

PREFACE

The California Hospital Association published this manual to make complying with complex federal and state patient privacy laws easier for California's hospitals, skilled nursing facilities, clinics, physicians, and other health care providers.

The fourth edition of the *California Health Information Privacy Manual* is expanded to include new state laws and Health Insurance Portability and Accountability Act (HIPAA) mandates under the federal Health Information Technology for Economic and Clinical Health (HITECH) Act. The manual reflects changes in legislation and regulations through June 2009. CHA considers this document a work in progress and intends to update it as privacy laws continue to evolve.

To provide further assistance to members between editions, CHA has created a privacy webpage which includes additional resources such as regulation text, acronyms, forms and links to sites referenced in the manual. Memos will also be posted as additional guidance from regulatory agencies becomes available and as judicial decisions are rendered. CHA members can access the webpage from www.calhospital.org.

CHA recognizes that complying with privacy protections is a tremendous undertaking. We are pleased to publish this manual as a service to our members and others and hope you find it useful. If you have any comments or suggestions on how to improve the *California Health Information Privacy Manual*, please feel free to contact me by phone or e-mail.

Lois J. Richardson, Esq.
Vice President, Legal Publications and Education
California Hospital Association
(916) 552-7611
lrichardson@calhospital.org

Information contained in the *California Health Information Privacy Manual* should not be construed as legal advice or used to resolve legal problems by health care facilities or practitioners without consulting legal counsel. A health care facility may want to accept all or some of the *California Health Information Privacy Manual* as part of its standard operating policy. If so, the hospital or health facility's legal counsel and its board of trustees should review such policies.

INTRODUCTION

Much has changed since CHA published the first edition of this manual in 2004. Even though California has long enacted some of the strictest patient privacy protections in the nation, privacy advocates believed the laws did not go far enough. Consequently, state and federal lawmakers recently enacted legislation that calls for even more complex, cumbersome and costly requirements.

While the first three editions focused on implementing HIPAA — the Health Insurance Portability and Accountability Act — in the context of existing state laws, CHA has significantly expanded and rewritten this fourth edition to encompass new state laws and new HIPAA mandates under the HITECH Act. As with the previous editions, our intent, however, remains the same:

To make your job of complying with complex patient privacy protections easier.

Today, California hospitals and other health care providers face stricter reporting requirements, greater penalties, and increased enforcement. Inside this edition you will find a synthesis of key privacy protection requirements, how best to follow them, and what you might expect down the road. New content includes:

1. A detailed analysis of new state laws.
2. A comprehensive summary of new HIPAA mandates contained in the HITECH Act of the federal stimulus package.
3. A chapter on breaches, what constitutes a breach of confidentiality, and what to report, by when, and to whom.
4. An updated Preemption Analysis — a side-by-side comparison of state and federal laws with guidance on which law to follow and when.
5. Updated sample forms, notices and business associate agreements that can be adapted to fit your hospital's needs.

REASON BEHIND NEW STATE PRIVACY LAWS

Curiosity is human. In our fame-obsessed culture, googling celebrities at home to satiate our curiosity is okay. Peeking at their medical record and selling the information to the *National Enquirer*, is clearly not.

Repeated and well-publicized privacy breaches occurring at hospitals in the past couple of years turned personal when Governor Schwarzenegger learned his wife's health record had been accessed inappropriately. As a result, the governor put his policy staff to work developing new privacy protections.

NEW LAWS STEP-UP ENFORCEMENT

On Sept. 30, 2008, Governor Schwarzenegger signed SB 541 and AB 211 into law; both health information privacy bills took effect Jan. 1, 2009. Even though state and federal laws already protected a patient's health information, imposing penalties in California was difficult unless a district attorney or the Attorney General took action. SB 541 requires hospitals and other health facilities to self-report a privacy breach within five days of detection, and gives the California Department of Public Health (CDPH) authority to impose fines on hospitals. Hospitals and other health facilities may be fined \$25,000 for the initial breach, and \$17,500 for subsequent breaches up to \$250,000 per reportable event.

AB 211 created the Office of Health Information Integrity (OHII) within the California Health and Human Services Agency. Formed with staff from the former Office of HIPAA Implementation, OHII holds individuals (including physicians, nurses, clerks, etc.) accountable for unlawful access, use or disclosure of protected health information (PHI). Once CDPH refers an offender to OHII, the agency has the authority to assess a penalty up to \$250,000; report the individual to the appropriate licensing board for discipline; and refer him or her to the local district attorney and the state Attorney General for action.

In the first two months of 2009 after the laws took effect, California hospitals and other health facilities self-reported nearly 300 breaches. Member hospitals have turned to CHA to help clarify the reporting requirements. While CHA advises hospitals to seek legal advice from their own counsel, this manual contains general guidance on where to report privacy breaches, what to report to CDPH, and addresses common concerns such as misdirected faxes or e-mails.

NEW HIPAA MANDATES BURIED IN STIMULUS BILL

Surprising to many, major new privacy protections ended up in the final version of the nearly thousand-page federal American Recovery and Reinvestment Act (ARRA) of 2009 with no public review. Privacy advocates, unhappy with HIPAA provisions they viewed as lax, successfully convinced lawmakers to add new privacy provisions to the federal stimulus package at the last minute. President Obama signed ARRA into law, significantly changing federal privacy and security law as it pertains to PHI.

The new protections are contained in ARRA under Title XIII's Health Information Technology for Economic and Clinical Health (HITECH) Act. The changes are part of the government's effort to protect patient privacy as it develops a nationwide health information technology infrastructure. The HITECH Act expands the reach of HIPAA with new

provisions that:

1. Impose new breach notification requirements on hospitals, other health care providers, and business associates.
2. Increase penalties and enforcement of privacy and security violations.
3. Expand patients' rights regarding their health information and limit certain disclosures.
4. Require the Office of Civil Rights under the U.S. Department of Health and Human Services to conduct more privacy and security audits.
5. Require a study to determine an incentive payment for patients to report privacy violations.
6. Require a national education initiative to inform people about their privacy rights and how their medical information may be used.

THE IMPACT ON CALIFORNIA HOSPITALS

Obviously, the impact of these new state and federal laws is major. Some hospitals have already created "Breach Specialists" at their facilities. While not mandatory, hospitals have created the position out of necessity. Once a breach is discovered, hospitals must enact a rapid decision tree that involves a myriad of factors, including whether to report the breach under HIPAA and/or state law.

CHA recognizes that complying with privacy protections is a tremendous undertaking. There is nothing intrinsically easy about complying with the new laws; however, CHA hopes this manual will make your job of complying easier. While everyone agrees that privacy is a fundamental American right, striking a balance between protecting the rights of individuals and protecting health care providers from burdensome regulation is exceedingly difficult. CHA will continue to work toward achieving a realistic balance.

If you have comments or suggestions on how to improve this manual, CHA welcomes your input. Please contact Lois Richardson by phone, (916) 552-7611, or by e-mail, Lrichardson@calhospital.org.

UNDERSTAND THE LAWS

I. INTRODUCTION

Health care providers in California must comply with a myriad of health information privacy laws. At the state level, there is the Confidentiality of Medical Information Act (CMIA), the Lanterman-Petris-Short (LPS) Act, special provisions regarding HIV test results, and the Patient Access to Health Records Act (PAHRA). At the federal level, there are special provisions for substance abuse programs, the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, and now the Health Information Technology for Economic and Clinical Health (HITECH) Act.

This chapter will help you understand the different laws that exist in California and which ones your organization must comply with. We'll start with a brief description of each law, and tell you where in this manual to find complete details about it.

II. STATE PRIVACY LAWS

A. CONFIDENTIALITY OF MEDICAL INFORMATION ACT

The Confidentiality of Medical Information Act (CMIA) is California's general medical privacy law. It was enacted in 1979 and applies to most health care providers, including hospitals, skilled nursing facilities, doctors, nurses, pharmacists, and others. The two significant exceptions are substance abuse programs and some mental health care providers. A complete discussion of the CMIA is found in chapter 5 of this manual.

B. THE LANTERMAN-PETRIS-SHORT ACT

Many providers of mental health services — primarily acute psychiatric hospitals, inpatient psychiatric units, and government-operated hospitals and clinics — are exempt from the CMIA and instead must follow the stricter confidentiality provisions of LPS. The LPS confidentiality provisions were written in 1969, when the mental health system was quite different from what it is today. A complete discussion of LPS is found in chapter 6 of this manual.

C. HIV TEST RESULTS

AIDS became recognized as a specific disease in the United States in 1981. Because of the stigma associated with the disease back then, the California legislature gave HIV test results extra confidentiality protection in 1985. These strict laws are still on the books. The confidentiality protections afforded to HIV test results are discussed in chapter 4 of this manual.

D. PATIENT ACCESS TO HEALTH RECORDS ACT

Although medical records are the property of the hospital, physician, or other health care provider that created them, patients in California have had a right to inspect or obtain copies of their medical records since 1988. An amendment allowing patients to add an addendum to their medical record, if they believe the record contains incorrect information, was added in 2000. Chapter 3 discusses patients' rights under California law to access and add a statement to their medical record (as well as the HIPAA right to amend).

III. FEDERAL PRIVACY LAWS

A. SUBSTANCE ABUSE PROGRAMS

The federal government has promulgated confidentiality rules that apply to drug and alcohol abuse treatment programs. These rules do not apply to all substance abuse patients; they apply only to "federally-assisted programs." These rules are described in detail in chapter 7 of this manual.

B. HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to deal with a wide array of issues. Because of this, HIPAA means different things to different people. To some, HIPAA means making sure workers and their families can still get health insurance coverage when they change or lose their jobs. To others, HIPAA means national provider identifiers, standards for electronic data interchange, standards to protect patient health information and much more. The latter provisions — the "administrative simplification" portions of the act — were meant to facilitate the electronic exchange of health information, insurance eligibility information, and claims information throughout the country, thus saving money.

Unlike California, some states had weak or nonexistent health information privacy laws prior to HIPAA. During the debate surrounding HIPAA and the movement to convert health information to electronic format, patients (or at least privacy advocates) were concerned that their health information would not remain private or secure. In HIPAA, Congress gave itself a three-year deadline to enact privacy legislation. If it failed to meet its deadline, which it did, it authorized the U.S. Department of Health and Human Services (DHHS) to promulgate privacy regulations. These regulations, effective in April 2003, were meant to provide a minimum level of privacy rights and privacy protection for health information throughout the country.

HIPAA is, in effect, a complicating overlay to California's patchwork of health information privacy laws. Under HIPAA preemption rules, health care providers must comply with whichever federal or state law is more stringent. Complicating matters further, providers must comply with whichever *provision* of the laws is stricter. This means that if the state law is more stringent than federal law, with the exception of one provision, providers must comply with the state law and the one provision in federal law that gives the patient greater privacy protection.

PREEMPTION ANALYSIS

On behalf of the California Hospital Association, health care attorneys with Davis Wright Tremaine, LLP, have conducted a preemption analysis which compares HIPAA with pertinent California laws, including the laws described above. The analysis outlines the extent to which HIPAA preempts state law, and provides practical guidance for California health care providers seeking to determine which law to follow under which circumstances. The results of the analysis are described throughout this manual. In addition, helpful Preemption Analysis Charts have been prepared for easy reference. Health care providers should study these three charts, as they form the basis for HIPAA compliance related to the disclosure of protected health information (PHI).

Chapters 4, 5 and 6 each contain a chart showing the results of the preemption analysis regarding, respectively, HIV test results, CMIA, and LPS.

C. THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

The American Recovery and Reinvestment Act (ARRA) of 2009, also known as the "economic stimulus" bill, was signed by President Obama on Feb. 17, 2009. Title XIII of Division A of ARRA is called the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The HITECH Act contains financial incentives, grants and loans to assist hospitals and others in adopting electronic health record (EHR) systems; penalties in the future for hospitals that fail to adopt EHRs; and, in Subtitle D, stricter privacy and security provisions. Prominent among these new provisions is a breach notification requirement, new restrictions on certain disclosures of PHI, and new rights for patients regarding electronic health records (EHR). The HITECH Act also requires additional enforcement activities by the Office of Civil Rights, and establishes higher penalties for health care providers found out of compliance with HIPAA and HITECH requirements. The HITECH provisions are described in appropriate chapters throughout the manual.

MORE REGULATIONS TO COME

The HITECH Act calls for the publication of approximately 15 new regulations and guidances as well as four reports regarding privacy and security over the next three years. Health care providers will have a lot to do to keep up with these changes. CHA has prepared a chart that outlines the timelines for the release of the new regulations. It is CHA's intention to track the regulations and provide members with additional guidance as the regulations evolve.

IV. STATE AND FEDERAL SECURITY AND BREACH REPORTING LAWS

Various state laws establish general security requirements for health information, both paper and electronic. These state laws are somewhat redundant and vague. In contrast, HIPAA's Security Rule requires covered entities (which includes hospitals) to have in place appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic PHI; to protect against any anticipated threats or hazards to the security or integrity of the PHI; and to protect against reasonably anticipated uses or disclosures that are not permitted. These requirements are discussed in chapter 10.

In addition, California has adopted two breach notification laws. The first law applies to breaches of unencrypted computerized data. The second law applies to breaches of patient privacy (whether the breach involves electronic, paper, or oral information) that are detected by a licensed health care facility. Finally, HITECH contains a breach reporting obligation that will become effective 30 days after publication of regulations by the Secretary of the Department of Health and Human Services. These regulations are expected by Aug. 17, 2009. Breach reporting laws are discussed in chapter 12.

V. HEALTH INFORMATION PRIVACY BASICS

A. WHO MUST COMPLY?

California health care providers must comply with either the CMIA, LPS, or the substance abuse regulations as described above. In addition, health care providers (as defined below) that transmit any health information in electronic form in connection with a transaction (as defined below) must comply with HIPAA [45 C.F.R. Section 160.103]. Health plans and health care clearinghouses must also comply. HIPAA refers collectively to those who must comply as "covered entities."

"**Health care provider**" is any person or organization who furnishes, bills or is paid for health care in the normal course of business.

“Transaction” means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Other transactions that the Secretary may prescribe by regulation.

A provider that does not do one of the above transactions directly, but instead uses an agent (such as a billing service or clearinghouse) for these electronic transactions is considered a “covered entity” and must comply with HIPAA. [45 C.F.R. Section 160.103]

The scope of this manual is limited to hospitals and other health care providers; requirements that are specific to health plans and clearinghouses are not addressed. Therefore, we often refer to “covered entities” as “health care providers” or “providers” in this manual.

B. WHAT DO THE LAWS REQUIRE PROVIDERS TO DO?

This manual covers in detail what providers must do to comply with state and federal confidentiality laws. In short, providers must:

1. Provide information, in writing, to patients about their privacy rights and how their information will be used.
2. Develop policies, procedures and systems to protect patient privacy and patients’ ability to access, amend and amend their records.
3. Train staff on these procedures.
4. Appoint a “privacy officer” to make sure privacy procedures are developed, adopted and followed.
5. Appoint a “security officer” to make sure security procedures are developed, adopted and followed.
6. Secure patient records that contain PHI from individuals who shouldn’t see them.

7. Account for specified disclosures of PHI.
8. Establish a complaint mechanism for privacy concerns.
9. Establish and enforce a system of sanctions for employees who violate privacy policies and procedures.
10. Notify patients and government agencies in the event of a breach, where required.

C. WHAT INFORMATION IS PROTECTED?

Providers must maintain the confidentiality and security of what HIPAA refers to as protected health information (PHI). **“PHI”** means individually-identifiable health information that is transmitted or maintained in electronic media or any other form or media.

“Individually-identifiable health information” is health information (including demographic information) that identifies or can be used to identify the individual.

“Health information” is broadly defined to include any information, oral or recorded in any form or medium, relating to the physical or mental health or condition of an individual, the health care provided to an individual, or payment for health care provided to an individual.

This protection covers information relating to a person’s health, the care received, and payment for services. PHI does not, however, include education records, student medical records or employment records held by a covered entity in its role as employer [45 C.F.R. Sections 160.103 and 164.500]. However, HIPAA does protect employee health information held by an employee group health plan, and California law restricts the use of employee health information. (*See chapter 9 regarding employee health information.*)

Providers must maintain the confidentiality and security of PHI in any form — electronic, on paper or oral. The general rule for the use or release of health information under HIPAA is similar to requirements called for by California’s privacy laws. In general, providers cannot use or disclose PHI unless the patient authorizes it, except for purposes of treatment, payment and health care operations. Some exceptions exist which are discussed later in this manual.

It is extremely important to note that these restrictions apply not only to disclosing PHI to third parties, but to the provider’s own use of this information internally, among staff and throughout departments.

D. PATIENT PRIVACY RIGHTS

Under state and federal laws, patients can:

1. Obtain a written notice from a provider explaining how it will use and disclose their information.

2. Access their medical records. This means patients can see their records, request copies, request an amendment to the records and get an accounting of specified disclosures. (However, patients are not entitled to take original record.)
3. Request that certain information be restricted from use or disclosure for purposes of treatment, payment, and health care operations (although providers are not required to comply with such requests, except in limited circumstances).
4. Obtain an accounting of how their information has been used for purposes not related to treatment, payment or health care operations.
5. Request that information be communicated to them in particular ways to ensure confidentiality, for example at work rather than at home.
6. Refuse to authorize the release of their information for most purposes not related to treatment, payment or health care operations.

In general, the health information privacy laws ensure that health information is used for health care-related purposes only. In addition, providers must limit their use and disclosure of PHI to the “minimum necessary” — that is, the minimum amount of information necessary to accomplish the goal. The same goes for requesting information. Providers who need information for payment or operations must limit their requests to other covered entities to the minimum amount of information they need. This provision doesn’t apply to requesting or disclosing medical records for treatment purposes. Physicians and other providers may need the complete medical record to provide the best care possible. (See chapter 4 for a complete discussion of the minimum necessary standard.)

E. PROVIDERS CAN USE OR DISCLOSE PHI FOR “TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS” WITHOUT PATIENT AUTHORIZATION

Providers may use or disclose PHI, without patient authorization, for what HIPAA calls “treatment, payment and health care operations.” “Use” applies to internal sharing of individually-identifiable health information while “**disclosure**” applies to the external release of information [45 C.F.R. Section 160.103]. Treatment, payment and health care operations are defined as follows:

“**Treatment**” means providing, coordinating or managing a patient’s care, including consultations between providers and referrals.

“**Payment**” is defined as activities related to paying or being paid for services rendered. These include eligibility and

coverage determinations, billing, claims management, utilization review and the like. It also includes using debt collection and location agencies, although a health plan or provider would need a business associate agreement with such an agency. The privacy rule also permits limited disclosures to consumer reporting agencies intended to enable covered entities to comply with the Fair Credit Reporting Act.

“**Health care operations**” covers a broad range of activities such as quality assessment, patient education and training, health practitioner training, contracting for health care services, medical review, legal services, auditing functions, business planning and development, business management and general administrative activities.

[45 C.F.R. Section 164.506]

In addition, HIPAA recognizes that “incidental” uses and disclosures will occur. For example, if two hospitalized patients share a room, it is inevitable that one patient will overhear medical information about the other. HIPAA explicitly permits covered entities to use or disclose PHI “incident to a use or disclosure otherwise permitted or required by” the HIPAA Privacy Rule, if the covered entity has complied with the minimum necessary standard; implemented appropriate administrative, technical, and physical safeguards; and made reasonable attempts to limit incidental uses and disclosures. For example, if a nurse needs to talk to a patient about his or her medical condition, it would be reasonable to ask the roommate’s visitors to step outside the room temporarily. However, it would not be necessary to require the roommate to be transferred to another room temporarily. [45 C.F.R. Section 164.502(a)(1)(iii)]

F. OTHER REQUIRED OR PERMITTED USES AND DISCLOSURES OF PHI WITHOUT PATIENT AUTHORIZATION

A provider must disclose PHI if the Secretary of Health and Human Services requires the information to investigate a provider’s compliance with HIPAA. Providers may also disclose PHI without authorization for a variety of public interest-related purposes. Each of these has its own requirements and limitations (see chapters 4-7 for permitted uses and disclosures of PHI). They include the following:

1. Public health activities that involve safety or communicable disease,
2. To report victims of abuse, neglect or domestic violence,
3. Judicial and administrative proceedings,
4. Law enforcement purposes,
5. Organ and tissue donations,

6. National security and intelligence activities,
7. Workers' compensation, and
8. Requests related to decedents.

G. USE AND DISCLOSURE OF PHI REQUIRING PATIENT AUTHORIZATION

Under HIPAA, providers may use and disclose PHI for treatment, payment and health care operations without the patient's authorization. They may also disclose health information for the public interest-related purposes described above. However, in order to use or disclose PHI for other purposes, providers need a specific written authorization. Examples are use for commercial purposes, or reporting health information to a patient's life insurer or employer.

Because it is focused on a particular use or disclosure, an authorization must be specific — with regard to the information to be disclosed, who may disclose it, and who may receive it. It must also be time limited. In many cases, a provider must obtain a patient's authorization to use or share information even within a facility. A detailed explanation of authorization can be found in chapter 4.

H. INFORMATION PROVIDERS CAN RELEASE FREELY

HIPAA does not protect health information that has been “**de-identified**” by removing, coding, encrypting, or otherwise eliminating or concealing individually-identifiable information. De-identified information may be used or disclosed freely if no means of re-identification is disclosed. [45 C.F.R. Section 164.502(d)] (*See Appendix PR 1-B, “HIPAA Standard Regarding De-identification and Re-identification of PHI.”*)

In addition, covered entities may use or disclose a limited data set for the purposes of research, public health, or health care operations if the covered entity enters into a data use agreement with the limited data set recipient [45 C.F.R. Section 164.514(e)]. (*See Appendix PR 1-C, “HIPAA Standard Regarding Limited Data Set,” for applicable requirements.*)

VI. ORGANIZATIONAL STRUCTURE

A. AFFILIATED COVERED ENTITY

HIPAA permits legally separate covered entities who are under common ownership or control to designate themselves as a single covered entity for HIPAA privacy purposes. Affiliated covered entities may share a privacy official, implement one Notice of Privacy Practices, conduct joint training, use one business associate agreement, etc. [45 C.F.R. Section 164.105(b)]

For example, a health system that includes one or more hospitals, clinics, a hospice program, etc. may wish to designate these entities as an affiliated covered entity. The designation must be documented in writing.

B. ORGANIZED HEALTH CARE ARRANGEMENT

HIPAA permits legally separate covered entities who may not be under common ownership or control, but serve a common set of patients, to designate themselves as an organized health care arrangement (OHCA) for HIPAA privacy purposes [45 C.F.R. Section 160.103].

OHCAs concern arrangements involving clinical or operational integration among legally separate covered entities in which it is often necessary to share PHI for the joint management and operations of the OHCA. HIPAA permits these legally separate entities within an OHCA to share PHI for health care operations purposes [45 C.F.R. Section 164.506(c)].

In order to become an OHCA, the entities must hold themselves out to the public as participating in a joint arrangement, and must jointly perform utilization review, quality assessment and improvement activities, or payment activities. For example, a hospital and members of its medical staff, who are not employed by the hospital, may designate themselves as an OHCA.

The HIPAA regulations do not require the OHCA designation to be formally designated in writing. However, taking this step is recommended. The Notice of Privacy Practices must clearly indicate which entities are included in the OHCA.

Health care providers considering designating themselves as affiliated covered entities or OHCAs should consult legal counsel.