PUBLICATIONS

Several helpful publications are available through CHA including:

* California Health Information Privacy Manual
* California Hospital Compliance Manual
* California Hospital Survey Manual — A Guide to the Licensing & Certification Process
* Consent Manual
* EMTALA — A Guide to Patient Anti-Dumping Laws
* Guide to Release of Patient Information
* Healthcare Workplace Violence Prevention
* Mental Health Law
* Minors & Health Care Law
* Model Medical Staff Bylaws & Rules
* Principles of Consent and Advance Directives
* Record and Data Retention Schedule
* The Cal/OSHA Safe Patient Handling Regulation

Plus numerous web seminar recordings available on CD, human resource and volunteer publications.

ORDERING INFORMATION

For more information, visit CHA online at

www.calhospital.org/publications

This publication is designed to produce accurate and authoritative information with regard to the subject matter covered. It is sold with the understanding that CHA is not engaged in rendering legal service. If legal or other expert assistance is required, the services of a competent professional person should be sought.

*California Health Information Privacy Manual*


Originally published as *The California Patient Privacy Manual*

© 2002, 2004 by the California Healthcare Association

All rights reserved. First edition 2002.


No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise (with exception of the forms, tables and appendices), without the prior written approval of:

California Hospital Association
Publishing Department
1215 K Street, Suite 800
Sacramento, CA 95814

Mary Barker, Vice President, Publishing and Education
Lois J. Richardson, Esq., Vice President, Privacy and Legal Publications/Education
Bob Mion, Director, Publishing and Marketing
Emily Stone, Publishing Manager

**It is the intent of CHA to strictly enforce this copyright.**

Published by the California Hospital Association.
Printed in the United States of America.
QUICK REFERENCE GUIDE

- Preface
- 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 Special Issues
Chapter 5 .......... Use and Disclosure of PHI: CMIA Patients
Chapter 6 .......... Use and Disclosure of PHI: LPS Patients
Chapter 7 .......... Use and Disclosure of PHI: Substance Abuse Patients
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.


In addition, CHA offers web seminars and posts information on the CHA website at www.calhospital.org/privacyhipaa.

Many thanks to 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.

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 email.

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 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.
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 or at www.law.cornell.edu.

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 or at www.ecfr.gov. 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 or at www.federalregister.gov.

The Centers for Medicare & Medicaid Services publishes its Interpretive Guidelines for surveyors on the internet. They may be found at www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo. 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 Managed Health Care. 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_Register.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

<table>
<thead>
<tr>
<th>Form</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>

### 3. Privacy Rights and Notice of Privacy Practices

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-1S</td>
<td>Notice of Privacy Practices: Acknowledgment of Receipt</td>
</tr>
<tr>
<td>15-2S</td>
<td>Model Notice of Privacy Practices</td>
</tr>
<tr>
<td>15-3S</td>
<td>Model Notice of Privacy Practices (For Mental Health Information Subject to the Lanterman-Petris-Short Act)</td>
</tr>
<tr>
<td>15-4S</td>
<td>Request to Amend Protected Health Information</td>
</tr>
<tr>
<td>15-5S</td>
<td>Response to Request to Amend Protected Health Information</td>
</tr>
<tr>
<td>15-6</td>
<td>Notification of Amendment to Protected Health Information</td>
</tr>
<tr>
<td>15-7S</td>
<td>Statement of Disagreement/Request to Include Amendment Request and Denial with Future Disclosures</td>
</tr>
<tr>
<td>15-8S</td>
<td>Request for an Accounting of Disclosures</td>
</tr>
<tr>
<td>15-9S</td>
<td>Response to Request for an Accounting of Disclosures</td>
</tr>
<tr>
<td>15-10S</td>
<td>Request for Special Restriction on Use or Disclosure of Protected Health Information</td>
</tr>
<tr>
<td>15-11S</td>
<td>Response to Request for Special Restriction on Use or Disclosure of Protected Health Information</td>
</tr>
<tr>
<td>15-12S</td>
<td>Termination of Special Restriction</td>
</tr>
<tr>
<td>15-13S</td>
<td>Request for Alternative Means of Communication</td>
</tr>
<tr>
<td>PR 3-A</td>
<td>Disclosures That Must Be Accounted For</td>
</tr>
</tbody>
</table>

### 4. Use and Disclosure of PHI: Fundamentals and Special Issues

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-1S</td>
<td>Authorization for Use or Disclosure of Health Information</td>
</tr>
<tr>
<td>24-5S</td>
<td>Request for Presence of Observer During Childbirth/Medical Procedure</td>
</tr>
</tbody>
</table>

### 5. Use and Disclosure of PHI: CMIA Patients

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-2S</td>
<td>Request to Withhold Public Release of Information</td>
</tr>
<tr>
<td>16-3</td>
<td>Response to Subpoena Duces Tecum</td>
</tr>
<tr>
<td>16-4</td>
<td>Time Extension for Compliance with Subpoena</td>
</tr>
<tr>
<td>16-5</td>
<td>Affidavit of Custodian of Medical Records to Accompany Copies of Records</td>
</tr>
<tr>
<td>16-6</td>
<td>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)</td>
</tr>
<tr>
<td>16-7</td>
<td>Civil Subpoena (Duces Tecum)</td>
</tr>
<tr>
<td>16-8</td>
<td>Deposition Subpoena for Personal Appearance and Production of Documents and Things</td>
</tr>
<tr>
<td>16-9</td>
<td>Deposition Subpoena for Production of Business Records</td>
</tr>
<tr>
<td>16-10</td>
<td>Notice to Consumer or Employee and Objection</td>
</tr>
<tr>
<td>16-11</td>
<td>Authorization for Disclosure of Health Information Pursuant to Evidence Code Section 1158</td>
</tr>
</tbody>
</table>

### 6. Use and Disclosure of PHI: LPS Patients

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-1</td>
<td>Response to Request for Confidential Information</td>
</tr>
<tr>
<td>17-2</td>
<td>Order for Production of Mental Health records</td>
</tr>
</tbody>
</table>

### 7. Use and Disclosure of PHI: Substance Abuse Patients

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-1</td>
<td>Substance Abuse Program Notice of Prohibition of Redisclosure</td>
</tr>
<tr>
<td>18-A</td>
<td>Order for Production of Substance Abuse Records</td>
</tr>
<tr>
<td>18-BS</td>
<td>Notice to Patient: Confidentiality of Substance Abuse Patient Records</td>
</tr>
</tbody>
</table>

### 10. Health Information Security

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR 10-A</td>
<td>HIPAA Security Standards Matrix</td>
</tr>
</tbody>
</table>

### 11. Business Associate Contracts

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR 11-B</td>
<td>Business Associate Addendum</td>
</tr>
</tbody>
</table>

### 12. Breaches

<table>
<thead>
<tr>
<th>Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR 12-A</td>
<td>Federal and State Breach Notification Laws for California</td>
</tr>
<tr>
<td>PR 12-B</td>
<td>HIPAA Breach Decision Tool and Risk Assessment Documentation Form</td>
</tr>
<tr>
<td>PR 12-C</td>
<td>Questionnaire and Confidentiality Agreement (Paper or Verbal PHI)</td>
</tr>
<tr>
<td>PR 12-D</td>
<td>Questionnaire and Confidentiality Agreement (Electronic PHI)</td>
</tr>
</tbody>
</table>

---

**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. Spanish Forms can be found on the enclosed CD.
# 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
F. Driver’s License Information .......................................................... 1.2
  Organ Procurement Organizations ................................................. 1.2
G. Limitations on Collection of Information When Accepting Payment by Check or Credit Card ...... 1.3
  Check ......................................................................................... 1.3
  Credit Card ................................................................................. 1.3

## III. FEDERAL PRIVACY LAWS 1.4

A. Health Insurance Portability and Accountability Act of 1996 ............. 1.4
  Preemption Analysis ....................................................................... 1.4
B. The Health Information Technology for Economic and Clinical Health Act ........................................... 1.5
C. Substance Abuse Programs ............................................................. 1.5
D. CMS CoP and Interpretive Guidelines for Patient Privacy .................. 1.5
  Overview ..................................................................................... 1.5
  Physical Privacy ........................................................................... 1.5
  Health Information Privacy ............................................................ 1.6
  Survey Procedures ........................................................................ 1.6
E. Telephone Consumer Protection Act .............................................. 1.6
  Overview ..................................................................................... 1.6
  Residential Lines .......................................................................... 1.7
  Cell Phones .................................................................................. 1.9
  Faxes ............................................................................................ 1.9
  Requirements for Artificial and Prerecorded Voice Messages .......... 1.9
  Obtaining Consent ....................................................................... 1.9
  Caution: Reassigned Phone Numbers and Wrong Numbers .......... 1.10
  Compliance Tips .......................................................................... 1.10

## IV. STATE AND FEDERAL SECURITY LAWS 1.11

A. Federal Laws ................................................................................ 1.11
  Background .................................................................................. 1.11
  General Requirements ................................................................... 1.11
B. State Laws ................................................................................... 1.11

## V. STATE AND FEDERAL BREACH NOTIFICATION LAWS 1.12

## VI. GOVERNMENT-OWNED HOSPITALS 1.12

A. The Federal Privacy Act of 1974 .................................................... 1.12
B. Federal Freedom of Information Act ............................................. 1.12
C. State Executive Order B-22-76 ....................................................... 1.12
D. State Agencies ............................................................................. 1.12
E. California Public Records Act ....................................................... 1.12

## VII. ENFORCEMENT AND PENALTIES 1.12

A. Federal Laws ................................................................................ 1.12
B. State Laws ................................................................................... 1.13

## VIII. HEALTH INFORMATION PRIVACY BASICS 1.13

A. Who Must Comply? ...................................................................... 1.13
B. What Do the Laws Require Providers to Do? ............................... 1.13
C. What Information is Protected? .................................................... 1.14
  Minimum Necessary ..................................................................... 1.14
D. Patient Privacy Rights .................................................................. 1.14
E. Providers Can Use or Disclose PHI for “Treatment, Payment, and Health Care Operations” Without Patient Authorization ......................................................... 1.15
F. Other Required or Permitted Uses and Disclosures of PHI Without Patient Authorization ................................................................. 1.16
  Incidental Uses and Disclosures .................................................... 1.16
G. Use and Disclosure of PHI Requiring Patient Authorization or Opportunity to Object ................................................................. 1.17
H. Information Providers Can Release Freely .................................... 1.17
  De-Identified Information ............................................................. 1.17
  Limited Data Set ......................................................................... 1.17

## IX. INTERNET RESOURCES 1.17
### FORMS & APPENDIXES

<table>
<thead>
<tr>
<th>PR 1-A</th>
<th>Acronyms</th>
</tr>
</thead>
<tbody>
<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 many 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, special provisions for federally-assisted substance abuse programs, and other laws.

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 to revise the regulations regarding accounting for disclosures, 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 LPS 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 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 for patients to access and amend their records 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 law applies to 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.

6. Sell, advertise for sale, or offer to sell an individual’s SSN. “Sell” does not include the release of a SSN incidental to a larger transaction if necessary to identify the individual to accomplish a legitimate business purpose. “Sell” also does not include the release of a SSN for purposes specifically authorized by state or federal law. Release of a SSN for marketing purposes is not permitted.

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]

California law also requires employers to print no more than the last four digits of an employee’s social security number on pay stubs or itemized statements. Alternatively employers may use employee identification number other than the social security number. [Labor Code Section 226(a)]

F. DRIVER’S LICENSE INFORMATION

California law limits the manner in which a business may use a driver’s license or DMV identification card. A “business” is defined as “a proprietorship, partnership, corporation, or any other form of commercial enterprise,” and thus includes a private (non-governmental) hospital.

A business may swipe a driver’s license or identification card issued by the Department of Motor Vehicles in an electronic device for the following purposes only:

1. To verify age or the authenticity of the driver’s license or identification card.

2. To comply with a legal requirement to record, retain, or transmit that information.

3. To transmit information to a check service company for the purpose of approving negotiable instruments, electronic funds transfers, or similar methods of payments, provided that only the name and identification number from the license or the card may be used or retained by the check service company.

4. To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation.

A business may not retain or use any of the information obtained by that electronic means for any purpose other than as provided herein. A violation of this law constitutes a misdemeanor punishable by imprisonment in a county jail for no more than one year, or by a fine of no more than ten thousand dollars ($10,000), or by both. [Civil Code Section 1798.90.1]

This law does not prohibit examining a driver’s license or DMV identification card, and does not prohibit photocopying the card and retaining the photocopy.

ORGAN PROCUREMENT ORGANIZATIONS

An organ procurement organization (OPO) designated by the Secretary of the U.S. Department of Health and Human Services may swipe a driver’s license or identification card issued by the DMV in an electronic device to transmit information to the Donate Life California Organ and Tissue Donor Registry to allow a person to identify himself or herself as a registered organ donor (see Health and Safety Code Section 7150.90). Information gathered or transmitted pursuant to this law must comply with the DMV Information Security Agreement.

Prior to swiping the license or ID card, the OPO must provide clear and conspicuous notice to the applicant and follow the procedure described below.

1. Once the applicant’s information is populated on the electronic form, the applicant must verify that the information is accurate and click “submit” after reading a clear and conspicuous consent message, which may not be combined with or contained within another message, acknowledging that the applicant’s information will be used for the sole purpose of being added to the registry.

2. The applicant must provide his or her signature to complete registration.

3. The organization or registry system must provide a written confirmation to the applicant confirming that he or she is signed up as an organ and tissue donor.
4. A business or OPO may not retain or use any of the information obtained by that electronic means for any purpose other than as provided herein.

“Organ procurement organization” means a person as an organ procurement organization.

G. LIMITATIONS ON COLLECTION OF INFORMATION WHEN ACCEPTING PAYMENT BY CHECK OR CREDIT CARD

CHECK
When accepting a check as payment for goods or services, a person or business may not:

1. Require the person paying by check to provide a credit card as a condition of accepting the check, or record the number of a credit card.
2. Require the person paying by check to sign a statement agreeing to allow his or her credit card to be charged to cover the check if returned as no good.
3. Record a credit card number in connection with any part of the transaction.
4. Contact a credit card issuer to determine if the amount of any credit available to the person paying by check will cover the amount of the check.

This law does not prohibit the following:

1. Requiring the production of reasonable forms of positive identification (other than a credit card), such as a driver’s license or a California state identification card, or where one of these is not available, another form of photo identification, as a condition of accepting a check.
2. Requesting, but not requiring, a purchaser to voluntarily display a credit card as an indicia of creditworthiness or financial responsibility, or as an additional identification, provided the only information concerning the credit card that is recorded is the type of credit card displayed, the issuer of the card, and the expiration date of the card. If a business requests the display of a credit card, the business must inform the customer, by either of the following methods, that displaying the credit card is not a requirement for check writing:
   a. By posting the following notice in a conspicuous location in the unobstructed view of the public within the premises where the check is being written, clearly and legibly: “Check writing ID: credit card may be requested but not required for purchases.”
   b. By training and requiring their employees who request the credit card to inform all check writing customers that they are not required to display a credit card to write a check.
3. Requesting production of, or recording, a credit card number as a condition for cashing a check.
4. Requesting, receiving, or recording a credit card number in lieu of requiring a deposit to secure payment in event of default, loss, damage, or other occurrence.
5. Requiring, verifying, and recording the purchaser’s name, address, and telephone number.
6. Requesting or recording a credit card number on a check used to make a payment on that credit card account.

A violation of this law is subject to a civil penalty not to exceed two hundred fifty dollars ($250) for a first violation, and not to exceed one thousand dollars ($1,000) for a second or subsequent violation. However, no civil penalty may be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant’s maintenance of procedures reasonably adopted to avoid such an error.

[Civil Code Section 1725]

CREDIT CARD
No person, firm, partnership, association, or corporation that accepts credit cards may do the following:

1. Request, or require as a condition to accepting the credit card as payment, the cardholder to write any personal identification information upon the credit card transaction form or otherwise.
2. Request, or require as a condition to accepting the credit card as payment, the cardholder to provide personal identification information, which the business accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise.
3. Utilize, in any credit card transaction, a credit card form that contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder.

Definitions
For purposes of this law “personal identification information,” means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder’s address and telephone number.
This law does not apply in the following instances:

1. If the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar occurrence.
2. Cash advance transactions.
3. If any of the following applies:
   a. The business accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction.
   b. The business accepting the credit card in a sales transaction at a retail motor fuel dispenser or retail motor fuel payment island automated cashier uses the Zip Code information solely for prevention of fraud, theft, or identity theft.
   c. The business accepting the credit card is obligated to collect and record the personal identification information by federal or state law or regulation.
4. If personal identification information is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of purchased merchandise, or for special orders.

This law does not prohibit a business from requiring the cardholder, as a condition to accepting the credit card as payment, to provide reasonable forms of positive identification, which may include a driver’s license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder’s driver’s license number or identification card number may be recorded on the credit card transaction form or otherwise.

A violation of this law is subject to a civil penalty not to exceed two hundred fifty dollars ($250) for the first violation and one thousand dollars ($1,000) for each subsequent violation. However, no civil penalty may be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant’s maintenance of procedures reasonably adopted to avoid that error.

[Civil Code Section 1747.08]

### 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. The regulations are often referred to as the “HIPAA Privacy Rule.”

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 patients greater privacy protection, or greater access to their own information. 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.
INDEX

A
AB 211, 12.5, 13.12
Abuse
    Child, 5.12, 5.22, 7.7
    Elder and dependent adult, 6.17
Accountable Care Organization (ACO), 2.3
Accounting of disclosures, 3.16 to 3.18
    Fees, 3.17
Accreditation organization, 5.20
Administrative agency, 5.5
Administrative safeguards, 10.3
Admission, notifying relatives of, 5.7, 6.19 to 6.21
Advocates, mental health, 6.21 to 6.27
Affirmative defense, 13.5, 13.10
Alcohol and drug abuse records, 5.9, 7.1 to 7.14
    Definition of, 4.15
Ambulance companies, release of patient information to, 5.22, 6.16
Amendment of PHI, 3.14 to 3.16
Arbitration, 5.5
Attorney, 5.14, 6.6
Audio monitoring, 1.5
Audit, 2.5, 13.3
Audit trails, 10.6
Authorization
    Compound, 4.4
    Employee health record, 9.3
    For use or disclosure, 4.2 to 4.9, 6.4 to 6.7, 7.5, 8.2
    Revocation, 4.5, 7.7
B
Boards — See also Medical Board of California
    Institutional Review, 8.4
    Licensing, 6.15
    Privacy, 8.4
Breach, 1.12, 12.1 to 12.18
    Committee, 2.2
    Unencrypted computerized data, 12.3
Business associates, 11.1 to 11.10
    Breach, 11.5, 12.9 to 12.10, 12.17
    Contracts, 2.7
        Policies, 2.4
        Required provisions, 11.4 to 11.6
C
California Department of Public Health (CDPH), 5.3, 6.14, 12.5, 12.9
California Department of Social Services (CDSS), 6.14
Celebrities, 5.28
Centers for Medicare & Medicaid Services (CMS), 1.5, 1.13
Certificates of confidentiality, 8.8
Check, 1.3
Childbirth, 4.25
Clergy, 5.23
Cloud service provider, 11.3
Committees
    Legislative, 6.15
    Quality assurance, 6.15
Complaint, 2.1, 2.4, 2.5 to 2.6, 3.3, 13.1 to 13.2
Compliance reviews, 13.2
Condition, notifying relatives of, 5.7, 6.19 to 6.21
Conditions of Participation (CoP), 1.5, 1.6
Confidentiality of Medical Information Act (CMIA), 1.1, 5.1 to 5.47, 9.3, 13.7
    Information not subject to, 5.2 to 5.4
Consent
    Observer of childbirth/medical procedure, 4.25 to 4.26
Conservatorship proceeding, 5.22, 6.8
Contractor
    Definition of, 4.13
Coroner, 5.5, 5.21
Correctional agencies, 6.14
County patients’ rights advocates, 6.24 to 6.27
County social worker, 5.10, 6.9
Court order, 4.8, 5.5, 5.43, 6.18 to 6.19, 7.10
Covered entities
    Definition of, 1.13
Credit card, 1.3
Credit reports, 10.7
Crime
    On program premises, 6.11, 7.7
Criminal investigation, 6.13, 13.6
D
Data aggregation services
    Definition of, 11.6
Death
    Release of information regarding, 5.1, 5.7, 7.4, 7.7
    Death, notifying relatives of, 5.7, 6.19 to 6.21
    Death review teams, 5.46, 6.17
Deceased patients, 4.3, 7.7, 8.6 to 8.7
De-identified PHI, 1.17, 8.1, 8.7
Deletion of medical information, 10.6
Department of Health and Human Services (DHHS) —
  See DHHS
Department of Insurance, 5.4
Department of Justice (DOJ), 6.11
Department of Managed Health Care, 5.3
Dependent child of juvenile court, 3.10, 6.6
Dependent child of the court, 5.10
Designated record set, 3.5
Destruction of medical information, 10.6
DHHS, 1.4, 5.7, 6.11, 8.2, 10.1, 12.16
  Audit program, 13.3
Disability Rights California (DRC), 6.21 to 6.27
Disappearance of patient, 6.12
Disaster
  Relief organization, 5.29
Discipline — See Employee sanctions
Disclosure
  Accounting of, 3.16 to 3.18
  Fees, 3.17
  Authorization for — See Authorization
  Definition of, 4.1
Disease management programs, 5.17
Disposal of medical information, 10.6
Documentation, 2.4, 2.7, 3.4, 3.14, 3.15, 3.18, 3.20, 10.3,
  12.9, 12.18 — See also Authorization
Domestic violence death review teams — See Death review teams
Driver’s License, 1.2
Duty to warn of dangerous psychiatric patient, 5.20, 5.25,
  6.16
Elder and dependent adult abuse, 6.17
  Release of information regarding, 5.25
Elder death review teams, 5.46
Elected officials, 6.11
Emergency Medical Services Authority, release of patient information to, 5.22, 6.16
Emergency personnel, release of patient information to, 5.22, 6.16
Employee
  Disciplinary proceedings, 6.10
  Group health plans, 9.3 to 9.5
  Handbook, 9.3
  Health information, 9.1 to 9.18
  Sanctions, 2.4, 2.6, 12.2, 13.8
Employer, 5.21, 6.7
Enforcement, 13.1 to 13.14
Escape of patient, 6.13

F
Fair and Accurate Credit Transactions (FACT), 10.7
Family, 5.7, 6.19 to 6.21
Family Educational Rights and Privacy Act, 4.2
Font size, 3.1, 3.3, 4.2
Food and Drug Administration (FDA), 5.22, 8.3
Foster care public health nurse, 5.10, 5.25, 6.9
Freedom of Information Act, 1.12
Friends, 5.7
Fundraising, 5.24
Funeral directors, 5.24

G
Genetic counseling, 6.7
Genetic Information Nondiscrimination Act, 9.5
Government-owned hospitals, 1.12
Grievance — See Complaint

H
Health care clearinghouse
  Definition of, 4.13
Health care provider
  Definition of, 4.13, 4.14
Health care service plan
  Definition of, 4.13
Health information
  Definition of, 4.15, 5.4
  Employee, 9.1 to 9.18
Health Information Technology for Economic and Clinical Health Act — See HITECH
Health Insurance Portability and Accountability Act of 1996 — See HIPAA
Health plan
  Definition of, 4.13
HIPAA, 1.4, 5.1
  Breach laws, 1.12, 12.10 to 12.18
  Compliance checklist for research, 8.10
  Mandatory disclosures, 5.7
  Permitted disclosures, 5.16
  Preemption rules, 4.12 to 4.18, 5.1
  Protective order, 5.33
  Security Rule, 1.11
HITECH, 1.1, 1.5, 12.10
Human Immunodeficiency Virus (HIV)
  Test results, 1.1, 4.6 to 4.9, 5.12
  Penalties for unlawful disclosure, 13.13

I
Immunization information, 5.44
Incapacitated patients, 4.2, 5.29, 6.5, 7.6
Incidental uses and disclosures, 1.16
Individually-identifiable health information
  Definition of, 4.1, 5.2, 5.4
Injury — See also Workers' compensation
Inmate, 3.4, 5.23
Institutional Review Boards (IRB), 8.4
Insurer, 5.17, 6.8
Interpretive Guidelines, 1.5

L
Lab test results, 3.13 — See also Human Immunodeficiency Virus (HIV), Tuberculosis screening
Lanterman-Petris-Short Act, 1.1, 6.1 to 6.28, 13.13
Law enforcement, 5.2, 5.43 to 5.44, 6.11, 6.13
Delay, 12.3, 12.8, 12.14
Legislative committee, 6.15
Liability insurer, 5.14, 5.19
Licensed health care professional
Definition of, 4.13
Licensing, 5.20
Boards, 6.15
Limited data set, 1.17, 8.1, 8.8

M
Managed Risk Medical Insurance Board, 5.4
Marketing, 4.9, 5.12
Media, 5.26 to 5.30, 12.4, 12.16
Medi-Cal, 5.3
Medical Board of California, 5.46
Medical emergencies, 7.8
Medical information
Definition of, 4.15, 5.2
Medical record
Deceased patient, 5.1, 5.7, 6.3, 7.4, 7.7
Medical record, release of information from
Ambulance companies, 5.22, 6.16
Emergency Medical Services Authority/Agency, 5.22, 6.16
Medical staff, 2.6
Mental health advocates, 6.21 to 6.27
Mental health patient
Minors, 5.9
Records, 3.12, 4.5, 4.15, 5.2, 5.24, 6.1 to 6.28
Military, 5.23
Minimum necessary, 4.11 to 4.12, 7.4, 8.3
Minor, 3.10, 5.7 to 5.8, 6.9, 7.6
Mitigate, 12.2
Multidisciplinary personnel teams, 5.11, 6.17

N
National security, 5.23
Noncustodial parent, 5.10
Notice of Privacy Practices, 2.4, 3.1 to 3.3, 3.16

O
Observer of childbirth/medical procedure, 4.25 to 4.26
Occupational exposures, 9.14
OCR
Audit program, 13.3
Office for Civil Rights (OCR) — See DHHS
Office of Health Information Integrity (OHII), 13.12
Organized health care arrangement, 2.3, 3.4, 11.3
Organ procurement organization, 1.2, 5.21 — See also Tissue bank

P
Parent — See also Personal representative
Foster, 5.10
Noncustodial, 5.11
Patient Access to Health Records Act, 1.1, 3.5
Patient access to PHI, 3.4 to 3.14
Patient-authorized disclosures, 6.7 — See also Authorization
Patient records
Definition of, 4.15
Patients’ rights advocates, 6.24 to 6.27 — See also Mental health advocate
Payment, 5.18, 6.8 — See also Insurer
Definition of, 5.17
Peer review, 5.19, 5.31
Penalties, 13.1 to 13.14
Personal representative, 3.5, 3.9, 3.13, 4.2, 6.5 — See also Authorization
Photocopying services, 5.15
Physical safeguards, 10.4
Policies and procedures, 2.4 to 2.7
Preemption, 4.1
Analysis, 1.4, 4.12 to 4.18
Prisoners — See Inmate
Privacy
Boards, 8.4
Officer, 2.1
Rights, 3.1
Privacy Act of 1974, 1.12
Privileged information, 5.30 to 5.32, 6.18
Probate court investigation — See Conservatorship proceeding
Probation officer, 5.10, 6.7, 6.9
Protected health information (PHI)
Amendment of, 3.14 to 3.16
Definition of, 4.1
Patient access to, 3.4 to 3.14
Sale of, 4.10
Unsecured, 12.13
Protection and advocacy, 6.21 to 6.27
Protective order, 5.33
Provider of health care
Definition of, 4.13
Psychiatric records, 6.1 to 6.28 — See also Psychotherapy notes
Psychotherapy notes, 3.11 to 3.20, 4.5 to 4.35, 5.12, 6.23
Definition of, 4.6
Public health, 5.20
Public health nurse, 5.10, 5.25, 6.9
Public Records Act, 1.12

Q
Quality assurance committee, 6.15

R
Ransomware, 10.2, 12.12
“Red Flags” rules, 10.8 to 10.9
Redisclosure, 3.6, 5.4, 6.24, 7.5, 8.6, 9.3
Re-identification, 1.17, 8.7
Remote access, 8.5, 10.1
Request for observer at childbirth/medical procedure, 4.25 to 4.26
Research, 5.21, 6.9, 7.8, 8.1 to 8.10
Compliance checklist, 8.10
Residential shelter services, 5.9
Retaliation, 2.5, 2.6, 13.2
Anti-retaliation policy, 2.6
Risk assessment, 10.3
Ryan White CARE Act, 4.8, 6.18

S
Safe surrender of newborn, 5.12
Sanctions, employees, 2.4, 2.6, 12.2
SB 541, 12.5
School, 5.46
Security, health information, 10.1 to 10.10
Security incident, 10.4, 11.4
Security officer, 2.2
Self-sufficient minor, 5.9
Sexual assault, 5.9
Social Security numbers, 1.1
Social worker, 5.10, 6.9
Special restriction, 3.18 to 3.20
Method of communication, 3.20
Subpoena, 4.9, 5.5, 5.30 to 5.43, 6.19, 7.10 to 7.12
Administrative agency, 5.41
Criminal, 5.42
Fees, 5.39
Investigative, 5.5
Substance abuse records, 5.2, 7.1 to 7.14

T
Tarasoff warnings, 5.20, 6.16
TCPA — See Telephone Consumer Protection Act (TCPA)
Technical safeguards, 10.4
Telephone Consumer Protection Act (TCPA), 1.6
Third party payer — See Insurer
Tissue bank, 5.21 — See also Organ procurement organization
TPO (treatment, payment, health care operations), 5.16
Trading partner agreement
Definition of, 11.8
Trainees, 2.4
Training, 2.4 to 2.5
Transfer, notifying relatives of, 6.19 to 6.21
Treatment, 5.17, 6.8
Definition of, 5.17
Treatment, payment, health care operations (TPO), 5.16
Tuberculosis screening
Release of screening results to public health officer, 5.44

U
Unencrypted computerized data, 1.12, 12.3
Use
Authorization for — See Authorization
Definition of, 4.2

V
Verification procedures, 3.10, 4.10 to 4.11, 7.4
Video monitoring, 1.5
Visitors, 4.25
Volunteers, 2.4, 2.6

W
Warrant, 5.5, 5.43, 6.13
Wellness program, 9.8
Whistleblowers, 2.6
Workers’ compensation, 5.3, 5.4, 5.22, 6.18
Appeals board, 6.18
Workforce
Definition of, 2.4
Workplace exposures — See Occupational exposures