Colantuono, Levin & Rozell, APC

THE HIPAA "PRIVACY RULE"

presented by

Merrilee Fellows
Assistant City Attorney
Cities of Barstow, Calabasas and La Habra Heights

League of California Cities
City Attorneys Department
Annual Conference
Sacramento, California

September 8, 2003

Colantuono, Levin & Rozell, APC
555 West 5th Street, 30th Floor
Los Angeles, CA 90013-1048

(213) 533-4203 (direct)
(213) 533-4191 (fax)

mfellows@clrlawfirm.com
www.clrlawfirm.com

THE HIPAA "PRIVACY RULE"

I. INTRODUCTION

In 1996, the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191; "HIPAA") became federal law. Sections 261 through 264[1] of that legislation require the Secretary of the U.S. Department of Health and Human Services ("HHS") to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known, somewhat ironically, as the *Administrative Simplification* procedures.[2] HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information held by covered entities if Congress did not enact privacy legislation within three years of passage of HIPAA. Because Congress did not enact such legislation, HHS established a set of national standards for the protection of certain health information in its *Standards for Privacy of Individually Identifiable Health Information*. These standards, or regulations, have become known as the "Privacy Rule" and constitute the regulations that implement some of the requirements of HIPAA. (45 CFR Parts 160 and 164, Subparts A and E.) These regulations govern a broad range of activities and are likely to affect most cities in some way.

The Privacy Rule standards address the use and disclosure of individuals' health information – called "protected health information" by organizations subject to the Privacy Rule – called "covered entities." They also address standards for individuals' privacy rights to allow individuals to understand and control how their health information is used. Where functions in which a city engages make it a "covered entity," the city must comply with this Privacy Rule. Additionally, many cities conduct functions that make them "business associates" of a covered entity. A "business associate" is a person or organization that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Thus, for example, a Fire Department may be a business associate of a paramedic service. In order to lawfully disclose protected health information to a business associate, a covered entity must enter into an agreement with each of its business associates. This agreement is required to obtain satisfactory assurances that the business associate will use the information only for the purposes for which the business associate has been engaged by the covered entity.

As may already be clear, the Privacy Rule comprises a lengthy and detailed set of regulations replete with complex requirements and definitions. The intent of this paper is ensure awareness that the requirements of the Privacy Rule may affect a municipality, and thus to provide guidance to analyze whether and how a city may be affected and consequently how and by when it must comply with the requirements of the Privacy Rule.

---

[1] Where sections 261 and 264 are cited here, they refer to those sections of Pub. L. 104-191.

[2] U.S. Department of Health & Human Services, OCR Privacy Brief, "Summary of the hipaa [sic] Privacy Rule," Office for Civil Rights, HIPAA Compliance Assistance, p. 5.

II. THE PRIVACY RULE IN THE CONTEXT OF HIPAA

Viewed as a whole HIPAA addresses a number of issues, among them health care access, portability and renewability, [3] preventing health care fraud and abuse, revising civil monetary penalties and criminal penalties, declaring that certain health insurance policies are not considered to duplicate benefits under Medicare, Medicaid or other policies if they meet certain conditions, patent extension, long-term care services and contracts and administrative simplification.

As summarized by the National Governors Association,

> "[u]nder HIPAA, administrative simplification is the common name given to seven different federal regulations issued by the U.S. Department of Health and Human Services (HHS). Collectively these rules require states to ensure individually identifiable health care information remains confidential and secure (i.e., privacy and security rules). They also require states to standardize the way administrative and financial health care information is exchanged electronically (i.e., transactions and codes, and identifier rules)."[4, 5]

The requirements regarding Transactions and Codes, the National Provider Identifier, the Health Plan Identifier and Employer Identifier are each addressed by the regulations governing "*Administrative Simplification*" and they relate generally to electronic formatting (coding) and electronic exchange of health information.[6] A table summarizing the purpose of each rule, status of adoption of the final rule for each element, and the compliance deadlines is provided at Attachment 3. The remainder of this paper discusses the protection of, and maintaining the privacy of, the transmission of individually identifiable health information, as it is that rule which will most commonly apply to California municipalities.[7]

---

[3] The law provides for increased portability when an insured changes employers through limitation on excluding new employees from medical insurance based on preexisting condition. (29 U.S.C. § 1181.)

[4] Robert Burns, Issue Brief, National Governors Association Center for Best Practices, May 28, 2002, http://www.nga.org/cda/files/HIPAA052802.pdf.

[5] These federal rules are codified as follows: the Privacy Rule (45 C.F.R. §§ 160 and 164, Parts A and E), Security (45 C.F.R. §§ 160, 162 and 164), Transactions and Codes (45 C.F.R. §§ 160 and 162), National Provider Identifier, Health Plan Identifier and Employer Identifier (45 C.F.R. §§ 160 and 162). The complete text of the Security Rule may be found at http://www.ohi.ca.agov/calohi/docs/Security_Final_Rule.pdf.

[6] *See, e.g.,* Robert Burns, National Governors Association, Center for Best Practices, HIPAA Regulation Status, http://www.nga.org/cda/files/0802HIPAA_REGSTATUS.pdf, also provided here at Attachment 3.

[7] In addition, a variety of government agencies and private firms now offer suggestions on their websites regarding the implementation of HIPAA regulations. Several of the more useful sites are identified in this document and at Attachment 1.

Section 264 directed the Secretary of HHS to submit to specified congressional committees detailed recommendations on standards with respect to the privacy of health information about individuals. The Secretary of HHS promulgated regulations and, as required, these regarded:

1. The rights that an individual who is a subject of individually identifiable health information should have.

2. The procedures that should be established for the exercise of such rights.

3. The uses and disclosures of such information that should be authorized or required. (Sec. 264(b).)

The regulations responsive to this legislative mandate are known as the Privacy Rule. [8]

III. PREEMPTION

Pub. L. 104-191, Section 264(c)(2) provided that the Privacy Rule shall not supercede state law if the state law is both contrary to the federal regulations and is more stringent than the requirements, standards or implementation specifications imposed under the regulation.[9] Thus, HIPAA privacy regulations set a minimum federal standard for protecting patient privacy. Consequently, because of the preemption provisions, the laws that entities covered by HIPAA must follow will actually be some combination of HIPAA and California patient-privacy laws.

As noted by Stephen A. Stuart, Senior Staff Counsel with the California Office of HIPAA Implementation ("CalOHI"):

> "Due to the complexity and ambiguity of federal regulations, and the vast amount of State privacy law which must be analyzed (particularly in California), the HIPAA preemption analysis is considered to be one of if not the most challenging aspects of HIPAA implementation. The analyses are also not static—current State laws may be amended and new laws promulgated which will necessitate re-analyses at least annually. In addition, HIPAA itself has been amended twice since issuance of the Privacy Rule in December, most recently in August of 2002."[10]

Health and Safety Code Section 130331.5 has been newly adopted to provide that any State law determined by CalOHI to be preempted shall not be applicable to the extent of that

---

[8] The Privacy Rule is comprised of Part 160 and Part 164, Subparts A and E. The text of 45 C.F.R. Part 160 is available at http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr160_02.html; Part 164 is available at http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html.

[9] *See* 45 C.F.R. Part 160, Subpart B.

[10] HIPAA/State Law Preemption Fact Sheet, available at http://www.ohi.ca.gov/calohi/docs/Preemption_Factsheet.pdf.

preemption and that the remainder of the State law shall remain in full force and effect. The language in the new law is designed to allow State departments and agencies to follow State health information privacy/access laws, but only to the extent these laws are not preempted by HIPAA. Health and Safety Code Section 130331.5 also requires CalOHI to provide statewide leadership, coordination, direction and oversight for determining which provisions of State law governing personal medical information are preempted by HIPAA.

HIPAA provides that states may, through their Governors, request an "exception determination" from federal HHS, with respect to a particular law, under certain circumstances. While the request for an exception determination is pending, covered entities must comply with HIPAA provisions.

Among the state legislation that requires preemption analysis is the California Public Records Act (Cal. Gov't Code §§ 6250 *et seq.*). CalOHI is completing preemption analyses of that act and others and is supporting the development of appropriate legislation. Thus a record that is subject to disclosure under the California Public Records Act might or might not be disclosable after consideration of the requirements of HIPAA's Privacy Rule whether a basis for that conclusion can be found in the Records Act or not.

IV. WHAT INFORMATION MUST BE PROTECTED AND BY WHOM?

Terms Used in the Regulations

A number of critical terms are defined by and used in the regulations. Discussed below are the terms "covered entity," "business associate," "health plan," "participant," "medical care," "protected health information," and "individually identifiable health information."

Covered Entity

The Privacy Rule requires that a Covered Entity – that is, an entity covered by the provisions of this Rule – must meet a number of requirements (discussed in Section VI). "Covered entity" means:

> "(a) Except as otherwise provided, the standard, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
>
> (1) A health plan.
>
> (2) A health care clearinghouse.
>
> (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." (45 C.F.R. 160.102(a).)

Cities will commonly be "covered entities" as "health care providers" as that term is defined below.

For assistance in determining whether an entity is covered, a variety of decision tools increasingly are being made by federal and state organizations responsible for implementation and compliance with this Rule. The Centers for Medicare & Medicaid Services provide, at their website, "flip charts" and "flowcharts." (*See* http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/CoveredEntityFlowcharts.pdf.)

The health plan or health care entities most likely to be relevant to a City are defined at 45 C.F.R. § 160.103, as follows:

> "Health plan means an individual or group plan that provides, *or pays the cost of*, medical care (as defined in section 2791(a)(2) of the PHS [Public Health Service] Act, 42 U.S.C. 300gg-91(a)(2)).
>
> (1) Health plan includes the following, singly or in combination:
>
> (i) A group health plan, as defined in this section.
>
> …
>
> (xvii) *Any* other individual or group *plan*, or combination of individual or group plans, *that provides or pays for the cost of medical care* (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2))." (Emphasis added.)

Examples include health insurance issuers, HMOs, group health plans, Medicare, Parts A and B, Medicare + Choice, and Medicaid. Because cities commonly self-insure certain medical benefits programs (such as dental plans, vision plans, and medical services provided via Employee Assistance Plans), they will commonly be covered entities by virtue of this definition.

"Group health plan" means, in relevant part:

> "an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
>
> (1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7); or
>
> (2) Is administered by an entity other than the employer that established and maintains the plan." (45 C.F.R. 160.103 (definitions in alphabetical order).)

29 U.S.C. 1002(1), referenced within the definition quoted above, defines the referenced term "employee welfare benefit plan" as follows:

> "(1) The terms 'employee welfare benefit plan' and 'welfare plan' mean any plan, fund, or program which was heretofore or is hereafter established or maintained by an employer or by an employee organization, or by both, to the extent that such plan, fund, or program was established or is maintained for the purpose of providing for its participants or their beneficiaries, through the purchase of insurance or otherwise,
>
> (A) medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, death or unemployment, or vacation benefits, apprenticeship or other training programs, or day care centers, scholarship funds, or prepaid legal services, or
>
> (B) any benefit described in section 186(c) of this title (other than pensions on retirement or death, and insurance to provide such pensions)."

Under ERISA, a group health plan is a separate legal entity from the employer/plan sponsor. Group health plans that do not receive protected health information (defined in the pages following) are subject only to limited requirements of the Privacy rule. The Privacy Rule does not cover employers or plan sponsors. (HHS/OCR 2003, 45 C.F.R. § 164.500)

29 U.S.C. 1002(7) defines "participant" as:

> "any employee or former employee of an employer, or any member or former member of an employee organization, who is or may become eligible to receive a benefit of any type from an employee benefit plan which covers employees of such employer or members of such organization, or whose beneficiaries may be eligible to receive any such benefit."

42 U.S.C. 300gg-91(a)(2), cited above, defines "medical care" as follows:

> "The term 'medical care' means amounts paid for -
>
> (A) the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,
>
> (B) amounts paid for transportation primarily for and essential to medical care referred to in subparagraph (A), and
>
> (C) amounts paid for insurance covering medical care referred to in subparagraphs (A) and (B)."

Note that these definitions carefully exclude mental health services from the definition of "medical care," although the distinction between mental health and medical treatments will not always be easily drawn. (But also note, as discussed in the following paragraphs, that the "individually identifiable health information" that must be protected *includes* information about an individual that relates to mental health.)

A health care provider is any person or organization who furnishes, bills, or is paid for health care in the normal course of business. (45 C.F.R. § 160.103.) Health care providers are covered only if they transmit health information electronically in connection with a transaction covered by the HIPAA transaction rule (*see* 45 C.F.R. §§ 162.1101 – 162.1802), directly or through a business associate.

"Individually Identifiable Health Information"

The Privacy Rule centers on "protected health information," requiring that all "individually identifiable health information" held (maintained) or transmitted, in any form or medium, whether electronic, paper, or oral (the "protected health information") be protected from unauthorized disclosure in a prescribed manner. (45 C.F.R. § 160.103.)

> "*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and:
>
> (1) Is created or received by a health care provider, health plan, employer, 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; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." (45 C.F.R. 160.103.)

Individually identifiable health information includes many common identifiers such as name, address, birth date and Social Security number. Excluded from protected health information are employment records that a covered entity maintains in its capacity as an employer, as well as education and certain other records. (20 U.S.C. § 1232g.)

There are, however, no restrictions on the use or disclosure of the Orwellian category of "de-identified health information." (45 C.F.R. 164.502(d)(2).) De-identified health information neither identifies nor provides a reasonable basis to identify an individual. (45 C.F.R. 164.514(a).) The two ways to de-identify information are by a formal determination by a qualified statistician or by removal of specified identifiers of the individual and the individual's

relatives, household members, and employers. De-identification is adequate only if the covered entity has no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information. (45 C.F.R. 164.514(b).)

Protected Health Information

"*Protected health information* means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium." (45 C.F.R. 164.501, terms listed alphabetically.)

Business Associate

"*Business associate* … (1) … means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." (45 C.F.R. 160.103.)

That is, a business associate is a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information. Thus, for example, a city that bills recipients of medical transport services rendered by a separate entity is a business associate of that separate medical transport provider. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. Note, too that a covered entity may be a business associate of another covered entity. Thus, a city could be a covered entity by virtue of a self-insured dental plan and a business associate of a medical benefits provider.

V. THE GENERAL PRINCIPLE FOR USES AND DISCLOSURES

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information except either (1) as authorized by the individual who is the subject of the information (or to the individual's personal representative) or (2) as the Privacy Rule permits or required. (45 C.F.R. § 164.502(1).) A covered entity *must* disclose protected health information in only two situations: (a) to individuals (or their personal representatives) when they request access to, or an accounting of disclosures of, their protected health information, and (b) to HHS when it undertakes a compliance investigation or review or enforcement action. You'll note that news coverage of accident and crime victims has often excluded information regarding the current medical condition of these persons, commonly reported prior to the April 2003 effective date of the Privacy Rule as to most large covered entities.

A. Permitted Uses and Authorized Uses

The Privacy Rule distinguishes between consent and authorization, terms which do not overlap.[11] The requirement to obtain a "consent" applies in different circumstances than the requirement to obtain an "authorization." In content, a consent and an authorization differ substantially from one another.

B. Uses by Consent[12]

A "consent" allows use and disclosure of protected health information only for treatment, payment, and health care operations. It is written in general terms and refers the individual to the

[11] This discussion is taken from the Federal Register, December 28, 2000 (Vol. 65, No. 250), pages 82461-82510, II. Section-by-Section Description of Rule Provisions, Section 164.506, as made available at http://www.advancednetworksystems.net/45_CFR_Parts_160_thru_164_B.html, p. 66 of 168.

[12] The consent requirements are stated at 45 C.F.R. 164.506.

covered entity's notice for further information about the covered entity's privacy practices. It allows use and disclosure of protected health information by the covered entity seeking the consent, not by other persons, and the use is to carry out treatment, payment or health care operations (known in HIPAA circles as "TPO"). Most persons who obtain a consent will be health care providers; health plans and health care clearinghouses may also seek a consent.

C. Authorized Uses[13]

With a few exceptions, to make uses and disclosures that are not covered by the consent requirements and not otherwise permitted or required under the final rule, covered entities must obtain the individual's "authorization." An "authorization" must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. In some instances, a covered entity may not refuse to treat or cover individuals based on the fact that they refuse to sign an authorization. Examples where authorization is required include psychotherapy notes and marketing. The core elements of a valid authorization are stated at 45 C.F.R. 164.508(c) and among others, require a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion, the name of the person authorized to make the requested use or disclosure, a description of each purpose of the requested use or disclosure, an expiration date, signature, statements adequate to place the individual on notice of his or her right to revoke the authorization in writing, the authorization to be in plain language and a copy of the signed authorization provided to the individual.

D. Opportunity to Agree or Object[14] and Exceptions Thereto

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure. The uses and disclosures covered here include use for facility directories, for involvement in the individuals' care and notification purposes (i.e., to notify a family member where the protected health information is directly relevant to such person's involvement with the individual's care or payment related to the individual's health care), and for disaster relief purposes. Uses and disclosures for which an authorization or opportunity to agree or object is not required include those uses and disclosures required by law, for public health activities (e.g., controlling disease, tracking FDA-regulated products, or to enable product recalls or repairs), regarding victims of abuse, neglect or domestic violence, for health oversight activities, for judicial and administrative proceedings, law enforcement purposes, regarding decedents, for cadaveric organ, eye or tissue donation purposes, for research, to avert a serious threat to health or safety, regarding military activities, and others. (45 C.F.R. 164.512.)

E. Summary

Covered entities may use or disclose protected health information only with consent, for treatment, payment or health care. They must use or disclose the protected health information as

[13] The requirements for authorization are stated at 45 C.F.R. 164.508.

[14] The requirements are found at 45 C.F.R. 164.510.

authorized by the individual for other disclosures after the individual is given an opportunity to agree or object, and in accordance with the specific public purposes under law. Also, a number of exceptions exist for which an authorization or opportunity to agree or object is not required.

Covered entities must disclose protected health information upon request by the individual and to the federal Office for Civil Rights for enforcement purposes.

VI. OBLIGATIONS OF COVERED ENTITIES

In summary form, the following requirements are triggered by status as a covered entity. Each covered entity must identify any business associates. The covered entity must enter into a contract with each such business associate that identifies the permitted uses and disclosures the business associate may make, require use of appropriate safeguards of the information, require the reporting of non-permitted uses and disclosures to the covered entity, and require the business associate to extend the same terms to its subcontractors and agents. (45 C.F.R. § 164.504(e).)[15] A sample business associate contract, provided by the U.S. Department of Health and Human Services, is attached to this paper as Attachment 2.

Practice Tip: While the attached sample includes the provisions required by the Privacy Rule, note that it does not include all elements to establish a valid contract (e.g., consideration), nor does it include a number of other provisions that are generally included in agreements between municipalities and other entities such as venue, severability, integration, notice, provisions for successors, and others. Another frequent failing by covered entities that submit these "form" contracts to their municipality business associates is that the contract fails to identify the parties clearly, and fails to refer with specificity to the underlying "service agreement."

If the City concludes that it is a covered entity, it must:

- Enter into agreements with all business associates.

- Develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. (45 C.F.R. § 164.530(i).)

- Designate a "privacy official" responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices. (45 C.F.R. § 164.530(a).) Given the relationship of the Privacy Rule to employee benefits programs, this responsibility will commonly be given to personnel directors.

[15] A "business associate" is exempted from some requirements such as disclosures to a provider for treatment to an individual, uses or disclosures by a government health plan (e.g., Medicare) to another agency (e.g., Social Security Administration) for eligibility or enrollment determinations if authorized by law. (*See* 45 C.F.R. § 164.502(e).)

- Train all workforce members on its privacy policies and procedures, as necessary,[16] and have and apply appropriate sanctions against workforce members who violate the privacy policies and procedures or the Privacy Rule. (45 C.F.R. § 164.530(e).)

- Mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule. (45 C.F.R. § 164.530(f).)

- Maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to the otherwise permitted or required use or disclosure. (45 C.F.R. § 164.530(c).)

- Have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. (45 C.F.R. § 164.530(d).) The covered entity must explain those procedures in its privacy practices notice. (45 C.F.R. § 164.520(b)(1)(vi).)

- Maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. (45 C.F.R. § 164.530(j).) This rule is an exception to the destruction after two years authorized by the Government Code for the destruction of public records and will generally require most local governments that are covered entities to revise their records retention policies.

In addition, a covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or other appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. (45 C.F.R. § 164.530(g).) Further, a covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility. (45 C.F.R. § 164.530(h).)

Exceptions

There are two exceptions to the obligations identified above – those for a "fully-insured group health plan" and for a "hybrid entity." A fully-insured health plan provides benefits solely through an insurance contract with a health insurance issuer (such as CalPERS or an HMO). The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of

[16] The State of California Health and Human Services agency summarizes a number of HIPAA training programs provided by Covansys, Gartner Consulting, KPMG Consulting and PricewaterhouseCoopers LLP. *See* http://www.training.ca.gov/hipaa/. A variety of legal counsel can provide these training services, as well.

protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan. (45 C.F.R. § 164.530(k).)

Practice Tip: Plan sponsors of fully-insured health plans that seek to avoid the more intensive requirements of the Privacy Rule should ensure that they do not become so involved in administration of the health plans that they inadvertently obtain protected health information.

The Privacy Rule also provides for reduction of the burden of these requirements on entities, such as cities, that conduct both covered and non-covered functions. Such an entity, known as a "hybrid entity" (164.504(a)-(c)), must designate in writing the operations it conducts that constitute covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule apply only to the health care components. Thus, for example, a city must train only those members of its workforce who are involved in the health care component of the city's operations, but it also must "firewall" the health care information available to those members (that is, identify the employees or classes of employees who will have access to protected health information, restrict access only to such employees and only for health plan functions; and provide procedures for resolving employee violations of the requirements of the Privacy Rule).

A covered entity that does not make this designation is subject to the Privacy Rule as to all of its staff and programs. It will be a useful strategy to attempt to establish your client as a hybrid entity to reduce the number of staff who must be trained and whose mistakes can generate adverse legal consequences under HIPAA.

VII. TIMES FOR COMPLIANCE

The Privacy Rule compliance date was April 14, 2003, though the deadline is extended to April 14, 2004 for entities entitled to either of two exceptions. For an entity which is a business associate by virtue of a written contract existing as of October 15, 2002 and not renewed or modified by April 14, 2003, the covered entity need not contract with the business associate to restrict the use of individually identifiable health data until April 14, 2004. (45 C.F.R. § 164.532(d).) In addition, the Privacy Rule extends compliance to April 14, 2004 for a "small health plan." A small health plan is "a health plan with annual receipts of $5 million or less." (45 C.F.R. 160.103.) Cities that are covered entities solely due to self-insured benefits programs may commonly be entitled to this status. The Department of Health and Human Services has issued guidance as to how to measure such receipts.[17] The guidance distinguishes between those health plans that do and do not report receipts to the IRS. As cities generally do not report receipts to the IRS on identified tax forms, the proxy measures for receipts are the following:

.

> "Health plans that do not report receipts to the IRS – for example, ERISA group health plans that are exempt from filing income tax returns – should use proxy measures to determine their annual receipts. Fully insured health plans should use the amount of total premiums which they paid for health insurance benefits during

[17] Guidance issued by Centers for Medicare & Medicaid Services, Department of Health and Human Services. See Q&A at http://questions.cms.hhs.gov.

the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine the proxy measures to determine their total annual receipts." (Guidance issued by Centers for Medicare and Medicaid Services; *see* http://questions.cms.hhs.gov/.)

VIII. PENALTIES

The regulations provide for a number of civil and criminal penalties for violation of the Administrative Simplification Portion of HIPAA. These are summarized below, in a table provided by the California Office of HIPAA Implementation.[18]

CIVIL PENALTIES

Monetary Penalty	Term of Imprisonment	Offense
$100	N/A	Single violation of a provision (can be multiple violations with penalty of $100 each as long as each violation is for a different provision)
$25,000	N/A	Multiple violations of an identical requirement or prohibition made during a calendar year

CRIMINAL PENALTIES

Monetary Penalty	Term of Imprisonment	Offense
Up to $50,000	Up to one year	Wrongful disclosure of individually identifiable health information
Up to $100,000	Up to five years	Wrongful disclosure of individually identifiable health information committed under false pretenses
Up to $250,000	Up to 10 years	Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm

[18] From http://www.ohi.ca.gov/calohi/docs/hipaa_penalities.doc.

IX. Conclusion

To protect the privacy of individual health information, the federal HIPAA legislation and regulations have imposed numerous requirements on entities that create, transmit or receive health information. The obligations of a covered entity are extensive and the penalties for noncompliance can be severe. While many municipalities may conduct health plans that result in their being a covered entity, even more cities are likely to be business associates of other covered entities. Given the size (as measured by receipts) of most California cities' health plans, it is likely they will be considered small health plans, thus compliance is not required until April14, 2004. Nevertheless, with the protections required, training and notices necessary to comply, it is wise to consider these issues now.

Attachment 1

HIPAA WEB RESOURCES

Text of the Regulation:

HHS/OCR Unofficial Version of the Regulation,
Text of 12/28/2000 as amended Part 160 (5/31/2002) and Parts 160, 164 (8/14/2002)
http://www.hhs.gov/ocr/combinedregtext.pdf
Text of Regulations also at:
http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr160_02.html (Part 160)
http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html (Part 164)

California Office of HIPAA Implementation:
http://www.ohi.ca.gov/

Extensive background information and guidance for compliance provided by HHS:
http://www.hhs.gov/ocr/hipaa/privacy.html
http://cms.hhs.gov/hipaa/hipaa2/default.asp

Decision Models for Whether and How HIPAA Applies:
http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/CoveredEntityFlowcharts.pdf

General Informative Site:
American Health Information Management Association (AHIMA)
(and free monthly HIPAA Newsletter (*In Confidence*)) from:
http://www.ahima.org

Technical Assistance:
Centers for Medicare and Medicaid Services
Email Questions: askhipaa@cms.hhs.gov
HIPAA Hotline for Questions: 1-866-282-0659
FAQs on Privacy Rule: http://questions.cms.hhs.gov/

Example of Privacy Notice:
http://www.gscares.com/pdf/PrivacyRights.pdf (English and Spanish)
(Santa Barbara County)

Attachment 2

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information[19]

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

[19] Sample provisions provided by U.S.Department of Health & Human Services Office for Civil Rights at: http://www.hhs.gov/ocr/hipaa/contractprov.html.

Sample Business Associate Contract Provisions[20]

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].

b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].

c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

[20] [Footnote 1 in original.] *Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.*

d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

j. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would

not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
[List Purposes].

b. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).

d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

    1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

    2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

    3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

    [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.

    1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors

or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

HHS Home | OCR Home | Topics | A-Z | For Kids
Disclaimers | Privacy Notice | FOIA | Accessibility | Contact Us

Last revised: August 14, 2002

Attachment 3

HIPAA Regulation Status

Privacy, Security, and Administrative Simplification (Title II)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires all health plans, health information clearinghouses, and providers who conduct certain health care transactions electronically (collectively known as covered entities) to ensure that individually identifiable health information remains private and secure. It also requires these covered entities (and their business associates) to standardize the way certain administrative and financial health care data is exchanged electronically. The U.S. Department of Health and Human Services (HHS) plans to issue seven different regulations to implement and enforce these requirements. These federal rules include:

Rule		Purpose	Enforcement Agency	Proposed Rule	Final Rule	Compliance Deadline[†]
Privacy [45 CFR § 160 and 164]		Prescribes the standards, procedures, and protocols covered entities must adopt to protect a patient's right to keep their medical records and other personal health information confidential. The privacy rule outlines the procedures required for the exercise of those rights and the conditions necessary for others to use or disclose protected health information.	OCR	11/3/99	8/14/02[‡]	4/14/03
Security [45 CFR § 160, 162, and 164]		Outlines the minimum administrative, technical, and physical safeguards required to prevent unauthorized access to health information.	CMS	8/12/98	4/21/03	4/21/05
"ADMINISTRATIVE SIMPLIFICATION"	**Transactions and Codes** [45 CFR § 160 and 162]	Establishes uniform standards to govern how certain treatment, billing, enrollment, and other health information must be formatted (codes) and exchanged (transactions) electronically.	CMS	5/7/98	3/24/03[±]	10/16/02[*]
	National Provider Identifier	Specifies the alphanumeric format for the code that must be adopted to uniquely identify providers (or sellers) of health care services for billing and other purposes.	CMS	5/7/98	—	—
	Health Plan Identifier	Specifies the alphanumeric format for the code that must be adopted to uniquely identify group plans providing health care benefits through insurance. Health plan identifiers are often used to enroll new employees; verify beneficiary (or employee) eligibility, benefits, and premium payments; and other purposes.	CMS	—	—	—
	Employer Identifier [45 CFR § 160 and 162]	Specifies the alphanumeric format for the code that must be adopted to uniquely identify health plan sponsors (or employers). Employer identifiers are often used to enroll new employees; verify beneficiary (or employee) eligibility, benefits, and premium payments; and other purposes.	CMS	6/16/98	7/30/02	7/30/04
Enforcement		Establishes the framework for enforcing the administrative simplification regulations.	OCR/CMS	4/17/03[γ]	—	—

OCR = HHS' Office for Civil Rights | *CMS = Centers for Medicare and Medicaid Services*

[†] *Small health plans have one additional year following this date to be compliant.*

[‡] *Originally finalized December 28, 2000, HHS proposed modifications to the privacy rule on March 27, 2002. The modifications were finalized on August 14, 2002. The compliance deadline did not change.*

[±] *Originally finalized on August 17, 2000, HHS proposed modifications to the transactions rule on May 31, 2002. The modifications were finalized on March 24, 2003. The compliance deadline did not change.*

[*] *The compliance deadline could have been extended by one year if a compliance plan was submitted to HHS before October 16, 2002. Small health plans were not eligible for the conditional extension.*

[γ] *The HIPAA enforcement rule is being released in stages to help covered entities gauge as soon as possible the procedural requirements that will later apply as compliance proceeds.*

Table by Robert J. Burns, Policy Analyst, Health Policy Studies Division, (202) 624-7729, rburns@nga.org
©2003 National Governors Association