

HIPAA:

“may not use or disclose protected health information” without a *patient Authorization* except for:

Treatment	Includes case management, continuation of care, placement activities.
Payment	Any use or disclosure necessary for payment of care actually rendered by the using / disclosing provider
Health Care Operations (minimum necessary standard)	<i>E.g.:</i> quality assessment and improvement peer review training programs business planning customer satisfaction / grievances reports required by law

Cal. CMIA:

Unless “expressly authorized” by the patient, “shall not intentionally share, sell, use for marketing, or otherwise use” medical information except for:

Medical diagnosis or treatment of the patient	Includes EMS transmissions, disclosure to those involved in caring for the patient and finding patient reps.
“Other lawful purpose”	As defined under the statute – payment, QA, underwriting, claims, accreditation, coroner, accreditation, public health reporting / research, worker’s comp, health plan operations, conservatorships, organ / tissue donation, otherwise required by law, disasters, encryption, disease management, warning third parties.

Notification Obligations for Medical Record Privacy “Breaches”

As of September 24, 2009

Authority	Who is Covered	What Must Be Disclosed	To	How Quickly	Possible Consequences
CMIA	Licensed Health Facilities, Clinics, Home Cares and Hospices in California	“unlawful” or “unauthorized” access to, use or disclosure of patient medical information	CDPH and Patient	5 days from “detection” (unless law enforcement requests a delay)	<ul style="list-style-type: none"> • Fines for underlying act (access, use, disclosure) • Fines for delays in disclosing • Referral of licensed individuals to OHII and licensing boards • Reputational harm • Civil suits • Enforcement action by state AG
HITECH	HIPAA “covered entities”	<p>“Breaches” – violations of the HIPAA privacy rule that involve “unsecured”** information and carry a significant risk of financial, reputational or other harm to the individual (based on a documented risk assessment)</p> <p>** “unsecured” = not encrypted or destroyed</p>	Patient DHHS Media	<p>To patient - “without unreasonable delay”, but no later than 60 days from time the CE knew or should have known of the breach (unless law enforcement requests a delay)</p> <p>To DHHS Secretary (> 500 individuals) – same time frame; (<500 individuals) – annual report</p> <p>To Media (> 500 in single state)</p>	

CMIA = Confidentiality of Medical Information Act

CDPH = California Department of Public Health
OHII = Office of Health Information Integrity,
California Health and Human Services Agency

DHHS = U.S. Department of Health and
Human Services

HITECH = Health Information Technology
for Economic and Clinical Health Act
(stimulus bill)