
State Law and Regulation Affecting Privacy and Security in California



HIPAA Summit West - Pre-Conference Symposia

Clark Stanton

Davis Wright Tremaine LLP

www.ehealthlaw.com

Revised: June 19, 2001



HIPAA Privacy — General Rules

- ◆ A “Covered Entity” may not use or disclose Protected Health Information (“PHI”) except:
 - ❖ as authorized by the individual, by -
 - verbal agreement - directories, release to family involved in treatment, etc.
 - consent - for treatment, payment, or healthcare operations (required for providers only)
 - authorization - for other purposes
 - ❖ for governmental or other specified purposes
 - ❖ as required by HIPAA



State Privacy Laws

- ◆ State laws on medical confidentiality:
 - ❖ California
 - Confidentiality of Medical Information Act - requires patient authorization for release of information unless release otherwise permitted or required by law
 - Lanterman-Petris-Short Act - protects mental health information
 - HIV test confidentiality law - strict protection for information concerning HIV tests, including identity of persons tested
 - Miscellaneous other provisions



HIPAA Meets State

- ◆ What happens when HIPAA meets California medical privacy law?
 - ❖ There are numerous differences between the protections to medical information provided under HIPAA and the protections provided under California law
- ◆ 50 states = 50 different combinations of HIPAA and State law



Preemption Primer /1

- ◆ Preemption is a product of our “federalist” system of government -
 - ❖ Single federal system with defined powers (e.g., coin money, declare war, regulate interstate commerce).
 - ❖ State governments have authority to govern and regulate in areas not reserved to the federal government (e.g., health and welfare of its citizens).



Preemption Primer /2

- ◆ Preemption predicate: “Supremacy Clause”
 - U.S. Constitution, Article VI, Clause 2:
 - ❖ The Constitution and laws of the United States are the “supreme law of the land.”
- ◆ Preemption question: When do laws passed by Congress override State laws?
 - ❖ Express, field & conflict preemption



Preemption Primer /3

- ◆ Total Preemption: Invalidates all State laws dealing with the regulated area regardless of whether they actually conflict with federal law.
- ◆ Partial Preemption: Allows States to legislate and regulate in an area covered by federal law, but only to the extent permitted by federal law or that it does not conflict with the federal law.



Preemption Analysis

- ◆ The preemption question: When and to what extent do laws passed by Congress override State laws dealing with the same subject.
 - ❖ Did Congress act within its scope of power?
 - Ex: Commerce clause versus health & welfare
 - ❖ If federal law is valid, did Congress expressly describe the intended scope of preemption?
 - ❖ If preemption is partial, to what extent does State law conflict with or present an obstacle to the federal law?



Preemption: Examples

- ◆ Transportation (interstate commerce)
 - ❖ Air travel; railways; interstate highways
- ◆ Immigration and naturalization
 - ❖ INS, border regulation
- ◆ Privacy initiatives pre-dating HIPAA
 - ❖ Fair Credit Reporting Act
 - ❖ Privacy Act of 1974
 - ❖ Alcohol & drug abuse information



Preemption Under HIPAA

- ◆ HIPAA:
 - Public Law 104-191; Section 1178:
HIPAA (any provision, requirement, standard or implementation specification of HIPAA) shall supersede any contrary provision of State law.
- ◆ Preemption applies to all of HIPAA, not just the privacy portion



Preemption Under HIPAA

- ◆ HIPAA gave Congress three years to pass *comprehensive* privacy legislation
 - ❖ Even now Congress could do so
- ◆ In such legislation, Congress would be free to decide whether HIPAA should provide for either total or partial preemption of State law
- ◆ Right now, privacy is controlled by the preemption scheme in HIPAA - ***partial*** preemption



Exceptions to Preemption

- ❖ State laws addressing controlled substances
- ❖ Where **DHHS** determines a State law is **necessary** --
 - to prevent fraud and abuse
 - to ensure appropriate regulation of health plans
 - for reporting on healthcare delivery or costs
 - to serve a ***compelling need*** related to public health, safety or welfare
 - DHHS must determine invasion of privacy is warranted when balanced against the need.



Exceptions to Preemption

- ❖ **Public health laws** for reporting disease, injury, child abuse, birth or death, or public health surveillance, investigation or intervention
- ❖ Laws requiring **health plans** to report or provide access to information for audits, program monitoring, or facility or individual licensure or certification.
- ❖ Laws relating to the privacy of health information that are ***contrary to*** and ***more stringent than*** the HIPAA requirements



Preemption: Contrary

◆ **Contrary** means -

❖ Covered entity could not comply with both State law and the HIPAA requirement

or

❖ State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA



Preemption: More Stringent

- ◆ **More stringent** means that State law -
 - ❖ Has stricter limits on use or disclosure of health information
 - Except for disclosures to DHHS or patient
 - ❖ Gives greater rights of access to or correction of health information by the patient
 - Does not affect State laws authorizing or prohibiting disclosure of information about a minor to parent or guardian
 - ❖ Has harsher penalties for unauthorized use or disclosure



Preemption: More Stringent

- ❖ Provides greater information to individuals regarding use, disclosure, rights or remedies
- ❖ Has stricter requirements for authorizing or consenting to the disclosure of information
- ❖ Has stricter standards for record-keeping or accounting for disclosures of information
- ❖ With respect to any other matter provides greater privacy protection to the patient



Requesting Exceptions

- ◆ Process for requesting exceptions from DHHS
 - ❖ Anyone may request an exception
 - Request by a state must be submitted through its chief elected official or designee
 - ❖ Must be in writing



Requesting Exceptions

- ◆ Request for exception must state:
 - ❖ State law for which exception requested
 - ❖ Portion of HIPAA for which the exception is requested
 - ❖ Portion of HIPAA that will not be implemented (or the additional data that will be collected) if the exception is granted
 - ❖ How CEs would be affected by the exception
 - ❖ Why State law should not be preempted.



Requesting Exceptions

- ◆ No time limit within which DHHS must make determination on exception request.
- ◆ HIPAA standard in question remains in effect until decision re exception is made.
- ◆ Exception determinations are to be made by DHHS Office for Civil Rights
- ◆ Advisory opinions dropped from final rule.



Duration of Exceptions

- ◆ If granted, exception remains in effect until -
 - ❖ The State law or the HIPAA provision that provided the basis for the exception is materially changed so that the basis for the exception no longer exists; or
 - ❖ DHHS revokes the exception based on a determination that the ground supporting the exception's need no longer exists.



How Preemption Will Work

- ◆ Preemption will focus on specific elements and aspects of State laws
 - ❖ HIPAA will be the baseline
 - ❖ State law will be given effect only to the extent that (a) there is no HIPAA law on the issue; (b) State law is more stringent; or (c) there is an exception
 - ❖ Exemptions will apply to specific State laws, not entire State schemes



How Preemption Will Work

- ◆ No California equivalents for --
 - ❖ Business associates
 - CEs must contract with entities that receive PHI in order to perform service for/on behalf of CE
 - ❖ Minimum necessary
 - CEs should not ask for or release more than the minimum necessary PHI required for the purposes for which release is sought



How Preemption Will Work

- ◆ No California equivalents (cont'd) --
 - ❖ Notice to patient of CE practices with respect to its handling of PHI
 - No notice requirement in CA law
 - ❖ Requirement of patient consent for use of PHI for treatment, payment and operations
 - California permits disclosure for such purposes without patient authorization or notice



Release/Use for Treatment

Release or use of information for treatment:

◆ HIPAA

- ❖ A provider must obtain patient's *consent* prior to use or disclosure of patient info for treatment of pt, *except* -
 - Provider has indirect treatment relationship with the patient (i.e., delivers care through another provider)

◆ California

- ❖ A provider may release patient info to other providers without authorization for purposes of diagnosis or treatment of patient



Release/Use for Treatment

Release of information for treatment of patient:

◆ HIPAA

- The patient is an inmate
- In emergencies (but must attempt to obtain consent thereafter)
- The provider is required by law to treat the patient and attempts but is unable to obtain consent

◆ California



Release/Use for Treatment

Release of information for treatment of patient:

◆ HIPAA

- The provider is unable to obtain consent due to communication barriers and determines that consent is “clearly inferred” from the circumstances

◆ California



Release/Use for Research

Release of information for research:

◆ HIPAA

- CE may use or disclose PHI for research, if:
 - An IRB or “privacy board” has approved an exception to the requirement for patient authorization
 - Additional req’ments for reviews prior to research or where patient is deceased

◆ California

- Provider may disclose patient information for “bona fide research purposes” to
 - public agencies
 - clinical investigators
 - health care research organizations
 - public or private nonprofit educational or health care entities



Release/Use for Research

Release of information for research:

◆ HIPAA

◆ California

- Documentation requirements, including
 - description of grounds used for waiver of patient's authorization
 - assurances against reuse or disclosure
 - description of the patient information needed for research



Penalties for Violation

Comparison of penalties for violation:

◆ HIPAA

- ❖ No private right of action under HIPAA
- ❖ Cal. B&P 17200?

◆ California

- ❖ CMIA: Patients may bring actions for violations of Cal. law -
 - compensatory damages
 - punitive damages \leq \$3,000
 - attorney's fees \leq \$1000



Penalties for Violation

Civil and criminal penalties:

◆ HIPAA

- ❖ Knowingly disclosing, obtaining or using is criminal offense

- ❖ Failure to comply:

- \$100/violation, not exceeding \$25,000/yr (civil fine)

◆ California

- ❖ Any violation is misdemeanor

- ❖ Negligent disclosure:

- Up to \$2,500/violation (civil fine)



Penalties for Violation

Civil and criminal penalties:

◆ HIPAA

❖ Knowingly disclosing, obtaining or using

- Up to \$50,000 and/or 1 year

❖ False pretenses

- Up to \$100,000 and/or 5 years

◆ California

❖ Knowingly & willfully obtaining, disclosing or using

- Up to \$25,000/violation



Penalties for Violation

Civil and criminal penalties:

◆ HIPAA

- ❖ For commercial or personal gain or malicious harm

- Up to \$250,000 and/or 10 years

◆ California

- ❖ For financial gain

- Up to \$250,000 per violation and disgorgement of proceeds received for information

State Law and Regulation Affecting Privacy and Security in California



HIPAA Summit West - Pre-Conference Symposia

Clark Stanton

Davis Wright Tremaine LLP

www.ehealthlaw.com

Revised: June 19, 2001