

CONFIDENTIALITY & SECURITY

Protecting and Releasing Health Information in California

November 2016
15th Edition

Allan D. Jergesen



CHIA
— AHIMA Affiliate
California Health
Information Association

SAMPLE

PREFACE

This publication is designed to produce accurate and authoritative information on the subject matter covered. It is sold with the understanding that CHIA is not engaged in rendering legal service. This publication should not be viewed as legal advice or take the place of advice provided by a health care provider's legal counsel. If legal or other expert assistance is required, if there are differences of opinion or where the law is unclear, the advice of legal counsel should be sought.

This publication is designed to inform health information management and other health care professionals about the new HIPAA privacy and security rules and includes the California Preemption rules.

This publication reviews situations in which providers are called upon to disclose information – including releases pursuant to court orders, subpoenas, reporting requirements, patient treatment regimens, and billing and payment activities.

This publication will go a long way towards familiarizing the reader with health information confidentiality, as governed by HIPAA, as amended by the HITECH Act and the HIPAA Omnibus Rule, and by California state law.

Copyright ©2016 by the California Health Information Association

All rights reserved.

First edition April 2003.

15th edition November 2016.

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 the exception of the forms, tables and appendices), without the prior written approval of the publisher. It is the intent of CHIA to strictly enforce this copyright.

Published by the California Health Information Association.
Printed in the United States of America.

For book ordering information visit the CHIA website: CaliforniaHIA.org/publications

Published by:

California Health Information Association
1915 North Fine Avenue, Suite 104
Fresno, California 93727-1565
(559) 251-5038
Info@CaliforniaHIA.org
CaliforniaHIA.org

ACKNOWLEDGMENTS

The California Health Information Association (CHIA) Board of Directors gives special thanks to Allan D. Jergesen, J.D., of the law firm of Hanson Bridgett LLP, for his valuable and capable legal assistance and for his significant contributions to this book. Mr. Jergesen is well known to California's health information management professionals, many of whom rely on articles authored by Mr. Jergesen, and published in each issue of the *CHIA Journal*, for advice on legal issues and interpretation and application of state and federal laws and regulations that relate to privacy and confidentiality of health information and the appropriate use and disclosure of that information. Mr. Jergesen has been a speaker at the CHIA annual Confidentiality and Release of Health Information seminars for over thirty years, and the legal and technical expertise he has brought is invaluable to health information management professionals.

Allan D. Jergesen
Hanson Bridgett LLP
425 Market Street, Suite 2600
San Francisco, CA 94105-5401
Tel: (415) 995-5023
Fax: (415) 995-3433
Email: ajergesen@hansonbridgett.com

Thanks also go to the many CHIA Members who have kindly taken their time to submit questions and make comments on the HIPAA regulations.

SAMPLE

TABLE OF CONTENTS

	<u>Page</u>
PART ONE PRIVACY: HIPAA IN CALIFORNIA	1
I. Background.....	1
A. Health Insurance Portability and Accountability Act of 1996 ("HIPAA").....	1
B. Congressional Direction to DHHS	1
C. DHHS Response	1
D. Subsequent Revisions.....	2
II. The State Law Preemption Issue	2
A. Preemption Rule.....	2
B. Exceptions.....	3
C. "More Stringent" Standard	3
III. California – Applicable Confidentiality Rules	4
A. HIPAA Privacy Rules.....	4
B. California Confidentiality Laws.....	5
C. Federal Alcohol and Drug Abuse Confidentiality Regulations	6
IV. Enforcement and Penalties	6
A. HIPAA	6
B. California Law [Cal. Civil Code §56.36]	7
PART TWO PRIVACY: GENERAL HEALTH INFORMATION	9
I. HIPAA and CMIA	9
A. Areas of Application	9
B. General Privacy Rule.....	9
C. Approach to Exceptions to Authorization Requirement	9
II. General Health Information – Exceptions to Written Authorization Requirement	10

A.	Disclosures under Legal Process	10
B.	Disclosures to Law Enforcement Agencies.....	13
C.	Disclosures to Patient or Patient’s Personal Representative.....	14
D.	Disclosures Otherwise Specifically Required by Law.....	14
E.	Disclosures to County Coroner.....	14
F.	Disclosures under Reporting Laws	14
G.	Disclosures for Public Health Activities.....	15
H.	Disclosures for Health Oversight Activities	16
I.	Disclosures for Workers’ Compensation.....	16
J.	Disclosures for Treatment Activities.....	16
K.	Disclosures for Payment Purposes.....	16
L.	Disclosures for Health Care Operations.....	17
M.	Disclosures to Business Associates	17
N.	Disclosures for Research	18
O.	Disclosures to Prevent Danger to Identified Person.....	19
P.	Disclosures for Organ Procurement.....	19
Q.	Disclosures Permitted by HIPAA and Not Recognized by CMIA.....	19
III.	Written Authorization.....	20
A.	Form.....	20
B.	SNFs and ICFs.....	20
C.	Contents.....	20
D.	Invalidity	21
E.	Signature.....	22
F.	Special Situations Requiring Authorizations	22
G.	Situation Where Authorization Is Insufficient.....	23

IV.	Release of Basic Patient Information	23
A.	General Rule	23
B.	Disclosures to Outside Inquirers.....	23
C.	Disclosures of Limited Information to Defined Recipients for Specific Purposes.....	24
PART THREE PRIVACY: PATIENT RIGHTS.....		27
I.	Notice of Privacy Practices	27
A.	Requirement of Notice.....	27
B.	Request for Acknowledgment.....	27
C.	Contents of Notice.....	27
D.	Model NPP (see Appendix U).....	28
II.	Patient Requests for Special Privacy Protection	28
A.	Request for Restrictions on Uses or Disclosures.....	28
B.	Request for Communications to Patient by Alternative Means or Locations.....	29
III.	Patient Access to Health Records.....	29
A.	Relevant Laws.....	29
B.	Person Granted Access.....	29
C.	Records Covered	30
D.	Right of Access	30
E.	Exceptions.....	33
F.	Summary of Patient Records.....	34
G.	Denial of Access.....	34
IV.	Patient Amendment of Health Records	34
A.	Applicable Laws	34
B.	Request for Amendment.....	35
C.	Decision Regarding Amendment	35

D.	Acceptance of Amendment.....	35
E.	Denial of Amendment.....	35
F.	Future Disclosures	36
V.	Accounting for Disclosures.....	36
A.	Patient Right to Receive Accounting.....	36
B.	Exceptions to Accounting Right	36
C.	Content of Accounting	37
D.	Time for Accounting	38
E.	Charges for Accounting	38
F.	Documentation	38
	PART FOUR PRIVACY: SPECIAL HEALTH INFORMATION.....	39
I.	Psychiatric/Mental Health Information.....	39
A.	Citation – Lanterman-Petris-Short Act	39
B.	Applicability	39
C.	General Rule of Confidentiality	39
D.	Exceptions – Written Authorization Needed.....	39
E.	Exceptions – No Written Authorization Needed	41
II.	Substance Abuse Information	45
A.	Citation.....	45
B.	Applicability	45
C.	Disclosures with Written Authorization.....	47
D.	Disclosures without Written Authorization.....	48
E.	Notice to Patient of Confidentiality Requirements	49
F.	Court Orders	50
III.	HIV Test Results.....	50

A.	General Rule	50
B.	Exceptions.....	50
PART FIVE SECURITY: HIPAA SECURITY RULES		53
I.	Background.....	53
A.	History	53
B.	Purpose.....	53
C.	California Security Requirements	53
D.	Application of HIPAA Security Rules	55
II.	General Methodology.....	56
A.	Safeguards.....	56
B.	Standards.....	56
C.	Implementation Specifications.....	56
III.	Safeguards, Standards, and Implementation Specifications.....	57
A.	Administrative Safeguards.....	57
B.	Physical Safeguards.....	58
C.	Technical Safeguards.....	59
IV.	Other Requirements.....	59
A.	Business Associate Agreements	59
B.	Policies and Procedures.....	60
C.	Documentation Requirements	60
PART SIX SECURITY: SPECIAL PATIENT PROTECTIONS		61
I.	Disclosure of Security Breaches	61
A.	New Focus on Protecting Patients from Security Breaches	61
B.	Laws Requiring Disclosure of Security Breaches.....	61
C.	Reporting and Disclosure Requirements	62
II.	Detection of Identity Theft	67

A.	Background.....	67
B.	Federal Red Flags Rule.....	67
C.	Requirements of Red Flags Rule.....	67
PART SEVEN	CURRENT TRENDS	69
I.	Changing Enforcement Focus.....	69
A.	Early Emphasis on Education.....	69
B.	Current Focus on Implementation	69
II.	OCR Audits.....	69
A.	Prescribed in HITECH Act [42 U.S.C. §17940]	69
B.	Phase 1 Pilot Audit Program (2012)	69
C.	Phase 2 Permanent Audit Program (2016)	69
III.	OCR Enforcement.....	70
A.	OCR Reports.....	70
B.	Sources of OCR Investigations.....	70
C.	Focus on Security Breaches of ePHI	70
D.	Examples	71
IV.	DPH Enforcement.....	71
A.	DPH as Enforcement Agency	71
B.	Use of Existing Citation System.....	71
V.	Private Enforcement	72
A.	Availability	72
B.	Liability for CMIA Violations	72
C.	Class Actions for Security Breaches.....	72
APPENDIX A.....	73
	AUTHORIZATION FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION.....	73

APPENDIX B	77
WRITTEN NOTICE ACCOMPANYING DISCLOSURE OF ALCOHOL OR DRUG ABUSE INFORMATION.....	77
APPENDIX C	79
FEDERAL ALCOHOL AND DRUG ABUSE CONFIDENTIALITY RULES – 42 C.F.R. §2.1 ET SEQ.	79
OBRA SNF RESIDENT ACCESS RULES – 42 C.F.R §483.10(b)(2)	93
APPENDIX D	95
HIPAA SECURITY AND PRIVACY RULES – 45 C.F.R. §160.102 <i>ET SEQ.</i>	95
APPENDIX E	167
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT: CALIFORNIA CIVIL CODE SECTION 56 <i>ET SEQ.</i>	167
CALIFORNIA MEDICAL IDENTITY THEFT LAW: CALIFORNIA CIVIL CODE SECTION 1798.82.....	183
APPENDIX F	187
CALIFORNIA IMPROPER ACCESS NOTIFICATION LAW – CALIFORNIA HEALTH & SAFETY CODE SECTION 1280.15.....	187
CALIFORNIA BLOOD DONOR LAW: CALIFORNIA HEALTH & SAFETY CODE SECTION 1603.3.....	188
CALIFORNIA BIRTH CERTIFICATE LAW: CALIFORNIA HEALTH & SAFETY CODE SECTION 102425 <i>ET SEQ.</i>	189
CALIFORNIA HIV CONFIDENTIALITY LAW: CALIFORNIA HEALTH & SAFETY CODE SECTION 120975 <i>ET SEQ.</i>	193
CALIFORNIA PATIENT ACCESS LAW: CALIFORNIA HEALTH & SAFETY CODE SECTION 123100 <i>ET SEQ.</i>	196
CALIFORNIA OFFICE OF INFORMATION INTEGRITY LAW: CALIFORNIA HEALTH & SAFETY CODE SECTION 130200 <i>ET SEQ.</i>	203
APPENDIX G	205
CALIFORNIA LANTERMAN-PETRIS-SHORT ACT, CALIFORNIA WELFARE & INSTITUTIONS CODE SECTION 5326 <i>ET SEQ.</i>	205
CALIFORNIA MEDI-CAL TELEMEDICINE LAW: CALIFORNIA WELFARE & INSTITUTIONS CODE SECTION 14132.725	211

APPENDIX H	213
CALIFORNIA PATIENT SUBPOENA NOTIFICATION LAW: CALIFORNIA CODE OF CIVIL PROCEDURE SECTION 1985.3.....	213
APPENDIX I	215
CALIFORNIA EVIDENCE CODE.....	215
APPENDIX J	221
CALIFORNIA TELEMEDICINE LAW: CALIFORNIA BUSINESS & PROFESSIONS CODE SECTION 2290.5	221
APPENDIX K	223
CALIFORNIA ADVANCE HEALTH CARE DIRECTIVE REGISTRY LAW: CALIFORNIA PROBATE CODE SECTION 4800 <i>ET SEQ.</i>	223
APPENDIX L	225
CALIFORNIA HOSPITAL LICENSING LAWS – 22 C.C.R.	225
APPENDIX M	227
HITECH ACT: 42 U.S.C. SECTION 17921 <i>ET SEQ.</i>	227
SECURITY BREACH NOTIFICATION REGULATIONS: 45 C.F.R. SECTIONS 164.400 - 164.414.....	237
APPENDIX N	241
FEDERAL RED FLAGS RULE: 16 C.F.R. SECTION 681.2.....	241
APPENDIX O	243
MODIFICATIONS TO THE STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION -- FINAL RULE	243
APPENDIX P	247
HHS ADOPTS FINAL SECURITY STANDARDS, TRANSACTION MODIFICATIONS FOR ELECTRONIC HEALTH INFORMATION UNDER HIPAA.....	247
APPENDIX Q	249
ADMINISTRATIVE SIMPLIFICATION UNDER HIPAA: NATIONAL STANDARDS FOR TRANSACTIONS, SECURITY AND PRIVACY.....	249

APPENDIX R253
 PROTECTING THE PRIVACY OF PATIENTS’ HEALTH INFORMATION253

APPENDIX S257
 Office of the Civil Rights – Frequently Asked Questions on HIPAA.....257

APPENDIX T259
 Legal References on the Internet.....259

APPENDIX U261
 Office of the Civil Rights – Notice of Privacy Practices261

SAMPLE

SAMPLE

PART ONE

PRIVACY: HIPAA IN CALIFORNIA

I. Background

- A. Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
 - 1. Enacted by Congress in 1996
 - 2. Divisions
 - a. “Portability” provisions – focus on ability of employees to maintain health coverage when moving between jobs (ERISA rules)
 - b. “Accountability” provisions – impose harsher penalties for Medicare/Medicaid fraud or abuse
 - c. “Administrative simplification” provisions – create national standards to facilitate transmission and use of electronic health information; includes national security and privacy standards
- B. Congressional Direction to DHHS – Congress directs federal Department of Health and Human Services (“DHHS”) to create rules governing electronic health care information in absence of congressional action
- C. DHHS Response – DHHS creates rules governing electronic health information
 - 1. Final e-healthcare transactions and code sets rules [65 Federal Register 50311 (August 17, 2000)] – prescribe standardized formats for electronic data interchange (“EDI”), effective for all covered entities on October 16, 2003
 - 2. Final national identifier rules [67 Federal Register 38009 (May 31, 2002) (employers), 69 Federal Register 3434 (January 23, 2004) (health care providers)] – create single employer and provider identifiers for electronic transmissions; no national patient identifier rules yet
 - 3. Final security rules [68 Federal Register 4334 (February 20, 2003)] – create national standards to protect electronic health information from loss or theft, effective on April 21, 2005.
 - 4. Final privacy rules [65 Federal Register 82461 (December 28, 2000); 67 Federal Register 53182 (August 14, 2002)] – create national confidentiality standards for all health information (both electronic and non-electronic), effective on April 14, 2003.

D. Subsequent Revisions

1. HITECH Act [42 U.S.C. §17921 *et seq.*] – generally effective on February 18, 2010
 - a. Enacted as part of American Recovery and Reinvestment Act of 2009 (“stimulus” bill)
 - b. Provides \$19 billion in federal assistance to hospitals and physicians to implement electronic medical record systems
 - c. Brings genetic information under within definition of “protected health information” – follows on protections provided by Genetic Information Nondiscrimination Act (“GINA”)
 - d. Imposes additional privacy and security requirements in limited areas – *e.g.*, for business associates
 - e. Creates obligation to report breaches in security of protected health information
 - f. Directs DHHS Office for Civil Rights to establish program for auditing compliance with HIPAA privacy and security rules
 - g. Emphasizes enforcement – increased penalties; potential enforcement by state attorney general; expanded focus on smaller organizations
2. Security breach notification rules [74 Federal Register 42740 (August 24, 2009)] – effective on September 23, 2009
3. HIPAA Omnibus Rule [78 Federal Register 5566 (January 25, 2013)] – compliance date of September 23, 2013
 - a. Implements HITECH Act
 - b. Makes further changes in specific portions of privacy and security rules, including security breach notification rules

II. The State Law Preemption Issue

A. Preemption Rule

A HIPAA “standard, requirement, or implementation specification” dealing with privacy “preempts” (i.e., supersedes) any provision of state law that is contrary to it [45 C.F.R. §160.203]

B. Exceptions

1. Provision of state law relates to the confidentiality of health information and is “more stringent” than the comparable HIPAA privacy rule [45 C.F.R. §160.203(b)]
2. Provision of state law provides for the (1) reporting of disease or injury, child abuse, birth, or death, or (2) conduct of public health surveillance, investigation, or intervention [45 C.F.R. §160.203(c)]
3. Provision of state law requires health plan to report, or to provide access to, information for purpose of management audits, financial audits, program monitoring and evaluation, or licensure or certification of facility or individual [45 C.F.R. §160.203(d)]
4. DHHS determines that provision of state law [45 C.F.R. §160.203(a)]:
 - a. Is necessary:
 - (1) To prevent fraud and abuse;
 - (2) To ensure appropriate state regulation of insurance and health plans;
 - (3) To report health care delivery or costs for state purposes; or
 - (4) To serve a compelling need related to public health, safety, or welfare, and DHHS determines that intrusion into privacy is warranted when balanced against need to be served,
 - b. Has as its principal purpose the regulation of controlled substances

C. “More Stringent” Standard – Provision of state law is deemed to be “more stringent” if [45 C.F.R. §160.202]:

1. With respect to a use or disclosure – state law provision prohibits or restricts use or disclosure where HIPAA privacy rules would permit it, unless disclosure is to (1) federal Department of Health and Human Services to determine if provider is complying with HIPAA rules, or (2) patient
2. With respect to patient’s access to or amendment of protected health information – state law provision permits greater rights of access or amendment (except that state law always prevails with respect to access to minor’s protected health information by parent, guardian, or other person *in loco parentis*)

3. With respect to authorization or any other permission from patient for release of protected health information – state law provision narrows scope or duration of authorization or permission, increases privacy protections, or reduces coercive effect
4. With respect to information provided to patient about use, disclosure, rights, or remedies – state law provision requires provider to give more information
5. With respect to recordkeeping or accounting requirements – state law provision provides for retention or reporting of more detailed information or for retention over a longer period
6. With respect to any other matter – state law provision provides greater privacy protections

III. California – Applicable Confidentiality Rules

A. HIPAA Privacy Rules

1. Apply to “use or disclosure” of “protected health information” by “covered entities” [45 C.F.R. §§160.102 & 164.502(a)]
 - a. Use or disclosure [45 C.F.R. §164.501]
 - (1) Use – sharing, employment, application, utilization, examination, or analysis of protected health information within a covered entity
 - (2) Disclosure – release, transfer, provision of access to, or any other divulging protected health information outside a covered entity
 - b. Protected health information (“PHI”)
 - (1) Individually identifiable health information – does not include health information with all identifiers redacted
 - (2) HIPAA definition now excludes information regarding persons who have been deceased for more than 50 years [45 C.F.R. §160.103] – but not applicable in California, which does not limit definition of “medical information” [Cal. Civil Code §56.05(g)]
 - c. Covered entities
 - (1) Health plans
 - (2) Health care clearinghouses
 - (3) Covered health care providers

2. Covered health care providers
 - a. Health care providers – providers as recognized by Medicare, or any other person or entity that furnishes, bills, or is paid for health care
 - b. Engaging in transmittal of health information in electronic form in course of standard HIPAA-covered transactions
 - (1) Electronic transmittal – excludes transmittal by telephone, voicemail, or fax
 - (2) Standard transactions – transactions between providers and payors using HIPAA-prescribed uniform data sets relating to such matters as eligibility for coverage, claims, payment, and coordination of benefits
- B. California Confidentiality Laws
 1. California Confidentiality of Medical Information Act (“CMIA”) [Cal. Civil Code §56 *et seq.*] – applies:
 - a. To all licensed health care professionals and facilities (as well as to contractors (e.g., IPAs and MSOs), and health care plans) [Cal. Civil Code §56.05(c),(d),(h)]
 - b. To all patients (living and deceased) [Cal. Civil Code §56.05(g)]
 - c. To all medical information – individually identifiable information, in electronic or physical form, regarding patient’s medical history, mental or physical condition, or treatment [Cal. Civil Code §56.05(f)]
 - d. To disclosure to outside parties – assumed that disclosure can be made within a provider to those persons who have a need for this information
 2. Patient access statute [Cal. Health & Safety Code §123100 *et seq.*] – gives patients the right to have access and to submit amendments to “patient records” held by “health care providers”
 3. Lanterman-Petris-Short Act (“LPS Act”) [Cal. Wel. & Inst. Code §5328 *et seq.*] – applies to mental health information held by inpatient psychiatric facilities (including psychiatric departments of general acute care hospitals), persons on psychiatric hold, patients of mental health clinics, and patients funded through local community mental health programs
 4. Statute protecting HIV test results [Cal. Health & Safety Code §120980 *et seq.*] – provides rules for disclosure of HIV test results

- C. Federal Alcohol and Drug Abuse Confidentiality Regulations [42 C.F.R. §2.1 *et seq.*] – apply to patient records of alcohol or drug abuse programs that receive federal assistance

IV. Enforcement and Penalties

A. HIPAA

1. Complaints and investigations [45 C.F.R. §160.300 *et seq.*]
 - a. Any person may file a written complaint either on paper or electronically with DHHS within 180 calendar days of when complainant knew or should have known of HIPAA violation
 - b. DHHS must investigate where violation appears to have been due to willful neglect; DHHS may investigate in all other cases – investigation is by means of a “compliance review”
 - c. DHHS will attempt to resolve issues of non-compliance by informal means – otherwise, DHHS may initiate formal proceedings
2. Penalties for non-compliance
 - a. Provider
 - (1) No automatic civil cause of action by injured patient – although possibility of patient lawsuit for personal injury with HIPAA privacy rules (like state confidentiality rules) being used as evidence of community standards [see, e.g., *Acosta v. Bynum*, 638 S.E.2d 246 (N.C. App. 2006) (HIPAA privacy rules used as evidence of community standard of care in lawsuit alleging invasion of privacy and negligent infliction of emotional distress under state law)]
 - (2) Civil and criminal penalties for negligent and willful failures to comply – enforced by DHHS Office for Civil Rights (“OCR”)
 - b. Workforce members – sanctions required
3. OCR as enforcement agency
 - a. Limited staff
 - b. Immediate focus on education and assistance with compliance
4. California Attorney General as enforcement agency – may bring HIPAA enforcement actions, including obtaining damages on behalf of injured patients [HITECH Act §13410(e); 42 U.S.C. §1320d-5(d)]

- B. California Law [Cal. Civil Code §56.36]
1. Violation of CMIA involving economic loss or personal injury to patient – misdemeanor
 2. Negligent release of health information in violation of CMIA
 - a. Civil action for:
 - (1) Nominal damages of \$1,000 – no need to show actual damages; but possibility of class action
 - (2) Actual damages
 - b. Administrative fine or civil penalty up to \$2,500 per violation.
 3. Knowing or willful obtaining, use, or disclosure of health information in violation of CMIA
 - a. Person or entity other than licensed health care professional – administrative fine or civil penalty up to \$25,000 per violation
 - b. Licensed health care professional – administrative fine or civil penalty up to \$2,500 per violation for first violation; \$10,000 per violation for second violation; \$25,000 per violation for subsequent violations
 4. Knowing or willful obtaining, use, or disclosure of health information in violation of CMIA for purpose of financial gain
 - a. Person or entity other than licensed health care professional – administrative fine or civil penalty up to \$250,000 per violation and disgorgement of any proceeds obtained
 - b. Licensed health care professional – administrative fine or civil penalty up to \$5,000 per violation for first violation; \$25,000 for violation for second violation; \$250,000 per violation for subsequent violations – and disgorgement of any proceeds obtained
 5. Knowing or willful obtaining, use, or disclosure of health information by person not authorized to receive it under CMIA without written authorization from patient or patient's representative

Civil penalty not to exceed \$250,000 per violation
 6. Relevant considerations in assessing administrative fine or civil penalty
 - a. Existence of reasonable, good faith attempts to comply with CMIA
 - b. Nature and seriousness of conduct

- c. Harm to patient
 - d. Number of violations
 - e. Persistence of misconduct
 - f. Length of time over which misconduct occurred
 - g. Willfulness of misconduct
 - h. Violator's assets, liabilities, and net worth
7. Enforcers
- a. Civil penalties – government attorneys in court
 - b. Administrative fines – DPH (for health facilities, clinics, home health agencies, and hospices); Cal OHI (for all others)

SAMPLE