



OAKLAND LEGAL OFFICE
433 Hegenberger Rd. Suite 220 Oakland Ca. 94621-1448
Telephone: (510) 430-8033 Fax: (510) 430-8246
Toll Free/TTY/TDD: (800) 776-5746
www.pai-ca.org

MEMORANDUM

TO: County Patients' Rights Advocates

FROM: Daniel Brzovic
Associate Managing Attorney

RE: HIPAA privacy regulations do not preempt PRA access and
monitoring authority

DATE: August 25, 2003

PAI has been asked whether the new HIPAA privacy regulations, which took effect April 14, 2003, limit the access and monitoring authority of patients' rights advocates (PRA's) under the Welfare and Institutions Code. In our opinion, they do not. The only exception is that HIPAA allows disclosure of hospital patient directory information only if the patient is asked for by name. This preempts California law which previously provided that a patient's name could be released if there was an inquiry concerning a specific patient.

This is an update and revision of our previous memo on the subject.

What is HIPAA?

HIPAA stands for Health Insurance Portability and Accountability Act of 1996. This is a federal statute that is best known for placing restrictions on the ability of employer-provided health insurance plans to deny coverage for preexisting medical conditions. HIPAA also contains standards for electronic transmission of health information, and for protecting the privacy of health information.

Even though HIPAA has been around since 1996, the privacy provisions were not implemented until 2003 because the issues are so controversial and complex. For example, the Department of Health and Human Services received 52,000 comments to the initial proposed privacy regulations.

The privacy regulations do three things: They place restrictions on the disclosure and use of individual health information; they allow individuals access to their health information; and they allow individuals to ask for amendment of inaccurate or incomplete health information about them.

Who administers the HIPAA privacy provisions, and where can I find the law and regulations?

The federal Department of Health and Human Services administers the HIPAA privacy provisions, and insures compliance with the HIPAA privacy requirements. The HIPAA privacy statute was enacted as part of Part C of Subtitle F of Public Law 104-191, sections 261-264. Most of the privacy statute is codified as sections 1171-1179 of the Social Security Act, 42 U.S.C. § 1320d-1320d-8. The implementing regulations, effective April 14, 2003, are found at 45 C.F.R. § 160.101 *et seq.* The regulations have the force of law.

What is the purpose of the HIPAA privacy regulations?

The purpose of the HIPAA “administrative simplification” provisions (which include the privacy protection requirements) is to improve the “efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.” Section 261 of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191. (The “administrative simplification” provisions are designed to produce a single set of national billing codes.)

The purpose of the HIPAA privacy regulations is to protect individual health information from unauthorized disclosure, and to improve the accuracy of individual health information by allowing individuals to access their health information and to request amendment of that information if it is inaccurate or incomplete. Minimum national privacy standards are necessary as more

and more health information is transmitted electronically. That is the reason for the federal standards.

The HIPAA privacy regulations require individual written authorization for release of protected health information unless disclosure without authorization is allowed under the regulations. There are many instances when disclosure without individual written authorization is allowed under the regulations. This includes disclosure required by law, such as disclosure under the Welfare and Institutions Code to PRA's.

The point here is that the regulations are designed to prevent unauthorized disclosure of protected health information. Disclosure is authorized if an individual consents to disclosure in writing, or if disclosure is otherwise required by law. This is similar to the privacy system under California law. *Cf.* Welfare and Institutions Code § 5328. The only real difference between the HIPAA system and the California system is in some of the technical details.

Who do the HIPAA privacy regulations apply to?

The HIPAA privacy regulations apply to health care providers, health plans, and health care clearinghouses (e.g. an entity that translates provider billing codes into standard HIPAA billing codes, and vice versa). 45 C.F.R. §§ 160.102(a), 160.103 (definition of "Covered entity").

What types of information do the HIPAA privacy regulations apply to?

The HIPAA privacy regulations apply to "protected health information" which is defined to mean: "...individually identifiable health information [transmitted or maintained in any form or medium, electronic, or otherwise, except]:

... ..

- (2)(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g
- (ii) Records described in 20 U.S.C. 1232g(a)(4)(B)(iv) [certain postsecondary school student medical treatment records]; and

(iii) Employment records held by a covered entity in its role as employer”

45 C.F.R. § 164.501 (definition of “Protected health information”).

“Health information” is defined to mean: “...any information, whether oral or recorded in any form or medium that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

45 C.F.R. § 160.103 (definition of “Health information”).

Do the HIPAA privacy regulations apply to recipients of protected health information?

No, unless the recipient is a covered entity as described above (i.e. a health plan, a health care provider, or a health care clearinghouse).

Does HIPAA preempt state law?

Yes and no. Any federal law preempts state law if the laws cover the same subject matter, unless the federal law has exceptions to preemption. The HIPAA privacy statute has a specific section dealing with preemption. The statute provides that the HIPAA privacy statute shall “supersede” any “contrary” provision of state law. Social Security Act section 1178(a)(1), 42 U.S.C. § 1320d-7(a)(1). The statute then lists several exceptions to preemption. Social Security Act section 1178(a)(2), 42 U.S.C. § 1320d-7(a)(2). The HIPAA privacy statute also provides that the HIPAA privacy regulations “shall not supercede a contrary provision of state law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.” Public Law 104-191, § 264(c)(2), Social Security Act section 1178(a)(2)(B), 42 U.S.C. § 1320d-7(a)(2)(B).

There is a three-step process for determining if a state law is preempted by HIPAA:

1. Is the law contrary to HIPAA?
2. Is the law more stringent than HIPAA?
3. Is there a provision of the HIPAA statute or regulations that otherwise excludes the law from HIPAA preemption?

The HIPAA regulations define “contrary” as follows:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

- (1) A covered entity would find it impossible to comply with both the State and federal requirements; or
- (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act [the HIPAA privacy statute] or section 264 of Pub. L. 104-191 [another provision of the HIPAA privacy statute], as applicable. [Italics in original].

45 C.F.R. § 160.202 (definition of “Contrary”).

A state law is more stringent than HIPAA if it meets the following conditions:

1. If a state law provides greater privacy protections to individuals than HIPAA does;
2. If a state law provides individuals with greater rights of access to, or rights to amend, their health information than HIPAA does.

45 C.F.R. § 160.202 (definition of “more stringent”) and § 160.203(b).

In addition, the HIPAA privacy regulations provide that state laws are not preempted if they relate to reporting of disease or injury, child abuse, birth, or death; the conduct of public health surveillance, investigation or intervention; health plan management audits, financial audits, program monitoring and evaluation; or the licensure or certification of facilities or individuals; or (with the approval of HHS) prevention of fraud and abuse; regulation of insurance and health plans; state reporting on health care delivery or costs; compelling need relating to public health, safety or welfare; or regulation of controlled substances. 45 C.F.R. § 160.203.

PRA access and monitoring probably do not fall under any of the above exceptions to preemption. However, this does not mean that PRA access and monitoring are restricted under the regulations. As discussed in the following sections, the HIPAA regulations themselves allow access and monitoring without individual authorization if disclosure and use of health information is required by law. Disclosure of health information to PRA's, without individual authorization, is required under state law. This means that the PRA access and monitoring provisions of the Welfare and Institutions Code are not preempted by HIPAA.

Do PRA's need written authorization from an individual client, patient or resident in order to access individual health information or monitor programs or facilities?

Only to the extent required under the Welfare and Institutions Code. This is because the HIPAA privacy regulations do not require written authorization for disclosure of health information if disclosure of the information is "required by law". 45 C.F.R. § 164.512.

The Welfare and Institutions Code contains the following PRA access provisions, all of which are mandatory and therefore not preempted by HIPAA:

1. Access to clients: Section 5530(a) provides that PRA's "shall have access to all clients and other recipients of mental health services in any mental health facility, program, or service at all times as are necessary to investigate or resolve specific complaints...."
2. Access to diagnostic or treatment staff: Section 5530(b) provides that PRA's "shall have the right to interview all persons providing the client with diagnostic or treatment services."
3. Access to records: Section 5328(m) provides that PRA's shall have access to records when they have been given "knowing voluntary authorization by a client or guardian ad litem." Section 5542 provides that PRA's "shall have the right" to inspect and/or copy any non-confidential records relating to an investigation on behalf of a PRA client, or which indicates compliance or lack of compliance with laws and regulations governing patients' rights. Section 5326.1 provides that the county mental health director or designee (which can include the PRA) shall have access to information pertaining to denial of

rights contained in the person's treatment record including consent forms, required documentation for convulsive treatment, documentation regarding the use of restraints and seclusion, physician's orders, nursing notes, and involuntary detention and conservatorship papers.¹ Sections 5520(b) and 5545 provide that PRA's are authorized to obtain access to otherwise confidential records of non-clients for purposes of monitoring to ensure compliance with patient's rights laws and regulations.

All of these sections impose mandatory duties on the part of facilities, programs and services to allow access and monitoring including disclosure of information. Therefore, the disclosure is "required by law."

The HIPAA privacy regulations set out the following standard for disclosure of health information required by law:

"A covered entity may use or disclose protected health information without the written authorization of the individual ... in the situations covered by this section, subject to the applicable requirements of this section.

... ..

(a) *Standard: uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c) [relating to disclosures about victims of abuse, neglect, or domestic violence], (e) [relating to disclosures for judicial and administrative proceedings], or (f) [relating to disclosures for law

¹County Patients' Rights Advocates have traditionally obtained access to the identity of the patient and the legal portion of the patient's record as the designee of the mental health director under section 5326.1. It should be noted that this section at one time did not allow access to records by the county mental health director or designee. 62 Ops. Cal. Atty. Gen 57 (1979). It has since been amended so that the county mental health director or designee has the same right of access to all information pertaining to denial of rights that the California Department of Mental Health had at the time of the referenced Attorney General opinion. This means access to all treatment records "without qualification" and "without the necessity of first securing the patient's consent as required by section 5328." Id. Since disclosure of the information to the director or designee is mandatory under the statute, there is no preemption under HIPAA.

enforcement purposes] of this section for uses or disclosures required by law. [Italics in original].

45 C.F.R. § 164.512(a).

The regulation broadly requires disclosure of information required by law under subsection (a), but imposes additional requirements (such as notice to the individual) for disclosure in connection with the specific types of activities listed in subsections (c), (e) and (f). None of those specific sections apply to PRA access or monitoring. Subsection (c), relating to disclosures about victims of abuse, neglect, or domestic violence, refers to reports made by the covered entity to agencies authorized to receive reports of abuse such as adult protective services or the police. This would include mandatory and non-mandatory reporting under the elder and dependent adult abuse reporting statute. It does not include disclosures to the PRA's because disclosure is at the request of the PRA, rather than under a reporting statute. Subsection (e) relating to disclosures for judicial and administrative proceedings does not apply because PRA access and monitoring is not part of a court or administrative hearing proceeding. Subsection (f) relating to disclosures for law enforcement purposes does not apply to PRA access or monitoring because that section refers to police procedures, warrants and law enforcement subpoenas. Therefore, the only restriction on disclosure to PRA's is the requirement that the disclosure "complies with and is limited to the relevant requirements of such law," i.e. the access and monitoring authority in the Welfare and Institutions Code.

The definition of "required by law" provides further detail:

"Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a

government program providing public benefits.” [Italics in original, underlining added]

45 C.F.R. § 164.501 (definition of “Required by law”).

PRA access and monitoring authority is enforceable in a court of law, Welfare and Institutions Code sections 5530(a), 5550(b), and 5550(e), and therefore clearly falls within the above definition of “required by law.”

Furthermore, 45 C.F.R. § 164.502(a)(1)(vi) makes it clear that under the HIPAA privacy regulations a covered entity is permitted to disclose protected health information in compliance with 45 C.F.R. § 164.512, discussed above. (Of course, the entity is required, not permitted, to make the disclosures under the Welfare and Institutions Code.) The covered entity does not have authority under the HIPAA privacy regulations to attempt to limit disclosure. 45 C.F.R. § 164.502(b)(2)(v). The entity must comply with the requirements of the law that requires the disclosure. 45 C.F.R. § 164.512(a)(1).

It should be noted that the HIPAA privacy regulations in many cases leave in place other laws, including state laws, that are consistent with the purpose of the HIPAA regulations. (See, e.g. 45 C.F.R. § 164.502(g)(4) which provides: “If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual’s estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.” [Emphasis added]) This is consistent with the purpose of the HIPAA privacy regulations to allow other laws to remain in force so long as the laws provide statutory requirements for the use and disclosure of health information.

Can PRA’s obtain the names of individual patients in a facility without authorization?

Yes, as the designee of the county mental health director.

As discussed above, Welfare and Institutions Code section 5326.1 provides that the county mental health director or designee (which can include the PRA) shall have access to information pertaining to denial of rights contained in the person's treatment record including consent forms, required

documentation for convulsive treatment, documentation regarding the use of restraints and seclusion, physician's orders, nursing notes, and involuntary detention and conservatorship papers. Necessarily, PRA's must have access to the names of patients in a facility in order to access this additional information pertaining to denial of rights. Section 5326.1 is broad enough to cover disclosure of patient names.

The California "patient directory" statute also allows facilities to release certain information upon an inquiry concerning a specific patient, unless the patient objects. California Civil Code section 56.16. However, this statute is preempted by HIPAA at least to the extent that it allows broader disclosure than is permitted under HIPAA regulations. HIPAA regulations allow disclosure of patient directory information only to persons who ask for the patient by name. (a)(1)(ii)(B). Therefore, HIPAA preempts the California provision which allowed disclosure of the name of a patient upon an inquiry concerning a specific patient.

The California statute provides for disclosure of the following information:

1. the patient's name (now prohibited under HIPAA),
2. the general condition of the patient (also allowed under HIPAA), and
3. other information such as the address, age, sex, and medical condition of the patient (now prohibited under HIPAA in the absence of written authorization).

HIPAA regulations allow a facility to maintain a directory of individuals in the facility, which includes: "(A) The individual's name; (B) The individual's location in the covered health care provider's facility; (C) The individual's condition described in general terms that does not communicate specific medical information about the individual." 45 C.F.R. § 164.510(a). HIPAA regulations require that before information can be added to the directory or released, the patient is "informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure." 45 C.F.R. §§ 164.510, 164.510(a). This is the "opt out" provision. It does not require consent to disclose; it allows disclosure if the patient has not requested that the information be withheld after being given an opportunity to object to disclosure. 45 C.F.R. § 164.510 (a)(2), California Civil Code section 56.16. In short, if a hospital wants to maintain a patient directory, it can do so, consistent with HIPAA and California law,

as long as it complies with the HIPAA limitations, including the “opt out” procedures.

In addition, under the HIPAA regulations, this information can be disclosed (for individuals asked for by name) if the individual lacks capacity to “opt out,” or in an emergency. Disclosure must be “[c]onsistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.” 45 C.F.R. §§ 164.510 (a)(3)(i)(A). Also, the provider “may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person’s involvement with the individual’s health care.” 45 C.F.R. §§ 164.510 (b)(3). Disclosure of directory information to a PRA under these sections would always be appropriate unless the provider knows that the patient has expressed a preference on a prior occasion that the information not be disclosed to the PRA.

Are there any other provisions of the HIPAA privacy regulations that may allow monitoring?

Yes. 45 C.F.R. § 164.512(d)(1) permits use and disclosure of protected health information to a “health oversight agency” for “oversight activities authorized by law.” This includes “civil ... investigations; inspections; ... or other activities necessary for appropriate oversight of: (i) The health care system; ... or (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.”

45 C.F.R. § 164.501 defines “health oversight agency” to mean “... an agency or authority of ... a State, ... a political subdivision of a State ... or a person or entity acting under a grant of authority from or contract with such public agency ... that is authorized by law to oversee the health care system (whether public or private) ... or to enforce civil rights laws for which health information is relevant.” This would include PRA’s acting in accordance with the Welfare and Institutions Code access and monitoring provisions.

Health oversight activities do not include activities where the individual is the subject of the investigation or activity. 45 C.F.R. § 164.512(d)(2). In other words, the care or services provided to the individual must be the subject of the investigation or activity, e.g. health records could not be

disclosed under this section as part of a criminal investigation of the individual.

Where can I get more information?

The Department of Health and Human Services Office for Civil Rights has a useful website. The website has a copy of the final regulations as well as HIPAA fact sheets. It can be found at: <http://www.hhs.gov/ocr/hipaa>.

The California Office of HIPAA Implementation (Cal OHI) also has a useful website. It can be found at:

<http://www.ohi.ca.gov/state/calohi/ohiHome.jsp>. Cal OHI is doing a section by section analysis to determine which sections of California law are preempted by HIPAA:

http://www.ohi.ca.gov/state/calohi/ohiGeneral.jsp?sCat=/Nav/Legal%20Issues#legal_completed_preemption_analyses_of_state_privacy_laws. Cal-OHI determinations are binding on departments and agencies of the executive branch of state government. H&SC § 130311, 130302(d). This includes the California Department of Mental Health.² Cal OHI has determined that Welfare and Institutions Code section 5328(m) is not preempted. In the future, it may do an analysis of other provisions of the Welfare and Institutions code relating to PRA access and monitoring authority.

The California Hospital Association Consent Manual also has up-to-date information on HIPAA.

The Georgetown University Health Privacy Project also has a useful website: <http://healthprivacy.com/>.

F:\DOCS\DAN\Health Care\HIPAA\HIPAA.PRA.preemption.memo.2003.08.25.doc

² It does not include county mental health departments, and probably does not include the University of California. Nevertheless those agencies should carefully consider Cal-OHI determinations in the interest of uniform application of HIPAA requirements.