CHA Labor and Employment Law Seminar

New Privacy Laws Impacting the Health Care Work Place

Presented by

Thomas E. Jeffry, Jr., Esq.

Arent Fox LLP

Washington, DC | New York, NY | Los Angeles, CA

November 12 & 19, 2009
Overview

1. Overview of California Privacy Laws & HIPAA

2. Breach Notifications Requirements

3. Liability for Breaches: Employer and Employee

4. Coordination and preparation to mitigate liability
Part I:
Overview of California Privacy Laws & HIPAA
California Law

• Confidentiality of Medical Information Act

  • Civil Code §§ 56 et seq.
  • “No provider of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization” except as otherwise allowed
  • Disclosure allowed to facilities and health care professionals for treatment and diagnosis
  • Disclosure allowed to any person who provides administrative services to a provider of health care so long as the recipient does not further disclose in any manner that violates CMIA
California Law – A.B. 211

- Adds Sections 130200-130205 to the Health and Safety Code

- Providers must implement safeguards to protect medical information and safeguard it from unauthorized or unlawful access, use, or disclosure

- Creates the California Office of Health Information Integrity (CalOHII) within the California Health & Human Services Agency to enforce these requirements and impose administrative fines
California Law – S.B. 541

- Amends Health & Safety Code Sections 1280.1 and 1280.3

- Adds Section 1280.15.

- Authorizes the Department of Public Health to impose administrative penalties for unauthorized access, use, or disclosure of patient information.

- Providers must report all incidents of unlawful or unauthorized access, use, or disclosure to the Department of Public Health and to the affected patient.
“Unauthorized Access” defined in §1280.15(i)(2):

“the inappropriate access, review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (CMIA)(Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or by any other statute or regulation governing the lawful access, use, or disclosure of medical information.”
A licensed clinic, health care facility, home health agency or hospice “shall prevent unlawful or unauthorized access to, and use or disclosure of patients’ medical information” as defined in the CMIA and consistent with H&S Code § 130203.
Use and disclosure of protected health permitted:

- To the individual
- For treatment, payment & health care operations
- Incidental to permitted uses & disclosure (subject to “minimum necessary”)
HIPAA Privacy Rule – Minimum Necessary

Standard difficult to understand and challenging to implement:

• Identify who in workforce needs access
• Create categories of PHI for which access is needed by identified workforce members
• Use reasonable efforts to limit access beyond information needed by such identified workforce members
• Develop criteria to limit PHI disclosure to information reasonably necessary to accomplish the lawful purpose
An individual has a right to receive an accounting of all unauthorized and some permitted disclosures of their PHI made by the covered entity for the past 6 years.
HIPAA Security Rule

• Applies to electronic PHI
• Requires implementation of safeguards (administrative, physical, technical) to:
  - Ensure confidentiality, integrity and availability
  - Protect against anticipated threats and hazards
  - Protect against anticipated uses and disclosures not permitted
  - Ensure compliance by its workforce
HIPAA Security Rule - Workforce

- Requires implementation for policies and procedures to give access to PHI to those workforce members who are permitted and prevent access to those who are not permitted
- Procedure for authorization/supervision of workforce
- Procedure to determine if access is appropriate
- Procedure for terminating access when employment ends or access criteria changes
- Security awareness and training
HITECH Changes to Privacy & Security

- Expands application of HIPAA to business associates and personal health record vendors
- New requirements for breach notification
- Changes provisions in the Privacy Rule related to:
  - Minimum Necessary standard
  - Accounting for disclosures
  - Disclosures by providers to health plans
- New privacy educational requirements
- New criminal and civil penalties; changes in enforcement responsibility
HITECH – Minimum Necessary

When using or disclosing PHI, or requesting PHI from another covered entity, must limit “to the extent practicable” disclosure of PHI to a limited data set. If more information is needed, only provide that information necessary “to accomplish the intended purpose of such use, disclosure, or request.

- Disclosing covered entity makes the determination
- Effective until the Secretary of HHS issues guidance on what is the ‘minimum necessary’
All disclosures made through an electronic health record must be accounted for and provided to the individual upon request for a period of 3 years.
Part 2:
Breach Notification Requirements
California v. Federal – Who must report

<table>
<thead>
<tr>
<th>Clinic</th>
<th>Covered Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Facility</td>
<td>Business Associate</td>
</tr>
<tr>
<td>Home Health Agency</td>
<td></td>
</tr>
<tr>
<td>Hospice</td>
<td></td>
</tr>
</tbody>
</table>
California v. Federal – What is reportable

Any unlawful or unauthorized access, use, or disclosure of a patient’s medical information.

A ‘breach’ which means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.

Guidance suggests misdirected communications within the facility or health care system do not need to be reported, but should be corrected.

Exceptions for unintentional or inadvertent access by employees as long as not used or disclosed in an unauthorized manner.
California v. Federal – When is it reportable

No later than 5 calendar days after the unlawful or unauthorized access, use, or disclosure has been detected by the health facility.

Guidance: “Facilities should not wait until they have conducted a preliminary review . . .”

(Note: S.B. 337 will change to 5 business days and provides for criminal investigation exception)

Without reasonable delay, but no later than 60 calendar days after the discovery of the breach (i.e. known by any employee, officer or other agent other than the person committing the breach).

Exception if will impede a criminal investigation or cause damage to national security.
California v. Federal – Who is it reported to

California Department of Public Health, Licensing and Certification District Office

Secretary of HHS

Affected patient or their patient representative

Affected patient or their patient representative

Substitute Notice on web site or major media

If >500, then to prominent media outlets
California v. Federal – Content of Notice

- Date & time of incident
- Facility name
- Facility location
- Contact person
- Name of patient
- Name of ‘alleged’ violators
- Description of circumstances of the breach
- Other information relevant to the department’s decision regarding on-site investigation
- Date of breach and date of discovery
- Identification of reporting entity
- Description of what happened
- Description of the types of PHI involved
- Steps individuals should take to protect from potential harm
- Description of investigation, corrective actions, and mitigation
- Contact procedures
Part 3: Liability for Breaches: Employer and Employee
California – Failure to Timely Report

Facilities subject to a fine of $100 per day per incident subject to cap of $250,000
California – Civil Penalties for Facilities

For failure to prevent unauthorized access, use, or disclosure, an administrative penalty of $25,000 per patient plus $17,500 for each subsequent unauthorized use subject to the $250,000 cap.

Penalties are discretionary and are based investigation and a number of factors:

- History of compliance
- Steps to detect and correct and prevent violations
- Outside the control of the facility
California – Civil Penalties for Individuals

- Negligent disclosure - $2,500 per violation
- Knowingly and willfully - $25,000 per violation
- Disclosure for financial gain - $250,000 per violation
- Sliding scale of penalties for licensed professions such as physicians and nurses
- Penalties discretionary based upon consideration of factors such as:
  - Nature and seriousness of the misconduct
  - Harm to the patient
  - Persistence and length of time misconduct occurred
  - Willfulness
  - Assets, liabilities and net worth
Violations of the CMIA that result in economic loss or personal injury to a patient is punishable as a misdemeanor.
Federal Civil Penalties – A tiered approach

Applies to covered entities, business associates and others.

- Did not know - $100-$50,000
- Reasonable cause - $1,000-$50,000
- Willful neglect/corrected - $10,000-$50,000
- Willful neglect/not-corrected - $50,000

Subject to annual cap of $1.5 Million for similar violations
HITECH clarifies that both individuals as well as the covered entities are subject to criminal prosecution (including felonies) under Section 1177 of the Social Security Act.
Part 4:
Coordination and Preparation to Mitigate Liability
Dealing with Breaches

• Identify individuals who make up the team to deal with reports of breaches
  ▪ IT
  ▪ HR
  ▪ Compliance
  ▪ Public Relations

• Develop policies and procedures so that staff knows who to report to and how that is transmitted for response
Dealing with Breaches

- Notes and documentation may be discoverable – keep track of times and dates
- Training – remind them about monitoring, penalties, etc.
- Technical safeguards – Break the Glass
Open issues and problems

- Business Associates and their employees
- Reporting before the investigation is complete
  - Government agency
  - Individual
- Coming to agreement as to whether a reportable breach occurred
- Consistency of employee discipline and discipline of medical staff members
- Government investigations and oversight
- Employees looking at their own records or the records of their family members
Questions and Discussion

Thomas E. Jeffry Jr.
Partner
Arent Fox LLP | Attorneys at Law
Gas Company Tower
555 West Fifth Street, 48th Floor
Los Angeles, CA 90013
213.443.7520 DIRECT | 213.629.7401 FAX
jeffry.thomas@arentfox.com