

**PRIVACY REGULATIONS AND RELATED ISSUES
FOR SELF-INSURED EMPLOYEE WELFARE BENEFIT PLANS
AND THIRD PARTY ADMINISTRATORS¹**

W. Fulton Broemer
BROEMER & ASSOCIATES, LLC
3104 Edloe, Suite 300
Houston, Texas 77027
Direct Dial: (713) 439-0079
Main Number: (713) 439-0033
Facsimile: (713) 439-0034
WFB@BroemerLaw.com

Recently issued guidance and new regulations regarding the privacy of health information will radically alter the way in which health care providers and plan sponsors handle patient records. This outline describes the key features of the new regulations and highlights some of the issues that employers, sponsors, insurers, and administrators of group health plans should begin to focus on in connection with medical record privacy.

**I.
BACKGROUND**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of Health and Human Services to propose standards protecting the privacy of individually identifiable health information by August 21, 1997. On September 11, 1997, the Secretary submitted a report to Congress recommending comprehensive privacy legislation. Under HIPAA, Congress was given two years (until August 21, 1999) to enact privacy legislation.

If Congress failed to act by that date, the Secretary was directed to finalize regulations containing proposed standards relating to the electronic transfer of medical information by February 21, 2000. The new regulations, while narrower in scope than the Secretary's 1997 recommendations, are responsive to this statutory mandate.

For many years, Congress has struggled with medical privacy issues. Even facing a statutory deadline, Congress was unable to reach consensus and failed to meet the August 21, 1999 deadline for legislation, although the issue was hotly debated. Congressional sponsors of pending privacy legislation have vowed to continue working to pass legislation by the end of the 106th Congress in 2000.

Since Congress failed to pass legislation by the statutory deadline, the Secretary of Health and Human Services moved forward as required by HIPAA. On November 3, 1999, a proposed rule was published in the *Federal Register* (64 Fed. Reg. 59918) establishing standards for privacy of electronically transmitted individually identifiable health information. A summary of the proposed standards prepared by the U.S. Department of Health and Human

¹Based on original materials produced by Phyllis Borzi.

Services is attached. It can also be downloaded from the Department's web-site at <http://aspe.hhs.gov/admnsimp/pvcsumm.htm>.

On August 17, 2000, the U.S. Department of Health and Human Services took the first definitive step toward enacting the proposed privacy regulations by issuing the National Standards for Electronic Transactions. The complete final rule can be found at <http://aspe.hhs.gov/admnsimp/>.

☞ **EFFECTIVE DATE:** The National Standards for Electronic Transactions become effective for most health plans on October 16, 2002. The National Standards for Electronic Transactions become effective for "small health plans" (plans with annual receipts of \$5,000,000 or less) on October 16, 2003.

Remaining to be enacted are:

- Standards for Privacy of Individually Identifiable Health Information
- National Standard Health Care Provider Identifier
- National Standard Employer Identifier
- Security and Electronic Signature Standards
- National Standard for Health Claim Attachments
- National Standard Identifiers for Health Plans

The proposed regulations for each of the issues listed above may be found at <http://aspe.hhs.gov/admnsimp/nprm/index.htm>.

II. THE BASIC RULE

The new regulations center around three main issues: "covered entities," "protected health information," and "permitted uses." Each of these three core terms will be discussed in greater detail below. In general, the new regulations provides that "covered entities" may only disclose "protected health information" (PHI) with the patient express authorization, or as explicitly permitted by the regulation ("permitted uses"). Additionally, even when a covered entity is acting within the requirements of the new regulations, only the "minimum necessary" PHI may be used or disclosed. PHI is protected throughout the life of the individual and for two years after the individual's death, subject to certain exceptions.

A. "Covered entities"

"Covered entities" are broadly defined. The term includes:

- health care providers,
- health plans,
- health care clearinghouses, and
- any health care provider who transmits health information in electronic form in connection with transactions (i.e., exchanges of information) referred to in

§1173(a)(1) of HIPAA (a standard electronic transmission of medical data).

“Covered entities” include any ERISA-covered group health plan with 50 or more participants, and any plan administered by an entity other than the employer/sponsor or any insurer of the plan (as defined by HIPAA to include an insurance company, insurance services, or insurance organization (including a health maintenance organization) which is licensed to engage in the business of insurance in a state and which is subject to state law regulating insurance (within the meaning of ERISA section 514(b)(2)). ERISA §733(b)(2). Medicaid, Medicare, the Veterans health system and the Federal Employees Health Benefit Program are covered entities.

☞ **NO EXEMPTIONS FOR GOVERNMENT AND CHURCH PLANS:** While exempt from ERISA, church plans and governmental plans are included in the new regulations as covered entities. See Preamble to proposed rule, II.A.7, 64 Fed. Reg. at 59931. The list of covered entities also specifically references employee welfare benefit plans sponsored by two or more employers, including MEWAs (multiple employer welfare arrangements).

B. Business partners

The proposed rules are also applicable to data exchanges between covered entities and their “business partners.” Business partners are defined as persons to whom a covered entity discloses protected health information so that the person can “carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity.” Business partners can include agents, contractors or other persons who meet the functional test described above (including lawyers, auditors, third-party administrators, billing agents, data processing entities, etc.). Employees of the covered entity are not business partners. The circumstances in which covered entities can disclose protected health information to their business partners is described below, but, generally speaking, covered entities may only share information with business partners pursuant to a contract that limits the use and disclosure of PHI under the same restrictions that apply to the covered entity.

C. “Protected health information” (PHI)

“*Protected health information*” or PHI means individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity (this information remains protected regardless of any subsequent form that it may take, i.e., it’s still protected after it is printed out).

“*Health information*” is any information (whether oral or recorded in any form or medium) created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of health care to an individual. This represents the broad

category of information governed by the administrative simplification provisions of HIPAA.

“Individually identifiable health information” is a subset of “health information.” It is information that identifies the individual or creates a reasonable basis to believe that the information identifies the individual. Data is “electronically maintained or electronically transmitted” if the source or target of a transmission is a computer. Once the data has passed through a computer, however, it remains protected regardless of whether or not it is subsequently transmitted by paper or voice.

As defined above, PHI is a subset of individually identifiable health information. Note that the protections described below apply to data or information about an individual, not to any particular record. However, once these privacy protections attach to data, the data must be protected by both the transmitter and receiver of the data in every record (written, electronic or other) in which the data appears. The proposed regulation also addresses the problems that covered entities will face with respect to mixed records (i.e., records containing both protected and unprotected data).

III. DISCLOSURE OF PHI

A. General rule

As previously noted, under the proposed rule covered entities (and their business partners) are prohibited from using or disclosing health information except:

- as authorized by the patient, or
- as explicitly permitted by the regulation.

In addition, certain individual rights (described below) are also incorporated in the proposed regulation.

B. Disclosures without patient authorization only for permissible uses

The new regulations permit use or disclosure of PHI without patient authorization for treatment, payment or health care operations related to treatment or payment.

“Health care operations” means certain services or activities necessary to carry out the management functions of the covered entity with respect to treatment or payment, such as conducting quality assessment and improvement activities, evaluating provider performance, engaging in accreditation, certification or licensing activities, underwriting relating to an existing contract for purposes of renewal, auditing, or compiling or analyzing information in connection with civil or criminal legal proceedings.

In addition, PHI could be used or disclosed for certain public-policy related purposes

(e.g., public health, research, health oversight, law enforcement, and use by coroners). Covered entities would be permitted to use and disclose PHI if required to do so by other law, such as a mandatory reporting requirement under State law or pursuant to a search warrant. Covered entities are required to disclose PHI only in two instances: to permit individuals to inspect and copy their own medical records and to enforce the proposed regulation.

Even if the covered entity is authorized to use or disclose PHI, it must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure (“minimum necessary use or disclosure”). In certain instances, it may be prudent that the decision as to what is the minimum necessary PHI that is disclosable should be made by someone other than the covered entity (for example, if disclosure is required under a State law requiring mandatory reporting of new tuberculosis infections, the minimum necessary determination is made by the State when it specifies what data needs to be reported). In addition, part of the “minimum necessary” determination must begin with an assessment of whether or not the intended use or purpose could be accomplished by de-identifying the data, rather than narrowing the scope of disclosure of PHI. Although recognizing the difficulty that covered entities will have in applying the “minimum necessary” rule in operation because it is not a bright-line test, the preamble to the proposed regulation contains several interesting operational observations:

- each proposed use or disclosure of PHI must be considered on a case-by-case basis;
- general policies adopted by covered entities to automatically approve all requests (or request for a certain type of information) may be problematic;
- use or disclosure of the whole medical record, absent explicit a request to do so, would presumptively violate the rule.

Under the proposed regulation, individuals could request that the covered entity restrict further uses and disclosures of PHI for treatment, payment or health care operations (but not if such uses or disclosures were mandated by law), but the covered entity would only be required to adhere to more restrictive policies and procedures if it agrees to the patient’s request.

C. Disclosure with patient authorization

The two most common situations in which disclosure or use of PHI with patient authorization are likely to occur are when (1) the individual wants access to his or her own medical information for personal use or wants the covered entity to disclose certain PHI to someone else (such as wanting his or her medical record to be forwarded to a new primary care physician or HMO) and (2) when the covered entity requests authorization because it wants to use or disclose the information for purposes other than treatment, payment or health care operations.

If the individual initiates the authorization for disclosure, the request must be sufficiently specific so that the covered entity knows what information is covered by the authorization. It must also identify the person(s) to receive the PHI, state a specific expiration

date for the authorization, include a signature or other authentication, and must acknowledge that the individual has the right to revoke the authorization at any time. In addition, if the proposed disclosure of PHI would be to an entity other than a covered entity, the authorization must clearly state that the individual understands that disclosure to non-covered entities would remove any privacy protections that had attached to the PHI.

If a covered entity initiates the authorization for disclosure, certain additional requirements are imposed, beyond those which the proposed regulation imposes when the individual initiates the authorization. Among the further requirements are: (1) the covered entity must specify the purposes for which the information is requested and how it will be used so that the individual can make an informed judgment whether to consent to the disclosure; (2) the request is subject to the “minimum necessary” requirements, described above; (3) individuals must be advised that they have a right to inspect and copy the information to be used or disclosed and that they have a right to refuse to authorize the requested use or disclosure; (4) treatment and payment cannot be conditioned or influenced by the individual’s authorization; and (5) if the covered entity would be receiving financial or in-kind compensation in exchange for using or disclosing the PHI, the authorization must state that disclosure would result in commercial gain to the covered entity. The proposed regulation provides examples of these situations: a health plan that wants to sell or rent its enrollee list or a pharmaceutical company that offer discounts to providers who share lists of patients with certain medical conditions, so that the company may market its products directly. The proposed regulation includes a model authorization form. See Appendix to Subpart E of Part 164, 64 Fed. Reg. 60065.

Note that general waivers of confidentiality of a patient’s medical information that often appear on enrollment or claims forms would no longer be valid under this proposed regulation.

D. Disclosure to business partners

Covered entities may disclose PHI only pursuant to a written contract that would, among other things, limit the business partner’s use and disclosure of PHI only to what was permitted by the contract. In addition, the contract must contain certain security, inspecting and reporting requirements. Covered entities would be responsible for certain violations of the new regulations committed by their business partners. Also covered entities could be business partners of other covered entities (e.g., an HMO which performs administrative services for an employer’s self-insured group health plan).

IV. RIGHTS OF INDIVIDUALS

Under the proposed regulation, certain rights of individuals are enumerated. For instance, individuals have a right to:

- inspect and obtain a copy of all PHI relating to the individual;
- amend and/or correct that PHI;

- an accounting of the uses and disclosure of their PHI (i.e., to know when and to whom disclosure has been made for purposes other than treatment, payment and health operations;
- notice and a full description of the covered entity's use and disclosure practices. Any use or disclosure of PHI not described in this notice is prohibited;
- challenge the covered entity's use or disclosure of PHI through (1) complaints to the privacy official designated by each covered entity and through the complaint process that must also be established or (2) through complaints to the Secretary of HHS through a process that the Secretary will establish.

V. NOTICE REQUIREMENTS

Individuals must be given a plain-language written notice of the covered entities practices and procedures regarding PHI. Generally the notice must describe what is done with their PHI, how it is safeguarded, and what rights individuals have with respect to that information, including the right to inspect and copy PHI. The notice must also identify the covered entity's privacy officer and, if different, a contact person for registering complaints and obtaining additional information. The notice must be distributed by the later of the effective date of the final regulation or at enrollment. In addition, the notice must be distributed at least once every three years thereafter. If a covered entity materially changes its procedures, it must update the notice and redistribute it within 60 days of the change.

In addition, as long as the covered entity maintains the PHI, individuals have a right to request a list of all instances in which PHI is disclosed by a covered entity for purposes other than treatment, payment and health care (some limited exceptions are provided for disclosures to law enforcement and oversight agencies). Covered entities must provide this information within a reasonable time after the request is made, but no later than 30 days following the receipt of the request.

VI. ADMINISTRATIVE REQUIREMENTS FOR COVERED ENTITIES

Among other things, covered entities must:

- designate a privacy official;
- develop a privacy training program for employees;
- implement safeguards to protect PHI from intentional or accidental disclosure or misuse;
- provide a complaint mechanism for individuals to challenge or dispute the use or disclosure of health information;
- develop sanctions for employees or business partners who violate the covered entity's privacy policy or procedures;
- maintain documentation of the covered entity's policy or procedures for complying with the proposed regulation.

VII.
PREEMPTION OF STATE PRIVACY LAWS

The new Federal privacy requirements create a minimum Federal floor of privacy protection. They do not generally supercede state medical privacy laws that relate to the privacy of individually identifiable health information, except to the extent that provisions of state law are “contrary” to the Federal requirements. However, state laws that impose “requirements, standards, or implementation specifications” with respect to individually identifiable health information that are more stringent than the Federal law are not considered “contrary” to Federal law. Certain other state laws may also be exempt from preemption if the Secretary determines they are necessary (1) to prevent fraud and abuse, (2) to ensure appropriate state regulation of insurance and health plans, and (3) for state reporting on health care delivery or costs. In addition, state laws which the Secretary finds address controlled substances are not preempted. The proposed regulation establishes a process under which the Secretary would issue advisory opinions regarding whether a state law was more stringent than the Federal law.

VIII.
ENFORCEMENT

The Secretary of HHS can bring enforcement actions against covered entities. Under HIPAA, the Secretary may impose civil monetary penalties of not more than \$100 per person per violation and up to \$25,000 for violations of a single standard within a single calendar year. In addition, criminal penalties are established under HIPAA for wrongful disclosures of PHI, which, upon conviction, could result in fines of not more than \$50,000 and/or imprisonment for not more than one year. Offenses committed with intent to sell, transfer or use PHI for commercial or personal gain or malicious harm are punishable by a fine not to exceed \$250,000 and/or 10-year imprisonment.

Private rights of action are not authorized for wrongful disclosure violations. However, the Secretary proposes to establish a complaint system to permit individuals to report violations to the Secretary so that appropriate investigation and enforcement activities could be undertaken by the Department on behalf of an aggrieved individual.

IX.
EFFECTIVE DATE

Covered entities must be in compliance not later than 24 months after the effective date of the final regulation. Covered entities that are small health plans (i.e., one with annual receipts of \$5 million or less) have 36 months after the effective date of the final regulation to comply.

X.
KEY ISSUES FOR SELF-INSURED PLANS

- ✓ Definitional ambiguities (e.g., “business partners,” “minimum necessary use or disclosure”)
- ✓ Effect on disease management and wellness programs
- ✓ Protecting against liability for unauthorized disclosures
- ✓ Agreements to restrict uses and disclosures
- ✓ Determining when PHI can be used or disclosed without individual consent
- ✓ Identifying and segregating PHI in mixed records (i.e., those containing both protected and non-protected information)
- ✓ Determining which state laws may be preempted and under what circumstances
- ✓ Costs and administrative burdens
- ✓ Notice requirements
- ✓ De-identifying information (i.e., removal of identifying personal characteristics)
- ✓ Determining what is the “minimum necessary use or disclosure”
- ✓ Creating “firewalls” within the covered entity and/or business partners to prevent inadvertent use or disclosure of PHI
- ✓ Review and possible renegotiation of contracts with entities considered “business partners”
- ✓ Establishing a system to monitor compliance of employees and business partners

XI. COMPLIANCE STRATEGY

- ✓ Review current systems for handling medical information and identify potential problem areas .
- ✓ Begin to develop policies and procedures to comply with proposed rule
- ✓ If at all possible, adopt HHS’s model authorization form and any other model forms that the final regulation includes.
- ✓ Establish procedures to document and monitor compliance.