill their requirements under the IIPPA and the Federal Privacy Rule since there are different events that trigger when the notices must be provided. In addition, the content elements of the notices differ substantially.[111]

Health insurers must give the privacy notices required by the Federal Privacy Rule to existing members no later than April 14, 2003 (April 14, 2004 for small plans). After this date, new enrollees must be given the notice at the time of enrollment.

Contents of a notice of privacy practice. 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:[112]

- Be written in plain language;
- Contain a prominent statement that the notice is about how medical information may be used and disclosed;
- Describe how the insurer 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 an insurer is permitted to make under the Privacy Rule for treatment, payment, and health care operations purposes;
- 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 of how they may obtain access to their health information, including obtaining copies;
- Include information about how individuals can file complaints about privacy matters with both their health care service plan 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. Health insurers subject to the IIPPA should already be familiar with providing enrollees access to their own personal information, including health information. The IIPPA also requires health insurers to permit individuals to see, copy, and correct or amend their health information.[113]

New requirements. The Federal Privacy Rule has a similar regulatory scheme. It requires covered health insurers to permit individuals to see and copy their health information that is in a "designated record set," a term that includes (with respect to plans) enrollment, payment, claims adjudication, and case or medical management record systems.[114] The Privacy Rule also grants individuals 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 the IIPPA.

Interplay between state and federal requirements. The net result of the interplay between state and federal patient access provisions is that, for the most part, health insurers who already comply with the state statute will not be required to substantially change their practices with the implementation of the Federal Privacy Rule. We will note the changes that will be necessary in the following discussion.

Scope. Under the IIPPA, an individual generally has the right to see and copy his or her own health information that is reasonably retrievable.[115] The Federal Privacy Rule gives individuals the similar right to see and copy their health information that is in the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.[116] Since records in these systems should be reasonably retrievable, the Privacy Rule generally does not appear to change the scope of information that must be made available to a person.

The one exception to this rule appears to be in the area of "privileged information." Under the IIPPA, the individual does not have a right of access with respect to "privileged information, " which is defined in IIPPA as information collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceedings. [117]

The Federal Rule has a similar, but narrower, exclusion. The Federal Rule excludes access to information compiled in reasonable anticipation of civil, criminal, or administrative actions. It does not appear to exclude access to information compiled in connection with or in reasonable anticipation of a claim for insurance benefits.[118] Therefore, health insurers will be required to provide access to this type of information after implementation of the Federal Privacy Rule

Requests. Under state law, an individual's request to inspect or copy his or her health information must be in writing.[119] The Federal Privacy Rule will allow this practice to continue so long as the plan has given the individual notice that it only accepts written requests.[120] The health insurer should require the individual to provide reasonable verification of identity before responding to the request.[121]

Time limits. A health insurer must generally respond to a request to see or copy health information within 30 days of receiving a request.[122] If an insurer cannot comply within this time frame, it may extend the response time until no more than 30 business days after receipt, if it notifies the individual of the delay.[123] Within the deadline, a health insurer must tell the individual the nature and substance of information they hold and must permit the person to see and copy the information in person or to obtain a copy by mail.[124]

Format of information. If the information is in coded form, a written accurate translation in plain language must be provided.[125]

Fees. Under the IIPPA, a health insurer was allowed to charge a "reasonable" fee to cover the costs incurred in providing a copy of health information to individuals. The Federal Privacy Rule specifies that those fees are limited to the cost of supplies and labor for copying, as well as postage.[126] Charging fees for retrieving and handling the information or for processing the request, however, is prohibited.[127]

Denying patients access. Under the IIPPA, the main category of health information that health insurers may deny access to (other than "privileged information"[128]) appears to be mental health record information. Under the IIPPA, a health insurer may not supply mental health record information directly to the individual without the approval of the qualified treating professional.[129]

The Federal Privacy Rule will alter this procedure. Under the federal rule, health insurers will no longer be able to deny access to mental health records by merely relying on the treating professional's say-so. There will have to be a professional determination that access to the information is reasonably likely to endanger the life or physical safety of the individual or another person.[130]

Individuals denied access to their health information by a health insurer have a right to have that decision reviewed under the Federal Privacy Rule.[131] A health insurer must give patients 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 individual requests a review, the health insurer must promptly refer the material to a licensed health care professional who did not participate in the original decision. The reviewer, who is selected by the health plan, makes a binding determination whether to grant or deny access.

Accounting of disclosures. When responding to a request for access to personal information under the IIPPA, a health insurer is already required to give individuals the identity, if recorded, of those persons to whom the plan has disclosed personal information, including health information, within the prior two years.[132] The Federal Privacy Rule expands on this requirement.

Under the accounting provisions of the Privacy Rule, within 60 days of receiving a request, health insurers will be required to give the patient a list of disclosures made within the past six years.[133] 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 health insurer's own organization). Additionally, the accounting provisions do not apply to any disclosures that are made for treatment, payment, or health care operations purposes. Health insurers will, however, be required to account for other disclosures that they may routinely make, such as those made to researchers and to health oversight agencies.

Amendment. The IIPPA contains a comprehensive framework granting individuals the right to request that health insurers correct, amend, or delete personal information, including health information, that the insurer maintains.[134] Because the IIPPA provides individuals greater rights of access and amendment than the Federal Privacy Rule, the new federal rule will have little impact on the state law.[135]

After implementation of the Federal Privacy Rule, individuals will continue to have the right to request that health insurers correct, amend, or delete health information.[136] Plans will have 30 business days to respond to these requests.[137] The steps that insurers must take if they either accept or deny the request remain essentially the same. Among other things, a health insurer must:

- Notify the individual, in writing, whether it has accepted or denied the request;
- If the request is accepted, make the requested change and inform third parties designated by the individual; and
- If the request is denied, afford the individual the opportunity to submit a statement in disagreement, and provide the statement not only in conjunction with subsequent disclosures of the contested information, but also to those designated by the individual as having received the contested information in the past two years.

Administrative Requirements for Health Insurers

The Federal Privacy Rule will impose a number of administrative requirements on all covered health insurers. For the most part, these requirements are fairly general. HHS, recognizing that there are vast differences in the nature, size, and organization of health insurers, 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 insurer's circumstances.[138] Some of the major administrative requirements are listed below.

Policies and Procedures

Health insurers must develop and implement policies and procedures for using and maintaining health information in compliance with the Privacy Rule.[139] 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 health insurer 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.[140] Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and using passwords for access to computers that contain identifiable health information.[141] HHS has emphasized that this rule requires only "reasonable efforts" to protect health information.

Training

A health insurer 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 with the regulation. New members of the workforce should receive training within a reasonable period of time after they begin working.[142] Again, training requirements are flexible and scalable and will vary with the size of the organization.

Privacy Officer and Contact Person

The Federal Privacy Rule requires a health insurer to designate a privacy official for the development and implementation of its policies and procedures.[143] In addition, a health insurer will be required to identify a contact person who is responsible for receiving complaints.[144] At its option, the insurer can designate one person for both functions.[145]

Complaint Procedure

Health insurers must establish a process for individuals to file complaints about the insurer's health privacy policies and practices and its compliance with the Federal Rule.[146]

Documentation

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

- Authorizations;[147]
- Consents, if they elect to use them;[148]
- Agreed restrictions on using or disclosing health information for treatment, payment and health care operations;[149]
- Disclosures for purposes other than treatment, payment, or health care operations;[150]
- Minimum necessary policies for use and disclosure of health information;[151] and

n Training of personnel.[152]

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.[153]

Looking Ahead

Clearly, the new Privacy Rule will require health insurers 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 insurer and doing a line-by-line comparison of these state requirements with those of the Privacy Rule. Insurers 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 insurers to complete the changes they will need to make and it is incumbent upon insurers to use this period wisely.

V. The Impact on Knox-Keene Health Care Service Plans

Because the state law [Knox-Keene] does not contain procedural requirements specifying when and how individuals must be given access to their own health information, health care service plans had a lot of discretion in this area… The Federal Privacy Rule… requires covered health plans to permit individuals to see and copy their health information… [and] grants individuals the right to request amendments.

Background

Over 23 million Californians receive their health care through health care service plans (popularly known as HMOs or managed care plans).[154] Most of these plans are licensed under the Knox-Keene Health Care Service Plan Act (Knox-Keene Act).[155]

Existing Requirements in California Law

These plans should already be familiar with state laws governing the use and disclosure of health information. Knox-Keene plans are subject to the Confidentiality of Medical Information Act (CMIA), which restricts how health care service plans may disclose their enrollees' and subscribers' "medical information."[156] CMIA covers individually identifiable information regarding a patient's medical history, mental or physical condition, and 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 or physical form.

Generally, the CMIA prohibits a health care service plan from disclosing medical information without a patient's written authorization.[157] 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 service plan must obtain a patient's authorization prior to disclosure. The Act sets out the form and substance for such authorizations.[158]

In addition to restricting the disclosure of medical information, California law (through the Knox-Keene Act) also requires health care service plans to have policies permitting patients access to their own medical records.[159] Furthermore, plans must provide individuals with a written statement describing how the plan maintains the confidentiality of medical information in their possession.[160]

New Requirements

The Federal Privacy Rule adopts a similar scheme: it permits health care service plans to use and disclose protected health information for specified purposes without the individual's written permission. To disclose health information for purposes not specified in the regulation, an authorization is required. Additionally, the Federal Privacy Rule grants patients the right to see and copy their own health information.

Key Differences between California Law and the Federal Privacy Rule

While the Privacy Rule is similar in many respects to the CMIA, there are some key areas where health care service plans will have to alter their practices under the Federal Privacy Rule, including:

- Health care service plans will be required to have contracts with those they share information with for administrative functions; the contracts will require those "business associates" to adequately safeguard the health information.
- In many circumstances, health care service plans will be required to limit the health information they request, use, or disclose to the minimum amount necessary to accomplish the intended purpose.
- Health care service plans will be required to provide individuals with a notice of privacy practices by April 14, 2003; after that date, new enrollees must receive notice at the time of enrollment.
- Having a general policy for allowing individuals access to their own health information will no longer be sufficient. Health care service plans will be required to follow a detailed set of regulatory provisions for permitting access.
- Individuals will now have the right to request that health care service plans amend their health information if it is incorrect.
- Health care service plans 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.

These key differences, as well as the rules that govern obtaining, using, and disclosing health information for particular purposes, are discussed below.

Restrictions on Use and Disclosure of Health Information

Oral Communications

Health care service plans must already comply with the CMIA, which governs the disclosure of medical information in electronic or physical form.[161] Although the CMIA does not expressly cover oral information, many health care service plans already have internal policies governing whom they may share information with orally. For example, many health care service plans have specific rules limiting who may be furnished claims information over the telephone. The Federal Privacy Rule formalizes these practices by covering health information transmitted or maintained in any format, including oral communications.[162]

Medi-Cal Requirements

A commercial health care service plan that contracts with either the state or a county to provide Medi-Cal services must comply with the Privacy Rule. In addition it must also adhere to Medicaid specific confidentiality requirements contained in the following sources:

- Its contract with the government agency
- The Federal Medicaid Regulations (Title 42, Code of Federal Regulations, Section 431.300 et seq.), and
- Section 14100.2 of the California Welfare and Institutions Code, and the related regulations.

In very general terms, these standards prohibit the disclosure of protected health information generated in connection with Medi-Cal services for any purpose not directly connected with the administration of the Medi-Cal program. Because the Medi-Cal standards for use and disclosure are more restrictive than the Privacy Rule, they will not be preempted by the Federal rule. It should be noted, however, that Medi-Cal patients will have the right to see, copy and amend their own health information, (including claims information).*

*The Federal Medicaid regulations (both those finalized and on hold, and those proposed) require states to ensure through their contracts that managed care plans establish and implement procedures to ensure that enrollees can request to see, receive a copy of, and request an amendment of their records. See 42 C.F.R. § 438.224(d) and 66 Fed. Reg. 43670 (Aug. 20, 2001) (notice of proposed rule making).

Minimum Necessary Standard

California law currently limits the amount of health information that can be disclosed in certain circumstances. For example, a provider may disclose health information to a health care service plan for payment purposes only to the extent necessary to allow responsibility for the payment to be determined and payment to be made.[163]

The Federal Privacy Rule builds on these existing rules and policies. The Privacy Rule is intended to make covered entities, including health care service plans, evaluate their privacy practices and improve them as needed to prevent unnecessary or inappropriate access to protected health information.[164] As a general rule, they do not require a case-by-case review.

For most routine purposes, the rule requires that health care service plans have policies and procedures to request, use, and disclose the minimum amount of health information necessary to accomplish the intended purpose. It is important to note that 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.[165] Neither does it apply to any use or disclosure that is required by law.[166]

Uses

For uses (i.e., utilizing or sharing health information within an organization), a health care service plan must identify those within their organization who need access to health information, the categories or type of information they need, and conditions appropriate to such access.[167] The health care service plan must develop policies and procedures that implement this analysis and must document them in written or electronic form.[168]

Disclosures and Requests for Disclosures

For routine or recurring requests for health information, a plan's policies must limit the protected health information requested to the minimum amount necessary to accomplish the use for which the information is requested.[169] The same standard applies to routine disclosures of health information—the plan is required to have policies in place that limit the type and amount of health information disclosed to the minimum amount necessary. These protocols must be maintained in written or electronic form.[170]

Uses, Requests, and Disclosures That Are Not Routine or Recurring

Most uses, requests, and disclosures that are out of the ordinary must be reviewed on an individual basis to determine the minimum amount necessary to fulfill the intended purpose. For certain requests, a health care service plan can rely on the requesters' representation that they have asked for the minimum amount of information necessary. For example, a health care service plan could rely on the representation of an attorney or other professional that he or she has requested the minimum amount of information necessary to provide a professional service.[171]

Limits on Requests

Health care service plans are limited in the type and amount of information they can request for payment and health care operations, but this limitation should not interfere with normal business practices. The minimum necessary standard does apply to requests for payment and health care operations purposes. However, the terms "payment" and "health care operations," are broadly defined in the Privacy Rule and, among other things, include:

- Determination of eligibility or coverage (including coordination of benefits or the determination of cost-sharing amounts);
- Risk-adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services;
- Contacting health care providers and patients with information about treatment alternatives;
- Evaluating practitioner and provider performance; and
- Conducting quality assessment and improvement activities.

Business Associates: Sharing Health Information for Administrative Purposes

Existing requirements. Health care service plans routinely hire other companies and consultants to perform a wide variety of functions for them. Plans, for example, may work with outside attorneys, accountants and bill collectors. Under the CMIA, health care service plans 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.[172]

New requirements. The Federal Privacy Rule takes this requirement one step further. Health care service plans that wish to use outside sources to perform these types of administrative functions will be required to enter into written contracts ensuring that the recipient of the information (a "business associate") appropriately safeguards the health information.[173] This may be a major change for many health care service plans.

Can a Health Plan Be Held Responsible if a Business Associate Violates its Contract?

Only if the plan 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.

See 45 C.F.R. § 164.504(e)(1(ii).

Definition of a "business associate." Under the federal regulation, anyone who performs a function involving the use of health information on behalf of a health care service plan or who furnishes certain services (such as legal, actuarial, or other administrative services) to the plan is a "business associate."[174] 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 also not intended to cover those who merely act as a conduit of protected health information, like the U.S. Postal Service or FedEx.[175]

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 business associate contract must provide that the business associate will:[176]

- 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;
- 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.

Uses and Disclosures That Do Not Require an Individual's Written Permission

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.[177] 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 are permitted without any patient permission and the details of the related conditions, only a few of these purposes are discussed.

Treatment, payment and health care operations. The CMIA allows health care service plans to disclose health information without the individual's written authorization for a number of purposes, including:[178]

- To providers of health care, health care service plans, contractors, or other health care facilities for purposes of diagnosis or treatment of the patient;
- To any person or entity responsible for paying for health care services rendered to the patient, to the extent necessary to allow responsibility to be determined and payment to be made;
- For billing, claims management, medical data processing, or other administrative services;
- To review health care services with respect to medical necessity, level of care, quality of care, or justification of charges; and
- For licensing and accrediting the health care service plan.

After implementing the Federal Privacy Rule, health care service plans will still be able to disclose health information without the individual's written permission for these purposes. The Federal Rule allows health plans, including health care service plans, to use and disclose protected health information without the individual's written permission for the core purposes of treatment, payment, and health care operations.[179] And all of the above purposes are considered to be treatment, payment, or health care operations functions.[180] (It should be noted that even though a health insurer can disclose health information without the individual's permission for these purposes, it may only do so in certain circumstances if a business associate contract is in place. (See "business associates," above.)

In contrast, health care providers must obtain a patient's consent prior to using health information for treatment, payment and health care operations purposes, under the Federal Privacy Rule.[181]

Health plans will still be able to use health information that they obtain from providers to administer their own plans. Once a provider has obtained a patient's consent, the provider may disclose health information to a health care service plan for payment purposes. The plan may then use this information without the patient's express permission for its own payment and health care operations purposes.[182]

Right to request heightened protections in the context of treatment, payment, and health care operations. Although health care service plans are not required to obtain written permission to use or disclose an individual's health information for treatment, payment, or health care operations purposes, this does not mean that the individual has no right whatsoever over the information. The Federal Privacy Rule gives individuals the right to request heightened protections in two manners: (1) by asking that a health plan restrict its uses and disclosures and (2) by asking that a plan send communications by specific means.[183] These rights were crafted, at least partially, in response to requests from advocacy groups representing those with sensitive medical conditions.

- ***Right to request restrictions.*** Individuals have the right to request that covered entities, including health care service plans, restrict how they use or share protected health information for the purposes of treatment, payment, and health care operations. Health care service plans are not required to agree to requests to restrict, but are bound by any agreements to which they agree.[184]
- ***Right to request confidential communications.*** Some individuals are concerned about receiving information about their health treatment or payment at home. Under the Federal Privacy Rule, individuals will have the right to request that covered entities, including health care service plans, contact them only in a specified manner (such as telephoning them only at work) or sending communications only to a specific location. A plan must agree to such a request if the individual clearly states that the disclosure of the protected health information could endanger him or her.[185]

Law enforcement. Under the CMIA and the Federal Privacy Rule, health care service plans may disclose health information pursuant to a search warrant lawfully issued to a governmental law enforcement agency.[186]

Civil discovery. A health care service plan may disclose protected health information in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order without the individual's authorization only when the health plan has received certain assurances.[187] In particular, the party seeking the information must provide a written statement that it has made reasonable efforts to ensure that the individual who is the subject of the information has been given notice of the request and a chance to object to it. Alternatively, the requester must present documentation that it has sought a protective order.[188]

Research. Both the CMIA and the Federal Privacy Rule permit providers to disclose health information for research purposes without the permission of the patient.[189] 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: (1)an Institutional Review Board (IRB), which reviews federally funded research; (2)or a "privacy board," a new board that will review privately funded research using the same principles as an IRB.[190] 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 health plan must obtain a patient's authorization prior to disclosing his or her health information.[191] The Federal Privacy Rule takes a similar approach. For purposes that are not expressly addressed in the Federal Privacy Rule, covered entities, including health care service plans, will be required to obtain a patient's authorization prior to using or disclosing his or her protected health information.[192] The authorization required by the Privacy Rule is quite similar to that provided for in the CMIA, but there are some different requirements.[193]

Essential elements of authorization forms. Most plans will probably prefer that a single authorization form that conforms to both federal and state requirements be submitted. In order to comply with both the CMIA and the Federal Privacy Rule, an authorization form must, at a minimum:

- Be handwritten by the person who signs it or be in 8-point typeface or larger;[194]
- Be separate (with some exceptions);[195]
- Be signed and dated;[196]
- Specifically describe the health information to be used or disclosed;[197]
- State the specific limitations on the type of information to be disclosed;[198]
- State the name or function of the person (organization) authorized to make the disclosure;[199]
- State the specific date after which the health care service plan is no longer authorized to disclose the information;[200]
- State the names or functions of persons (organizations) authorized to use or receive the information;[201]
- State the specific uses and limitations on the use of medical information by the persons authorized to receive the information;[202]
- Advise the individuals of their right to receive a copy of the authorization;[203]
- Inform individuals of their right to revoke the authorization under the Federal Privacy Rule;[204] and
- 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.[205]

When a health care service plan 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:[206]

- If applicable, state that the plan 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 plan that obtains an authorization for its own uses or disclosures must give the individual a copy of the signed authorization.[207]

Revocation of authorizations.[208] An individual has the right to submit a written revocation of his or her authorization at any time. A revocation is not effective, however, to the extent that a covered entity has taken action in reliance on it. Neither is a revocation effective with respect to authorizations that were obtained as a condition of obtaining insurance coverage when other laws provide the insurer with the right to contest a claim under the policy.

Marketing

Among the more controversial aspects of the Federal Privacy Rule are the "marketing provisions." Under these provisions, providers and health plans are permitted to use health information for marketing purposes (for their own services 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.[209] This essentially gives the health plan one chance to send the patient marketing materials before the patient is even given the opportunity to object.

Health care service plans in California, however, should be aware that the CMIA appears to require a patient's written authorization before engaging in many marketing activities.[210] Because this standard is more consumer-protective than the federal regulation, the state law will remain in effect, and health care service plans should get patients' written authorization before using or sharing their health information for marketing.

Information Related to Psychotherapy

Information related to psychotherapy is given heightened protection by both California law and the Federal Privacy Rule. The rules vary depending on the specific type of psychotherapy-related information being sought.

Psychotherapy-related information other than notes of a therapy session. If a health care service plan wishes to obtain psychotherapy-related information from a provider, the plan must submit a detailed, written request (under the CMIA)[211] to that provider.[212] The request must include: (1) the specific information related to psychotherapy treatment that is being requested; (2) the specific intended use of the information; (3) how long the information will be used; and (4) other information. The patient's signature is not required on the request, but he or she must be provided with a copy. For example, a health care service plan desiring information about a diagnosis related to psychotherapy would need to submit to the provider a written request specifically detailing the information it desires.

Psychotherapy Notes. The Federal Privacy Rule imposes even more restrictions on the disclosure of psychotherapy notes (i.e., notes documenting or analyzing the contents of conversations taking place during therapy).[213] A request under the CMIA will not be sufficient for obtaining these notes. Rather, if a health plan wishes to obtain this information it must submit to the provider a detailed authorization form signed by the patient that specifically permits the use or disclosure of psychotherapy notes. Perhaps most importantly, health plans are prohibited from conditioning enrollment or payment of claims on a patient's signing such an authorization to disclose psychotherapy notes.[214]

Patient Rights

In addition to imposing restrictions on how health care service plans can use and disclose protected health information, both California law and the Federal Privacy Rule grant individuals rights with respect to their own health information. These rights are based in fair information practice principles, and essentially give people the right: (1) to know how their health information is being used; (2) to know with whom it is being shared; (3) to review their health information; and (4) to amend it, if necessary.

Notice of Privacy Practices

Currently, health care service plans licensed under the Knox -Keene Act are required, upon request, to give enrollees and subscribers a written statement that describes how the health care service plan maintains the confidentiality of medical information in its possession.[215] If a plan contracts with others to provide health care services, the notice must also describe the contracting organization's privacy practices.[216] Additionally, the notice must contain information about how patients, subscribers and enrollees may obtain access to their medical information, including obtaining copies.[217]

The Federal Privacy Rule requires a similar notice of privacy practices, which must be given to enrollees upon request and at other specified times.[218] Under the Federal Privacy Rule, health care service plans are required to provide a notice of privacy practices to individuals covered by the plan by April 14, 2003 (the compliance deadline for the federal rule).[219] After that date, the notice must be given to new enrollees at the time of their enrollment, and upon request.[220]

We anticipate that most health care service plans will want to use a single notice of privacy practices to comply with both state and federal law. This can be accomplished by crafting a notice that contains the elements required by both state and federal law. Plans should furnish the notice upon request and at the times specified by the Federal Privacy Rule in order to comply with both state and federal law.

Contents of the notice of privacy practice. Generally, a notice of privacy practices must contain all of the specific requirements of the Knox-Keene Act plus the requirements of the Federal Privacy Rule. While the requirements under the Knox-Keene Act are fairly brief, the Federal Privacy Rule is quite detailed in the content requirements for a notice of privacy practices. Health care service plans will need to consult the rule to determine the exact language that a notice requires in order to be in compliance. In order to comply with both laws, a notice of privacy practices generally must:

- Be written in plain language;[221]
- Be in 12-point or larger typeface;[222]
- Contain a heading that the notice is about how medical information may be used and disclosed;[223]
- Advise individuals how they may obtain access to their health information, including obtaining copies;[224]
- Describe how the plan protects health information under the respective laws;[225]
- Describe when health information may be released without the individual's prior authorization;[226]
- Advise individuals that any disclosure of medical information beyond the provisions of law is prohibited;[227]

- Describe the types of medical information that may be collected and the type of sources that may be used to collect the information, and the purposes for which the plan will obtain medical information from other health care providers;[228]
- 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;[229]
- Include information about how an individual can file complaints about privacy matters with both their health care service plan and the Department of Health and Human Services;[230] and
- Provide the name of a contact person for additional information. [231]

Giving Patients Access to Their Own Health Information

Under the Knox-Keene Act, health care service plans currently must have policies and procedures that give individuals access to their own health information that is maintained by the plan.[232] Because the state law does not contain procedural requirements specifying when and how individuals must be given access to their own health information, health care service plans had a lot of discretion in this area. This will change under the Federal Privacy Rule, which contains detailed provisions governing individuals' rights to see, copy, and amend their own health information.

Generally, the Privacy Rule requires covered health plans to permit individuals to see and copy their health information that is in a "designated record set," a term that includes (with respect to plans) enrollment, payment, claims adjudication, and case or medical management record systems.[233] The Privacy Rule also grants individuals the right to request amendments to their health information if it is incorrect or inaccurate.

Scope. In general, individuals will have the right to see and copy their own enrollment, payment, claims adjudication, and case or medical management records maintained by a health care service plan.[234]

Requests. A health care service plan may require that individuals submit their requests to inspect or copy their own medical records in writing, so long as the plan has given notice that it only accepts written requests.[235] The health care service plan should require individuals to provide some reasonable verification of their identity before providing access to the requested information.[236]

Time limit. In general, a health care service plan will have 30 days after receipt to respond to a request to see and copy health information. The deadline may be extended up to 30 days without a reason if the plan notifies the patient.[237]

If the health care service plan does not maintain the requested health information, but knows where the information is kept, the plan must let the individual know where to direct his or her request.[238] (For example, if a person requests a medical record from a health care service plan which does not maintain medical records, and the plan knows that the record is kept by one of its contracting providers, the plan must advise the person to direct the request to the contracting provider.)

Format of information. The health care service plan generally must provide the health information in the format requested by the individual.[239] The plan may give the individual an explanation or summary of the information, instead of the actual record, if the individual agrees in advance.[240]

Fees. A health care service plan may charge a reasonable fee for providing the individual with a copy of health information. The fee can include the cost of supplies and labor for copying as well as postage.[241] Charging fees for retrieving and handling the information or for processing the request, however, is prohibited. [242]

A plan can also charge a reasonable cost-based fee for explaining or summarizing health information when an individual has agreed to an explanation or summary in lieu of the actual record.[243]

Denying patients access. The Federal Privacy Rule permits providers to deny patients access to health information in some circumstances. In some instances the right to deny access is absolute and there is no review process. In others, the patient has the right to have the decision to deny access reviewed.

No right of review. When an individual requests information in the following categories, a health care service plan may deny the request without affording the patient any right of review of the decision.[244]

- Psychotherapy notes;
- Information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding;
- Protected health information maintained by a covered entity that is subject to Clinical Laboratory Improvements Amendments (CLIA) or exempt from CLIA regulations;
- Information obtained from someone other than a health care provider under a promise of confidentiality where access would be reasonably likely to reveal the source of that information.

Right to review. In the following three circumstances, a health care service plan may deny an individual access to his or her protected health information, but must provide an opportunity for review of that denial if:

- A licensed health care professional, in the exercise of professional judgment, determines that it is reasonably likely that access to the requested information would endanger the life or physical safety of the individual or another person;
- The requested information makes references to another person and the licensed health care professional, in the exercise of professional judgment, determines that access is reasonably likely to cause substantial harm to that other person; or
- The request for access is made by the individual's personal representative and a licensed health care professional, in the exercise of professional judgment, determines that providing access to that representative is reasonably likely to cause substantial harm to the individual or another person.

Review of denials. The Federal Privacy Rule creates a framework for reviewing denials of access to health information.[245] As a preliminary matter, when a health care service plan decides to deny access to health information, it must furnish individuals with a written denial in plain language within 30 days of receiving the individual's request. The denial notice must generally explain the basis of the denial and advise the individuals of their right to have this decision reviewed.[246]

If the individual requests a review, the plan must promptly refer the material to a licensed health care professional who did not participate in the original decision.[247] The designated reviewer, who is selected by the plan, makes the final determination whether access should be granted or denied.[248]

Accounting of Disclosures

The Federal Privacy Rule also grants individuals the right to receive an accounting of prior disclosures of health information.[249] Within 60 days of receiving a request, a health care service plan will be required to give an individual a list of disclosures made within the past six years.[250] 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 plan's organization).[251] Additionally, the accounting provisions do not apply to any disclosures that are made for treatment, payment, or health care operations purposes.[252] Plans will, however, be required to account for other disclosures that they may routinely make, such as those made to researchers and to health oversight agencies.

Right to Amend Health Information

The Federal Privacy Rule gives individuals the right to amend or supplement their health information that is maintained by a covered entity, including health care service plans.[253] For example, an individual who disagrees with a medical opinion can submit a second opinion to be included in the medical record. The individual has this right for as long as the health care service plan maintains the information.[254] The plan must act on an individual's request for amendment no later than 60 days after it receives the request.[255] The deadline may be extended up to 30 days.

Accepting requests for amendment. If the health care service plan accepts the request, it must (1) make the appropriate amendment, and (2) inform the individual in a timely fashion that the amendment is accepted. The plan must then furnish the amendment both to entities identified by the individual and to other entities known to have received the erroneous information.[256]

Denying requests for amendment. A health care service plan may deny individual's request for amendment if the plan determines that the information or record: (1) was not created by the plan, unless the originator of the protected health information is no longer available to make the amendment; (2) is not a part of the designated record set; (3) would not be available for inspection (see summary of right of access, above); or (4) is accurate and complete.[257]

If the health care service plan denies an individual's request, it must give the individual a timely, written denial, which 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 health care service plan 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.[258]

If the individual files a statement of disagreement, the covered entity can prepare a rebuttal to the individual's statement. The entity must provide a copy of the rebuttal to the individual. 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.[259]

Administrative Requirements for Health Care Service Plans

The Federal Privacy Rule will impose a number of administrative requirements on health care service plans. 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 plans, 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 plan's circumstances.[260] Some of the major administrative requirements are listed below.

Policies and Procedures

Health care service providers must develop and implement policies and procedures for using and maintaining health information in compliance with the Privacy Rule.[261] 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 health care service plan 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[262]. Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring that file cabinets containing such records be locked.[263]

Training

A health care service plan 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 the compliance date. New members of the workforce should receive training within a reasonable period of time after they begin working.[264]

Again, training requirements are flexible and scalable. For example, a small health care service plan may be able to satisfy the training requirement by providing each new member of the workforce with a copy of the plan's privacy policies and requiring these members to acknowledge that they have reviewed the policy.[265]

Privacy Officer and Contact Person

The Federal Privacy Rule requires a health care service plan to designate a privacy official for the development and implementation of its policies and procedures.[266] In addition, a plan will be required to identify a contact person who is responsible for receiving complaints.[267] At its option, the plan can designate one person for both functions.[268] The implementation of these requirements will depend on the size and organization of the plan's office.

Complaint Procedure

Health care service plans 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.[269]

Documentation

Health care service plans will be required to maintain documentation in a variety of areas including, but not limited to, the following:

- Agreed restrictions on using or disclosing health information for treatment, payment and health care operations;[270]
- Authorizations;[271]
- Disclosures for purposes other than treatment, payment and health care operations;[272]
- Minimum necessary policies for use and disclosure of health information;[273] and
- Training of personnel.[274]

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.[275]

Looking Ahead

Clearly, the new Privacy Rule will require health care service plans 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 plan and doing a line-by-line comparison of these state requirements with those of the Privacy Rule. Health plans 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 plans to complete the changes they will need to make and it is incumbent upon them to use this period wisely.

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. 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.).
2. Standards for Privacy of Individually Identifiable Health Information: Guidance (hereinafter "HHS Guidance") (July 6, 2001). Available online at http://www.hhs.gov/ocr/hipaa/.
3. 45. C.F.R. § 160.102 and § 164.104.
4. 45 C.F.R. § 160.103 (defining "covered entity").
5. 45 C.F.R. § 160.103 (defining "health plan").
6. 45 C.F.R. § 160.103 (defining "health plan").
7. 45 C.F.R. § 160.103 (defining "health care clearinghouse").
8. 45 C.F.R. § 160.102 and § 164.104 (explaining "applicability).
9. 45. C.F.R. § 160.103 (defining "health care provider").
10. 45 C.F.R. § 160.103 (defining "health care").
11. 65 Fed. Reg. 82477.
12. *See* Standards for Privacy of Individually Identifiable Health Information: Proposed Rule, Preamble ("Preamble to Proposed Privacy Rule"), 64 Fed. Reg. 59937 (November 3, 1999).
13. There is some controversy concerning whether a provider must actually use the required format to become a "covered entity" or whether they may become "covered" by merely electronically conducting one of the transactions listed in HIPAA.
14. *See* 42 U.S.C. Sec. 1320d-2(a) for the full list of electronic transactions that will trigger coverage of the privacy regulation.
15. 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).
16. *See* Standards for Privacy of Individually Identifiable Health Information: Final Rule, Preamble ("Preamble to Privacy Rule") 65 Fed. Reg. 82477.
17. 45 C.F.R. § 164.500.
18. 45 C.F.R. § 164.501 (defining "protected health information" and "individually identifiable health information") and § 160.103 (defining "health information").
19. 45 C.F.R. § 160.103 (defining "health information").
20. 45 C.F.R. § 164.501 (defining "individually identifiable health information").
21. 45 C.F.R. § 164.502 and § 164.514.
22. 45 C.F.R. § 164.501 (defining "individually identifiable health information").
23. 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.C). S. Car.) (filed 7/16/01).
24. *See* 45 C.F.R. § 164.501 (defining "use" and "disclosure").
25. 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").
26. Although Congress recently extended the deadline for complying with the transaction standards, it did not alter the deadline for complying with the Privacy Rule. *See* Administrative Simplification Compliance Act, Pub. Law 107-105.
27. 45 C.F.R. § 160.103 (defining "small health plan") and § 164.534 (specifying compliance dates).
28. *See* HHS Guidance at 6-7, stating that HHS intends to alter the rule.
29. Statement of Delegation of Authority, 65 Fed. Reg. 82381 (Dec. 28, 2000).
30. Preamble to Proposed Privacy Rule, 64 Fed. Reg. 6002.
31. *See* HHS Guidance, note 5.

32. *See* HHS Guidance, note 5, at 3; 45 C.F.R. § 160.304 and 65 Fed. Reg. 82603.
33. *See* 45 C.F.R. § 160.310.
34. 45 C.F.R. § 160.306.
35. 45 C.F.R. § 160.308.
36. 45 C.F.R. § 160.310.
37. *See* discussion of documentation requirements in "Administrative Requirements," above.
38. 45 C.F.R. § 160.310.
39. 42 U.S.C. § 1320d-5.
40. 42 U.S.C. § 1320d-6.
41. Preamble to Privacy Rule, 65 Fed. Reg. 82487.
42. 45 C.F.R. § 160.202.
43. 45 C.F.R. § 160.202.
44. Cal. Civ. Code § 56-§ 56.37.
45. Cal. Ins. Code § 791-§ 791.27
46. Cal. Health & Safety Code § 1340-§ 1399.76
47. Cal. Welf. & Inst. Code § 14100.2.
48. The Lanterman-Petris-Short Act, codified at Cal. Welf. & Inst. Code § 5328 et seq.
49. Cal. Health & Safety Code § 120775, § 120975-§ 121020.
50. Cal. Welf. & Inst. Code § 11970.5-§ 11977.
51. Cal. Ins. Code § 791 et seq. The IIPPA applies to a broad category of insurers; however, this discussion is limited to health insurers because only they will be subject to the requirements of the Federal Privacy Rule.
52. "Personal information" is defined as "individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics"). The definition of "personal information" specifically includes "medical record information....Cal. Ins. Code § 791.02 (defining "personal information").
53. *See* 45 C.F.R. § 164.500.
54. Cal. Ins. Code § 791.13.
55. 45 C.F.R. § 164.502(b) (explaining when minimum necessary standard applies).
56. Guidance at 20.
57. 45 C.F.R. § 164.514(d)(2).
58. 45 C.F.R. § 164.530(j).
59. 45 C.F.R. § 164.514(d)(3) and (4).
60. 45 C.F.R. § 164.530(j).
61. Cal. Ins. Code § 791.13(b)(1).
62. 45 C.F.R. § 164.502(e).
63. 45 C.F.R. § 160.103 (defining "business associate").
64. 65 Fed. Reg. 82476.
65. 65 Fed. Reg. 82476.
66. 45 C.F.R. § 164.504(e)(2).
67. *See* generally Cal. Ins. Code § 791.13(b)-(r).
68. It is beyond the scope of this guide to address every circumstance under which disclosure is permitted without the individual's permission. The IIPPA alone lists 18 of these circumstances.
69. Cal. Ins. Code § 791.13(b), (c), (d), and (q).
70. Cal. Ins. Code § 791.13(b) allows insurers to disclose health information to a third party to perform "business, professional or insurance function(s)." This broad provision appears to cover functions such as "customer service" and business planning and development" that would be considered to be treatment, payment, and health care operations under the Federal Privacy Rule. For these functions, no individual authorization would be required. The state provision however appears broad enough to cover other functions that might not come within the definitions of "treatment, payment and health care operations." For these functions, a health insurer would be required to obtain a patient's permission.
71. *See* note 289.
72. *See* note 289.
73. 45 C.F.R. § 164.502(a).
74. *See* 45 C.F.R. § 164.501 (defining these terms).
75. 45 C.F.R. § 164.506(a).
76. 45 C.F.R. § 164.522.
77. 45 C.F.R. § 164.522(a).
78. 45 C.F.R. §164.522(b).
79. Cal. Ins. Code § 791.13(g).
80. 45 C.F.R. § 164.512(a)
81. 45 C.F.R. § 164.512(f).

82. The IIPPA allows an insurer to disclose health information to a third party without an individual's written permission for marketing purposes so long as the individual is given the opportunity to "opt out" of such uses. The third party is permitted to use the information for its own purposes. Cal. Ins. Code § 791.13(k). In contrast, the Federal Privacy Rule would require an individual's written authorization in this scenario. Therefore, the Federal Privacy Rule appears to be more stringent.
83. CITE
84. 45 C.F.R. § 164.
85. Although the Federal Privacy Rule allows providers to disclose health information to insurance companies for health care operations with a general consent form, pre-enrollment underwriting is not considered to be a health care operation of the provider and an authorization to disclose is required. 65 Fed. Reg. 82490
86. 45 C.F.R. § 164.508.
87. *See* Cal. Civ. Code § 56.11.
88. 45 C.F.R. § 164.508(c)(2).
89. *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.
90. Cal. Ins. Code § 791.13 and 45 C.F.R. § 164.508(c)(1).
91. 45 C.F.R. § 164.508(c).
92. 45 C.F.R. § 164.508(c).
93. 45 C.F.R. § 164.508(c) and Cal. Ins. Code § 791.13.
94. 45 C.F.R. § 164.508(c).
95. 45 C.F.R. § 164.508(c).
96. 45 C.F.R. § 164.508(c).
97. Cal. Ins. Code § 791.06.
98. 45 C.F.R. § 164.508(d).
99. 45 C.F.R. § 45 C.F.R. § 164.508(d)(2).
100. 45 C.F.R. § 164.508(b)(5).
101. Per Cal. Dept. of Ins.
102. *See* 45 C.F.R. § 164.504(f)(3) (describing limitations on group health plans and the plans that issue their coverage).
103. 45 C.F.R. § 164.504(f)(1).
104. 45 C.F.R. § 164.504(a) (defining "summary health information").
105. *See* 45 C.F.R. § 164.504(e) and 65 Fed. Reg. 82509.
106. Cal. Civ. Code § 56.104. In order to release the information, the provider must have, in addition to the request, a signed general consent permitting it to use and disclose health information for treatment, payment, and health care operations under the Federal Privacy Rule. *See* 45 C.F.R. § 164.506.
107. The patient may waive receiving a copy of the request by submitting a signed letter to this effect to the provider. *See* Cal. Civ. Code § 56.104.
108. *See* 45 C.F.R. § 164.508(a)(2) and § 164.501 (defining "psychotherapy notes").
109. *See* 45 C.F.R. § 164.508(b)(4).
110. *See* Cal. Ins. Code § 791.04.
111. Compare Cal. Ins. Code § 791.04(a) with 45 C.F.R. § 164.520(b) and (c).
112. 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.
113. Cal. Ins. Code § 791.08 and 791.09.
114. *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").
115. Cal. Ins. Code § 791.08.
116. 45 Fed. Reg. § 164.524 and § 164.501(defining designated record set).
117. *See* Cal. Ins. Code § 791.08 (providing for access to "personal information"); 791.02(s) (defining "personal information" as not including "privileged information") and 791.02(v) (defining "privileged information").
118. *See* 45 C.F.R. § 164.524(a).
119. Cal. Ins. Code § 791.08(a).
120. 45 C.F.R. § 164.524(b)(1).
121. Cal. Ins. Code § 791.08(a); 45 C.F.R. § 164.514(h).
122. 45 C.F.R. § 164.524(b)(2).

123. The federal rule gives a health plan 30 days to respond and allows them one 30 day extension, so long as they notify the individual of the delay. 45 C.F.R § 164.524(b)(2). California law requires a health plan to respond to such requests within 30 business days (a period which is longer than "30 days," because it excludes weekends and holidays, but shorter than the extended period allowed by the federal rule). Cal. Ins. Code § 791.08.

124. Cal. Ins. Code § 791.08(a).

125. Cal. Ins. Code § 791.08(a).

126. 45 C.F.R. § 164.524(c).

127. 45 C.F.R. 164.524 and 65 Fed. Reg. 82557 (explaining acceptable fees).

128. Privileged information is information that is collected in connection or anticipation of a claim for insurance benefits or civil or criminal proceedings. Cal. Ins. Code § 791.02. *See* discussion above about scope of access provisions.

129. Cal. Ins. Code § 791.08(c).

130. 45 C.F.R. § 164.524(a)(3).

131. 45 C.F.R. § 164.524(a)(3).

132. Cal. Ins. Code § 791.08(a).

133. 45 C.F.R. § 164.528.

134. Cal. Ins. Code § 791.09.

135. The IIPPA amendment provisions will not be preempted by the Federal Privacy Rule because they do not conflict with the federal regulation. *See* 45 C.F.R. §§ 160.202 and 160.203 (explaining when state law is preempted by the Federal Privacy Rule). Plans can easily comply with both the state and federal law by meeting the higher standards of the state law.

136. Cal. Ins. Code § 791.09.

137. Cal. Ins. Code § 791.09.(a).

138. 65 Fed. Reg. 82471.

139. 5 C.F.R. § 164.530.

140. 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.

141. 65 Fed. Reg, 82562 and HHS Guidance at 22.

142. 45 C.F.R. § 164.530(b).

143. 45 C.F.R. § 164.530(a).

144. 45 C.F.R. § 164.530(a).

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

146. 45 C.F.R. § 164.506(d).

147. 45 C.F.R. § 164.508(b)(6).

148. 45 C.F.R. § 164.506(b).

149. 45 C.F.R. § 164.522(a).

150. 45 C.F.R. § 164.528(d)(1).

151. 45 C.F.R. § 164.514 and § 164.530(i) and 164.530(j).

152. 45 C.F.R. § 164.530(b) and § 164.530(j)(1).

153. 45 C.F.R. § 164.530(j)(2).

154. Benedict Carey, A Referee in Disputes between Patients, HMOs: A year after its debut, a state agency offers a glimpse of how expanded rights may play out nationwide. Health; S-1 (July 30, 2001).

155. This discussion focuses on health care service plans that are subject to the Knox-Keene Act. There are, however, some health care service plans that are exempt from the Knox-Keene Act. *See* Cal. Health & Safety Code § 1343(e).

156. 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.

157. Cal. Civ. Code § 56.10.

158. Cal. Civ. Code § 56.11.

159. Cal. Health & Safety Code § 1364.5.

160. Cal. Health & Safety Code § 1364.5.

161. Cal. Civ. Code § 56.10 and § 56.05(f) (defining "medical information").

162. 45 C.F.R. § 164.501 (defining "protected health information"). In general, the Privacy Rule restricts the sharing of health information orally, but does not provide access to oral communications. Under the Rule, 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").

163. Cal. Civ. Code § 56.10(c)(2).

164. Guidance at 20.

165. 45 C.F.R. § 164.502(b) (explaining when minimum necessary standard applies).

166. 45 C.F.R. § 164.502(b)(2).

167. 45 C.F.R. § 164.514(d)(2).

168. 45 C.F.R. § 164.530(j).

169. 45 C.F.R. § 164.502(b) and § 164.514(d)(4).

170. 45 C.F.R. § 164.530(j).

171. 45 C.F.R. § 164.514(d).

172. Cal. Civ. Code § 56.10(c)(3).

173. 45 C.F.R. § 164.502(e).

174. 45 C.F.R. § 160.103 (defining "business associate").

175. 65 Fed. Reg. 82476.

176. 45 C.F.R. § 164.504(e)(2).

177. *See* generally Cal. Civ. Code § 56.10and 45 C.F.R. § 164.512.

178. Cal. Civ. Code § 56.10(c).

179. 45 C.F.R. § 164.502(a).

180. *See* 45 C.F.R. § 164.501 (defining these terms).

181. 45 C.F.R. § 164.506(a).

182. Although the CMIA allows providers who contract with health care service plans to share health information with those plans for the purpose of administering the plan without a patient's express permission, this state law will be superceded by the Federal Privacy Rule which requires written consent prior to such a disclosure. Cal. Civ. Code § 56.10(c)(10).

183. 45 C.F.R. § 164.522.

184. 45 C.F.R. § 164.522(a).

185 45 C.F.R. §164.522(b).

186. Cal. Civ. Code § 56.10(b) and 45 C.F.R. § 164.512.

187. Cal. Civ. Code § 56.10(b) and 45 C.F.R. § 164.512(f).

188. 45 C.F.R. § 164.512(f).

189. Cal Civ. Code § 56.10 (c)(7) and 45 C.F.R. § 164.512(i).

190. 45 C.F.R. § 164.512(i).

191. Cal. Civ. Code § 56.10(a).

192. 45 C.F.R. § 164.508. .

193. *See* Cal. Civ. Code § 56.11.

194. Cal. Civ. Code § 56.11.

195. *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.

196. Cal. Civ. Code § 56.11 and 45 C.F.R. § 164.508(c)(1).

197. 45 C.F.R. § 164.508(c).

198. Cal. Civ. Code § 56.11.

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

200. 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).

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

202. Cal. Civ. Code § 56.11.

203. Cal. Civ. Code §56.11.

204. 45 C.F.R. §164.508(c).

205. 45 C.F.R. § 164.508(c).

206. 45 C.F.R. § 164.508(d).

207. 45 C.F.R. § 45 C.F.R. § 164.508(d)(2).

208. 45 C.F.R. § 164.508(b)(5).

209. 45 C.F.R. § 164.514(e).

210. 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.

211. Cal. Civ. Code § 56.104.

212. In order to release the information, the provider must also have a signed consent permitting it to use and disclose health information for the purposes of treatment, payment, and health care operations under the Federal Privacy Rule. *See* 45 C.F.R. § 164.506.

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

214. *See* 45 C.F.R. § 164.508(b)(4).

215. Cal. Health & Safety Code § 1364.5(b).

216. Cal. Health & Safety Code § 1364.5(b).

217. Cal. Health & Safety Code § 1364.5(b).

218. 45 C.F.R. § 164.520.

219. 45 C.F.R. § 164.520(c). April 14, 2004 is the compliance date for small health plans (i.e., those health plans with annual receipts of $5 million or less). 45 C.F.R. § 160.103 (defining "small health plan") and § 164.534 (specifying compliance dates).

220. 45 C.F.R. § 164.520(c).

221. 45 C.F.R. § 164.520(b).

222. Cal. Health & Safety Code § 1364.5(c).

223. 45 C.F.R. § 164.520(b).

224. Cal. Health & Safety Code § 1364.5(c) and 45 C.F.R. 520(b).

225. Cal. Health & Safety Code § 1364.5(c) and 45 C.F.R. 520(b).

226. Cal. Health & Safety Code § 1364.5(c) and 45 C.F.R. 520(b).

227. Cal. Health & Safety Code § 1364.5(c).

228. Cal. Health & Safety Code § 1364.5(c).

229. 45 C.F.R. § 164.520(b).

230. 45 C.F.R. § 164.520(b).

231. 45 C.F.R. § 164.520(b).

232. Cal. Health & Safety Code § 1364.5(c)(4).

233. *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").

234. 45 C.F.R. § 164.524(a) and § 164.501 (defining a "designated record set"). As a general rule, providers in a group practice prepayment plan maintain the actual medical records, and must give the individual access to those records.

235. 45 C.F.R. § 164.524(a).

236. 45 C.F.R. § 164.514(h).

237. 45 C.F.R. § 164.524(b).

238. 45 C.F.R. § 164.524(d).

239. 45 C.F.R. § 164.524(c).

240. 45 C.F.R. § 164.524(c).

241. 45 C.F.R. § 164.524(c).

242. 45 C.F.R. § 164.524 and 65 Fed. Reg. 82557 (explaining acceptable fees).

243. 45 C.F.R. § 164.524(c).

244. 45 C.F.R. § 164.524(a). There are additional circumstances, such as requests from inmates, that generally would not be encountered by health care service plans.

245. 45 C.F.R. § 164.524(d).

246. 45 C.F.R. § 164.524(d).

247. 45 C.F.R. § 164.524(d).

248. 45 C.F.R. § 164.524(d).

249. 45 C.F.R. § 164.528.

250. 45 C.F.R. § 164.528(a).

251. 45 C.F.R. § 164.528(a) (providing accounting of "disclosures") and § 164.501 (defining "disclosure" and "use").

252. 45 C.F.R. § 164.528(a).

253. 45 C.F.R. § 164.526.

254. 45 C.F.R. § 164.526(a).

255. 45 C.F.R. § 164.526(b).

256. 45 C.F.R. § 164.526(c).

257. 45 C.F.R. § 164.526(d).

258. 45 C.F.R. § 164.526(d).

259. 45 C.F.R. § 164.526(d).

260. 65 Fed. Reg. 82471.

261. 45 C.F.R. § 164.530.

262. § 164.530(c). In addition, HHS is to issue more detailed final HIPAA-mandated security regulations.

263. 65 Fed. Reg, 82562.

264. 45 C.F.R. § 164.530(b).

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

266. 45 C.F.R. § 164.530(a).

267. 45 C.F.R. § 164.530(a).

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

269. 45 C.F.R. § 164.506(d).

270. 45 C.F.R. § 164.522(a).

271. 45 C.F.R. § 164.508(b)(6).

272. 45 C.F.R. § 164.528(d)(1).

273. 45 C.F.R. § 164.514 and § 164.530(i) and 164.530(j).

274. 45 C.F.R. § 164.530(b) and § 164.530(j)(1).

275. 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