CALIFORNIA
HEALTH INFORMATION
PRIVACY MANUAL

October 2012
4th Edition
QUICK REFERENCE GUIDE

- Preface
- Introduction
- Where to Find Laws and Other Resources Referenced in the Manual
- Numerical Listing of Forms and Appendixes

Chapter 1 .......... Understand the Laws
Chapter 2 .......... Administrative Processes and Considerations
Chapter 3 .......... Privacy Rights and Notice of Privacy Practices
Chapter 4 .......... Use and Disclosure of PHI: Fundamentals and Preemption Analysis
  - Preemption Analysis: HIV Test Results
Chapter 5 .......... Use and Disclosure of PHI: Patients Covered by CMIA
  - Preemption Analysis: Patients Covered by CMIA
Chapter 6 .......... Use and Disclosure of PHI: Patients Covered by LPS
  - Preemption Analysis: Patients Covered by LPS
Chapter 7 .......... Use and Disclosure of PHI: Substance Abuse
Chapter 8 .......... Privacy and the Conduct of Research
Chapter 9 .......... Employee Health Information
Chapter 10 .......... Health Information Security
Chapter 11 .......... Business Associate Contracts
Chapter 12 .......... Breaches
Chapter 13 .......... Enforcement and Penalties
  - Index
The California Hospital Association publishes 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 October 2012. 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 website that includes additional resources such as regulation text, 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 website from www.calhospital.org.

CHA would like to thank W. Clark Stanton, Esq., of Hooper, Lundy & Bookman, PC, for his extensive work in developing previous editions of this manual. CHA would also like to acknowledge the contributions of Paul Smith, also of Hooper, Lundy & Bookman, PC, to previous editions of this manual.

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, Privacy and Legal Publications/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 2002. Even though California has long enacted some of the strictest patient privacy protections in the nation, privacy advocates believe the laws do not go far enough. Consequently, state and federal lawmakers continue to enact legislation that calls for even more complex, cumbersome and costly requirements. Our intent in publishing this edition of the manual remains the same:

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

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

REASON BEHIND 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 few years turned personal when former Governor Schwarzenegger learned his wife’s health record had been accessed inappropriately. As a result, the governor put his policy staff to work developing additional privacy protections.

On Sept. 30, 2008, the governor 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 had been 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. CDPH and private lawyers have been very busy enforcing privacy laws against hospitals since SB 541 took effect.

AB 211 created the California Office of Health Information Integrity (CalOHII) within the California Health and Human Services Agency. Formed with staff from the former Office of HIPAA Implementation, CalOHII holds individuals (including physicians, nurses, clerks, etc.) accountable for unlawful access, use or disclosure of health information. Once CDPH refers an offender to CalOHII, 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.

THE IMPACT ON CALIFORNIA HOSPITALS

Obviously, the impact of these state and federal laws is major. Some hospitals have 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 these 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.
WHERE TO FIND LAWS AND OTHER RESOURCES REFERENCED IN THE MANUAL

All of the laws discussed in the California Health Information Privacy Manual can be found on the Internet.

I. FEDERAL LAW

A federal statute is written by a United States Senator or Representative. It is voted on by the United States Senate and the House of Representatives, and then signed by the President. A federal statute is referenced like this: 42 U.S.C. Section 1395. “U.S.C.” stands for “United States Code.” Federal statutes may be found at www.gpo.gov/fdsys.

A federal regulation is written by a federal agency such as the U.S. Department of Health and Human Services or the U.S. Food and Drug Administration. The proposed regulation is published in the Federal Register, along with an explanation (called the “preamble”) of the regulation, so that the general public and lobbyists may comment on it. The federal agency must summarize and respond to each comment it receives on the proposed regulation. The agency may or may not make changes to the proposed regulation based on the comments. The final regulation is also published in the Federal Register. A federal regulation is referenced like this: 42 C.F.R. Section 482.1 or 42 C.F.R. Part 2. “C.F.R.” stands for “Code of Federal Regulations.” Federal regulations may be found at www.gpo.gov/fdsys. The preamble, however, is only published in the Federal Register and not in the Code of Federal Regulations. The Federal Register may be found at www.gpo.gov/fdsys.

The Centers for Medicare & Medicaid Services publishes its Interpretive Guidelines for surveyors on the internet. They may be found at www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs.html. Click on Publication 100-07, State Operations Manual, then “Appendices Table of Contents.” There are several appendices that hospitals will find useful, for example, A (hospitals), AA (psychiatric hospitals), V (EMTALA), and W (critical access hospitals).

A federal law must be obeyed throughout the United States, including in California, unless the federal law expressly states otherwise. As a general rule, if a federal law conflicts with a state law, the federal law prevails, unless the federal law expressly states otherwise.

If there is no conflict, such as when one law is stricter but they don’t actually conflict with each other, both laws generally must be followed. For example, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal law states that providers must conform to whichever provision of federal or state law provides patients with greater privacy protection or gives them greater access to their medical information (see chapter 3).

II. STATE LAW

A state statute is written by a California Senator or Assembly Member. It is voted on by the California Senate and Assembly, and then signed by the Governor. A state statute is referenced like this: Civil Code Section 56 or Health and Safety Code Section 819. State statutes may be found at www.leginfo.ca.gov. Proposed laws (Assembly Bills and Senate Bills) may also be found at this website.

A state regulation is written by a state agency such as the California Department of Public Health or the California Department of Mental Health. A short description of the proposed regulation is published in the California Regulatory Notice Register, more commonly called the Z Register, so that the general public and lobbyists may request a copy of the exact text of the proposed regulation and comment on it. The state agency must summarize and respond to each comment it receives on the proposed regulation. The agency may or may not make changes to the proposed regulation based on the comments. A notice that the final regulation has been officially adopted is also published in the Z Register. The Z Register may be found at www.oal.ca.gov/notice.htm.

A state regulation is referenced like this: Title 22, C.C.R., Section 70707. “C.C.R.” stands for “California Code of Regulations.” State regulations may be found at www.calregs.com.

A state law must be obeyed in California only. As a general rule, if a California law conflicts with a federal law, the federal law prevails, unless the federal law expressly states otherwise. (If there is no conflict, such as when one law is stricter but they don’t actually conflict with each other, both laws generally must be followed.)

III. INTERNET RESOURCES

The Office of Civil Rights (part of the U.S. Department of Health and Human Services) is responsible for enforcing the HIPAA Privacy and Security Rules. Its website contains many useful resources, and may be found at www.hhs.gov/ocr/privacy/index.html.
# NUMERICAL LISTING OF FORMS AND APPENDIXES

## 1. UNDERSTAND THE LAWS
- **PR 1-A** Acronyms
- **PR 1-B** HIPAA Standard Regarding De-Identification and Re-Identification of PHI
- **PR 1-C** HIPAA Standard Regarding Limited Data Set

## 2. ADMINISTRATIVE PROCESSES AND CONSIDERATIONS
- **PR 2-A** Sample Job Description Privacy Officer
- **PR 2-B** Sample Job Description Security Officer

## 3. PRIVACY RIGHTS AND NOTICE OF PRIVACY PRACTICES
- **15-1S** Notice of Privacy Practices: Acknowledgment of Receipt
- **15-2S** Model Notice of Privacy Practices
- **15-3S** Model Notice of Privacy Practices (For Mental Health Information Subject to the Lanterman-Petris-Short Act)
- **15-4S** Request to Amend Protected Health Information
- **15-5S** Response to Request to Amend Protected Health Information
- **15-6** Notification of Amendment to Protected Health Information
- **15-7S** Statement of Disagreement/Request to Include Amendment Request and Denial with Future Disclosures
- **15-8S** Request for an Accounting of Disclosures
- **15-9S** Response to Request for an Accounting of Disclosures
- **15-10S** Request for Special Restriction on Use or Disclosure of Protected Health Information
- **15-11S** Response to Request for Special Restriction on Use or Disclosure of Protected Health Information
- **15-12S** Termination of Special Restriction
- **15-13S** Request for Restriction on the Manner/Method of Confidential Communications
- **PR 3-A** Disclosures That Must Be Accounted For

## 4. USE AND DISCLOSURE OF PHI: FUNDAMENTALS AND PREEMPTION ANALYSIS
- **16-1S** Authorization for Use or Disclosure of Health Information

## 5. USE AND DISCLOSURE OF PHI: GENERAL PATIENT
- **16-2S** Request to Withhold Public Release of Information
- **16-3** Response to Subpoena Duces Tecum
- **16-4** Time Extension for Compliance with Subpoena
- **16-5** Affidavit of Custodian of Medical Records to Accompany Copies of Records
- **16-6** Request for Access to Hospital Records or Other Documents (By Authorized State or County Department of Public Health Representatives for Licensure and Other Statutory Purposes)
- **16-7** Civil Subpoena
- **16-8** Deposition Subpoena for Personal Appearance and Production of Documents and Things
- **16-9** Deposition Subpoena for Production of Business Records
- **16-10** Notice to Consumer or Employee and Objection

## 6. USE AND DISCLOSURE OF PHI: MENTAL HEALTH AND DEVELOPMENTAL DISABILITIES
- **17-1** Response to Request for Confidential Information
- **17-2** Order for Production of Mental Health records

## 7. USE AND DISCLOSURE OF PHI: SUBSTANCE ABUSE
- **18-1** Substance Abuse Program Notice of Prohibition of Redisclosure
- **18-A** Order for Production of Substance Abuse Records
- **18-BS** Notice to Patient: Confidentiality of Substance Abuse Patient Records

## 10. HEALTH INFORMATION SECURITY
- **PR 10-A** HIPAA Security Standards Matrix

## 11. BUSINESS ASSOCIATE CONTRACTS
- **PR 11-B** Business Associate Addendum

## 12. BREACHES
- **PR 12-A** Federal and State Breach Notification Laws for California

---

**NOTE:** Forms that begin with a number originated in CHA’s *Consent Manual*. For example, Form 16-1 (Authorization for Use and Disclosure of Health Information) originated in chapter 16 of the *Consent Manual*. Forms that begin with “PR” originated in CHA’s *California Health Information Privacy Manual*. For example, Form PR 3-A (Disclosures That Must Be Accounted For) originated in chapter 3 of the *California Health Information Privacy Manual*.

“S” denotes that the form is provided in English and Spanish.
# UNDERSTAND THE LAWS

## I. INTRODUCTION 1.1

## II. STATE PRIVACY LAWS 1.1

A. Confidentiality of Medical Information Act 1.1

B. The Lanterman-Petris-Short Act 1.1

C. HIV Test Results 1.1

D. Patient Access to Health Records Act 1.1

E. Social Security Numbers 1.1

## III. FEDERAL PRIVACY LAWS 1.2

A. Health Insurance Portability and Accountability Act of 1996 1.2

B. The Health Information Technology for Economic and Clinical Health Act 1.2

C. Substance Abuse Programs 1.3

## IV. STATE AND FEDERAL SECURITY LAWS 1.3

A. Federal Laws 1.3

B. State Laws 1.3

## V. STATE AND FEDERAL BREACH NOTIFICATION LAWS 1.4

## VI. GOVERNMENT-OWNED HOSPITALS 1.4

A. The Federal Privacy Act of 1974 1.4

B. Federal Freedom of Information Act 1.4

C. State Executive Order B-22-76 1.4

D. State Agencies 1.4

E. California Public Records Act 1.4

## VII. ENFORCEMENT AND PENALTIES 1.4

A. Federal Laws 1.4

B. State Laws 1.5

## VIII. HEALTH INFORMATION PRIVACY BASICS 1.5

A. Who Must Comply? 1.5

B. What Do The Laws Require Providers To Do? 1.5

C. What Information Is Protected? 1.6

D. Patient Privacy Rights 1.6

E. Providers Can Use or Disclose PHI for “Treatment, Payment, and Health Care Operations” Without Patient Authorization 1.7

F. Other Required or Permitted Uses and Disclosures of PHI Without Patient Authorization 1.7

G. Use and Disclosure of PHI Requiring Patient Authorization or Opportunity to Object 1.7

H. Information Providers Can Release Freely 1.8

## IX. INTERNET RESOURCES 1.8

### FORMS & APPENDIXES

<table>
<thead>
<tr>
<th>Form Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR 1-A</td>
<td>Acronyms</td>
</tr>
<tr>
<td>PR 1-B</td>
<td>HIPAA Standard Regarding De-Identification and Re-Identification of PHI</td>
</tr>
<tr>
<td>PR 1-C</td>
<td>HIPAA Standard Regarding Limited Data Set</td>
</tr>
</tbody>
</table>
CHAPTER 1

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, the Patient Access to Health Records Act (PAHRA), and other laws. At the federal level, there is the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (including special restrictions for psychotherapy notes), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and special provisions for federally-assisted substance abuse programs.

This chapter will help you understand the different laws that apply 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.

Readers should be aware that, at the time of publication of this manual, the U.S. Department of Health and Human Services is working on new and revised regulations under HIPAA and HITECH, which may alter the information provided in this manual. Readers should consult their legal counsel for updates.

II. STATE PRIVACY LAWS

A. CONFIDENTIALITY OF MEDICAL INFORMATION ACT

The Confidentiality of Medical Information Act (CMIA) is California’s general health information privacy law. It was enacted in 1979 and applies to most health care providers, including hospitals, skilled nursing facilities, doctors, nurses, pharmacists, and others. Two significant exceptions to CMIA’s application are federally-assisted substance abuse programs and those mental health care services covered by LPS. The CMIA limits the circumstances under which medical information may be used or disclosed [Civil Code Section 56 et seq.]. 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, government-operated hospitals and clinics, and health care providers serving involuntarily detained mental health patients — are exempt from the CMIA and instead must follow the stricter confidentiality provisions of LPS. (Mental health services provided in a private office setting are governed by CMIA and not LPS.) The LPS confidentiality provisions were written in 1969, when the mental health system was quite different from what it is today. As a result, some of the provisions are somewhat outdated. Like the CMIA, LPS limits the circumstances under which health information may be disclosed [Welfare and Institutions Code Section 5328 et seq.]. 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 B. “HIV Test Results,” page 4.6.

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. In 2000, this law was expanded to allow patients to request a correction, or to add an addendum, to their medical record if they believe the record contains incorrect information. Chapter 3 of this manual discusses patients’ rights under California law to access their medical information, request a correction to their medical record, or add a statement to their medical record. The HIPAA rights to access and amend are also discussed in chapter 3.

E. SOCIAL SECURITY NUMBERS

California has enacted a law prohibiting various uses of Social Security numbers (SSN). It is illegal for any person or business to do any of the following:

1. Publicly post or display an individual’s SSN.
2. Require an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted.
3. Require an individual to use his or her SSN to access a website, unless a password or unique personal identification number or other authentication device is also required to access the site.
4. Print an individual’s SSN on any materials mailed to that individual, unless state or federal law requires the
SSN to be on the document to be mailed. This includes hospital bills mailed to the individual. An exception exists for applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSN. However, the SSN may not be printed in whole or in part on any post card or mailer without an envelope, or visible in any way without the envelope having been opened.

5. Print an individual’s SSN on any card required for the individual to access products or services.

The SSN may not be encoded or embedded in a card or document using a barcode, chip, magnetic strip or other technology instead of removing the SSN as required by this law.

This law does not prevent the collection, use or release of a SSN as required by state or federal law, nor does this law prevent the use of a SSN for internal verification or administrative purposes.

[Civil Code Section 1798.85]

III. FEDERAL PRIVACY LAWS

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996 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 for the country’s health system.

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. A “preemption analysis” must be undertaken to determine which law to follow.

PREEMPTION ANALYSIS

The California Hospital Association has conducted a preemption analysis that 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).

Chapter 4 contains a discussion of HIPAA preemption rules and how to conduct a preemption analysis. In addition, chapters 4, 5 and 6 each contain a chart showing the results of the preemption analysis regarding, respectively, HIV test results, CMIA, and LPS.

B. 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 provisions is a breach notification requirement, additional restrictions on certain disclosures of PHI, and additional rights for patients regarding EHRs. In addition, the HITECH Act extends the HIPAA Privacy Rule and Security Rule to business associates of covered entities.

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.

Some of the regulations promulgated pursuant to the HITECH Act are integrated within the previously existing HIPAA regulations (within the Privacy Rule and the Security Rule). Therefore, the terms “HIPAA regulations,” “Privacy Rule” and “Security Rule” may include regulations promulgated pursuant to the HITECH Act as well as pursuant to HIPAA.

C. 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 patients served by “federally-assisted programs.” These rules are described in detail in chapter 7 of this manual.

IV. STATE AND FEDERAL SECURITY LAWS
Both state and federal laws address health information security issues in the health care context.

A. FEDERAL LAWS
The HIPAA Privacy Rule, which was promulgated before the HIPAA Security Rule, contains a broad, general security provision that applies to all individually-identifiable health information in the hands of covered entities. The rule requires covered entities to have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. This broad mandate applies to PHI in all forms, paper and electronic. Compliance with the HIPAA Security Rule will ensure compliance with the security provision of the HIPAA Privacy Rule.

On Feb. 20, 2003, DHHS published a separate rule containing standards for the security of electronic health information (the “Security Rule”). For most covered entities, the deadline for complying with the Security Rule was April 20, 2005.

BACKGROUND
The Security Rule applies to a wide range of health care providers and health plans that have greatly varying operations and technical capabilities. It is intended to be flexible and scalable, and gives providers broad discretion in the choice and implementation of technology. Covered entities may use any security measures that allow reasonable and appropriate implementation of the standards. In deciding which security measures to use, a covered entity must take into account the following factors:

1. The size, complexity, and capabilities of the covered entity;
2. The covered entity’s technical infrastructure, hardware, and software security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to electronic PHI.

This approach emphasizes security management as an ongoing process of assessing and balancing the vulnerabilities of health information against the costs of protecting against them.

GENERAL REQUIREMENTS
The Security Rule requires a covered entity to:

1. Appoint a security officer to make sure security procedures are developed, adopted and followed.
2. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.
3. Protect against any reasonably-anticipated threats or hazards to the security or integrity of the information.
4. Protect against any reasonably-anticipated uses or disclosures of the information that are not permitted or required under the Privacy Rule.
5. Ensure compliance by workforce members.

These broad requirements are amplified in administrative, physical, and technical standards. Most of the standards also have more detailed implementation specifications. These specifications are either “required” or “addressable.” Required specifications must be implemented. When a standard includes addressable specifications, a covered entity must assess whether each specification is a reasonable and appropriate safeguard in its environment, and determine whether to implement it, implement an alternative measure to accomplish the same goal, or not implement it. The covered entity must document its determination for each addressable specification.

The Security Rule is discussed in detail in chapter 10 of this manual.

B. STATE LAWS
Although California has adopted some provisions addressing security, the provisions are fairly broad and nonspecific. Compliance with the HIPAA Security Rule will generally ensure compliance with the California statutes. However, California providers must also comply with a new provision, effective Jan. 1, 2012, that requires EHRs to automatically record and preserve any change or deletion of any electron-
ically-stored medical information (in other words, to automatically generate and store detailed audit trails). Chapter 10 includes a discussion of California security requirements.

V. STATE AND FEDERAL BREACH NOTIFICATION LAWS

The HITECH Act includes a requirement to report privacy breaches to patients and to the federal government, effective Sept. 23, 2009. 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.

It is important to note that the requirements under state and federal breach notification laws are different in many significant respects with regard to what constitutes a breach, what needs to be reported, to whom, and in what time frame. Providers must analyze each potential breach under the two state laws and one federal law to determine the appropriate actions to take. Penalties also differ and, in some circumstances, employees who knowingly access, use or disclose PHI without a valid reason can be held personally liable.

The breach reporting laws are described in detail in chapter 12 of this manual.

VI. GOVERNMENT-OWNED HOSPITALS

This portion of the manual briefly describes privacy laws that apply to the federal and state governments. These laws are not discussed in detail in this manual. Hospitals that are government-owned should consult with legal counsel regarding specific requirements of these laws.

A. THE FEDERAL PRIVACY ACT OF 1974

The federal Privacy Act of 1974 [5 U.S.C. Section 552a] controls the collection and dissemination of information about an individual by federal government agencies. The federal Privacy Act establishes the subject’s rights to access and to request amendment to the records. The federal Privacy Act does not apply to nonfederal public hospitals or private hospitals. It does, however, apply to federal hospitals and entities performing “governmental functions” (e.g., Medicare and Medicaid fiscal intermediaries).

B. FEDERAL FREEDOM OF INFORMATION ACT

The federal Freedom of Information Act governs the public’s access to records kept by federal government agencies. This law does not seem to afford any greater access to records than permitted under the Federal Privacy Act of 1974. [5 U.S.C. Section 552]

C. STATE EXECUTIVE ORDER B-22-76

Executive Order B-22-76 governs the acquisition and use of data pertaining to individuals by state government agencies. It does not apply to municipal, county, district, University of California, private nonprofit or proprietary hospitals. It does, however, apply to hospitals operated by agencies within the executive branch of state government not created by constitutional provision (e.g., hospitals operated by the Department of Social Services and the Department of Veterans Affairs).

D. STATE AGENCIES

Medical information in the possession of a state office, officer, department, division, board, commission or other state government agency (including a state hospital), except the Legislature, judiciary and State Compensation Fund, is subject to the CMIA’s requirements, as well as those requirements imposed by the California Information Practices Act of 1977, found at Civil Code Section 1798 et seq. [Civil Code Section 56.29]

E. CALIFORNIA PUBLIC RECORDS ACT

The California Public Records Act governs access to records kept by state and local agencies. It does not apply to private hospitals. Most, if not all, medical records are exempt from disclosure under the California Public Records Act. If a request for information is made pursuant to the California Public Records Act, the hospital’s legal counsel should be consulted. [Government Code Sections 6250-6276.48]

VII. ENFORCEMENT AND PENALTIES

This section briefly describes the various government entities that are responsible for enforcing privacy and security laws, and who may bring lawsuits against providers for violation of the laws. (See chapters 12 and 13 for detailed information about breaches, enforcement, and potential penalties.)

A. FEDERAL LAWS

Responsibility for enforcing the HIPAA Privacy and Security Rules rests with the DHHS Office for Civil Rights (OCR). Any person, organization, or group that believes that an entity has violated HIPAA may file a complaint. The complainant does not need to be the subject of the PHI. Therefore, complainants may include a provider’s employees, business associates, or patients, as well as accrediting, health oversight or advocacy agencies. OCR is also required by law to conduct random audits and compliance reviews.

Noncompliance with the HIPAA rules has serious potential implications. HIPAA provides for fines of up to $50,000 per violation and criminal penalties of up to 10 years in prison.
INDEX

A
AB 211, 12.4, 13.11
Abuse
  Child, 5.13, CMIA.2, CMIA.4, 6.12, LPS.5,
  LPS.6, 7.7
  Elder and dependent adult, CMIA.3, CMIA.5,
  6.12, LPS.7
Accounting of disclosures, 3.14 to 3.15
Fees, 3.15
Accreditation organization, 5.11, CMIA.4
Administrative agency, CMIA.5, CMIA.7
Administrative safeguards, 10.3
Admission, notifying relatives of, 5.16, 6.15 to 6.16,
  LPS.14
Advocates, mental health, 6.16 to 6.22, LPS.1 to LPS.40
Affirmative defense, 13.5, 13.8
Alcohol and drug abuse records, 5.20, 7.1 to 7.12
  Definition of, 4.14
Amendment of PHI, 3.12 to 3.13
Arbitration, 5.7
Assault, CMIA.3
Attorney, 5.6, CMIA.28, 6.4, LPS.28
Audit, 2.5, 13.3
Audit trails, 10.5
Authorization
  Compound, 4.4
  Employee health record, 9.7
  For use or disclosure, 4.2 to 4.9, 5.4 to 5.7,
    6.3 to 6.5, 7.5, 8.2
  Revocation, 4.4, 7.6

B
Boards — See also Medical Board of California
  Institutional Review, 8.4
  Licensing, 6.11
  Privacy, 8.4
Breach, 1.4, 12.1 to 12.14
  Committee, 2.2
  Unencrypted computerized data, 12.2
Business associates, CMIA.6, 11.1 to 11.10
  Breach, 11.5, 12.7 to 12.8, 12.14
Contracts, 2.5
  Policies, 2.3
  Required provisions, 11.3 to 11.6
  Definition of, 11.1

C
California Department of Public Health (CDPH), 5.3,
  6.10, LPS.38, 12.4, 12.7, 13.10
California Department of Social Services (CDSS), 6.10,
  LPS.38
Celebrities, 5.25
Committees
  Legislative, 6.11, LPS.27
  Quality assurance, 6.11
Complaint, 2.1, 2.3, 2.4, 3.3, 13.1 to 13.2
Compliance reviews, 13.2
Condition, notifying relatives of, 5.16, 6.15 to 6.16
Confidentiality of Medical Information Act (CMIA),
  1.1, 5.1 to 5.42, 9.7, 13.7
  Information not subject to, 5.2 to 5.4
Conservatorship proceeding, CMIA.7, CMIA.9, 6.6,
  LPS.9
Contractor
  Definition of, 4.13
Coroner, 5.8, 5.12, CMIA.7, CMIA.9, 6.14, LPS.10
Correctional agencies, 6.10, LPS.16
County patients’ rights advocates, 6.19 to 6.22, LPS.29
County social worker, 5.15, 6.6, LPS.10
Court order, 4.7, 5.7, 5.39, CMIA.8, CMIA.10,
  6.13 to 6.14, LPS.11, 7.9
Covered entities
  Definition of, 1.5
Credit reports, 10.6
Crime
  On program premises, 6.7 to 6.8, 7.7, LPS.18,
    LPS.19
Criminal investigation, 6.9, 13.5

D
Data aggregation services
  Definition of, 11.6
Death, notifying relatives of, 5.16, 6.15 to 6.16
Death review teams, CMIA.8, CMIA.10, 6.13
Deceased patients, 4.2, CMIA.9, 7.6, 8.6 to 8.7
De-identified PHI, 8.1, 8.7
Deletion of medical information, 10.5
Department of Health and Human Services (DHHS) —
  See DHHS
Department of Insurance, 5.3
Department of Justice (DOJ), 6.8, LPS.22

NOTE: Index terms that originated in the Preemption Analysis begin
with the acronym reflective of that analysis. For example, “Preemption
Analysis: HIV Test Results” is indexed as HIV; “Preemption Analysis:
Patients Covered by CMIA” is indexed as CMIA; and “Preemption
Analysis: Patients Covered by LPS” is index as LPS.
NOTE: Index terms that originated in the Preemption Analysis begin with the acronym reflective of that analysis. For example, “Preemption Analysis: HIV Test Results” is indexed as HIV; “Preemption Analysis: Patients Covered by CMIA” is indexed as CMIA.; and “Preemption Analysis: Patients Covered by LPS” is index as LPS.
I

Immunization information, 5.39
Incapacitated patients, 4.2, 5.25, 6.3, 7.6
Incidental uses and disclosures, 1.7
Individually-identifiable health information
Definition of, 4.1, 5.1, 5.4
Injury, CMIA.3, CMIA.13 — See also Workers’ compensation
Inmate, 3.4, 5.16, CMIA.16
Institutional Review Boards (IRB), 8.4
Insurer, CMIA.17, CMIA.19, 6.6

L

Lab test results, 3.11 — See also Human Immunodeficiency Virus (HIV), Tuberculosis screening
Lanterman-Petris-Short Act, 1.1, 6.1 to 6.24, 13.9
Law enforcement, 5.2, 5.38 to 5.39, CMIA.19, CMIA.21, 6.7, 6.10, LPS.16, LPS.23
Delay, 12.3, 12.6, 12.11
Subpoena, CMIA.17
Legislative committee, 6.11, LPS.27
Liability insurer, 5.5, 5.11
Licensed health care professional
Definition of, 4.13
Licensing, 5.11, CMIA.21
Boards, 6.11, LPS.32
Limited data set, 1.8, 8.1, 8.8

M

Managed Risk Medical Insurance Board, 5.3
Marketing, 4.8, 5.4, CMIA.22
Media, 5.23 to 5.25, CMIA.25, 12.3, 12.13
Medi-Cal, 5.2
Medical Board of California, 5.7
Medical emergencies, 7.7 to 7.8
Medical information
Definition of, 4.14, 5.2
Medical staff, 2.5
Mental health advocates, 6.16 to 6.22, LPS.29 to LPS.31
Mental health patient
Minors, 5.20
Records, 3.10, 4.14, 6.1 to 6.24, LPS.1 to LPS.40
Mental health records, 4.5, 5.2, 5.17
Military, 5.16, CMIA.26
Minimum necessary, 4.10 to 4.11, 7.4, 8.3
Minor, 3.8, 5.19 to 5.23, 6.6, LPS.10, 7.5 to 7.6
Mitigate, 12.1
Multidisciplinary personnel teams, CMIA.6, CMIA.8, CMIA.11, 6.12, 6.13, LPS.5, LPS.7

N

National security, 5.16, CMIA.27
Noncustodial parent, 5.21
Notice of Privacy Practices, 2.3, 3.1, 3.1 to 3.3, 3.14

O

Occupational exposures, HIV.6, 9.4
Office for Civil Rights (OCR) — See DHHS
Office of Health Information Integrity (OHII), 13.11
Organized health care arrangement, 2.2, 3.4, 11.3
Organ procurement organization, 5.13, CMIA.27 — See also Tissue bank

P

Parent — See also Personal representative
Foster, 5.21
Noncustodial, 5.22
Patient Access to Health Records Act, 1.1, 3.4
Patient access to PHI, 3.4 to 3.12
Fees, 3.7
Patient-authorized disclosures, 6.5 — See also Authorization
Patient records
Definition of, 4.14
Patients’ rights advocates, 6.19 to 6.22, LPS.29 to LPS.31
— See also Mental health advocate
Payment, 5.10, 6.6, LPS.31 — See also Insurer
Definition of, 5.9
Peer review, 5.11, CMIA.29, CMIA.31
Penalties, 13.1 to 13.12
Personal representative, 3.4, 3.8, 3.11, 4.2, 6.3, LPS.33 — See also Authorization
Photocopying services, 5.6
Physical safeguards, 10.3
Policies and procedures, 2.3 to 2.5
Preemption, 4.1
Analysis, 1.2, 4.11 to 4.16, 5.1
General patient, CMIA.1 to CMIA.36
HIV Test Results, HIV.1 to HIV.6
Mental health and developmental disabilities, 6.1, LPS.1 to LPS.40
Prisoners — See Inmate
Privacy
Boards, 8.4
Officer, 2.1
Rights, 3.1
Privacy Act of 1974, 1.4
Privileged information, 5.26 to 5.27, 6.14
Probate court investigation — See Conservatorship proceeding
Probation officer, 5.15, 6.4, 6.6, LPS.10, LPS.32
Protected health information (PHI)
Amendment of, 3.12 to 3.13
Definition of, 4.1
Patient access to, 3.4 to 3.12
Fees, 3.7
Sale of, 4.9
Unsecured, 12.9
Protection and advocacy, 6.16 to 6.22, LPS.1 to LPS.40, LPS.29 to LPS.31
Protective order, 5.29
Provider of health care
Definition of, 4.13
Psychiatric records, 6.1 to 6.24, LPS.1 to LPS.40 — See also Psychotherapy notes
Psychotherapy notes, 3.9 to 3.17, 4.5 to 4.16, 5.4, 6.19, LPS.3
Definition of, 4.5
Public health, 5.14, CMIA.30
Public Records Act, 1.4

Q
Quality assurance committee, 6.11, LPS.33

R
“Red Flags” rules, 10.7 to 10.8
Redisclosure, 3.6, 5.42, 6.19, 7.5, 8.6, 9.7
Re-identification, 1.8, 8.8
Remote access, 8.5, 10.1
Research, 5.12, CMIA.32, 6.6, LPS.35, 7.8, 8.1 to 8.10
     Compliance checklist, 8.9
Residential shelter services, 5.20
Retaliation, 2.4, 2.5, 13.1
     Anti-retaliation policy, 2.4
Risk assessment, 10.2, 12.10
Ryan White CARE Act, 4.7, HIV.5, 6.13, LPS.37

S
Safe surrender of newborn, 5.22
Sanctions, employees, 2.3, 2.5, 12.1
SB 541, 12.4, 13.10
Security, health information, 10.1 to 10.8
Security officer, 2.1
Self-sufficient minor, 5.20
Sexual assault, 5.20
Social Security numbers, 1.1
Social worker, 5.15, 6.6, LPS.10
Special restriction, 3.15 to 3.17
     Method of communication, 3.17
     Services paid in full, 3.16
Subpoena, 4.8, 5.26 to 5.38, CMIA.35, CMIA.36, 6.14, 7.9 to 7.11
     Administrative agency, 5.36, CMIA.18
     Criminal, 5.37
     Fees, 5.35
     Investigative, 5.7
     Law enforcement, CMIA.17
Substance abuse records, 5.2, 7.1 to 7.12

T
Tarasoff warnings, 5.15, CMIA.31, 6.11 to 6.12, LPS.26
Technical safeguards, 10.4
Third party payer — See Insurer
Tissue bank, 5.13, CMIA.27 — See also Organ procurement organization
TPO (treatment, payment, health care operations), 5.10
Trading partner agreement
     Definition of, 11.7
Trainees, 2.3
Training, 2.3 to 2.4
Transfer, notifying relatives of, 6.15 to 6.16
Treatment, 5.10, 6.5, LPS.40
     Definition of, 5.9
Treatment, payment, health care operations (TPO), 5.10
Tuberculosis screening, 5.41

U
Unencrypted computerized data, 1.4, 12.2
Use
     Authorization for — See Authorization
     Definition of, 4.2

V
Verification procedures, 3.8, 4.9 to 4.10, 7.4
Violence against hospital personnel, CMIA.3
Volunteers, 2.3, 2.5

W
Warrant, 5.7, 5.39, CMIA.18, 6.10, LPS.23
Whistleblowers, 2.5
Workers’ compensation, 5.3, 5.12, CMIA.36, CMIA.36
Workforce
     Definition of, 2.3
Workplace exposures — See Occupational exposures

NOTE: Index terms that originated in the Preemption Analysis begin with the acronym reflective of that analysis. For example, “Preemption Analysis: HIV Test Results” is indexed as HIV; “Preemption Analysis: Patients Covered by CMIA” is indexed as CMIA.; and “Preemption Analysis: Patients Covered by LPS” is index as LPS.