

HIPAA

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

<p>Rose Ann Davis ABC CONSULTING SERVICES 102 Lakeside Drive Kemah, TX 77565-2007 Cell Phone: (713) 412-5249 Main Number: (281) 334-5554 Facsimile: (281) 538-1087 roseadavis@earthlink.net</p>	<p>W. Fulton Broemer BROEMER & ASSOCIATES, LLC 3336 Richmond Avenue, Suite 400 Houston, Texas 77098 Direct Dial: (713) 328-1101 Main Number: (713) 328-1100 Facsimile: (713) 328-1130 WFB@BroemerLaw.com</p>
--	---

I. OVERVIEW

The issuance of new regulations and the passage of new legislation have imposed numerous legal requirements upon group health plans that affect virtually every aspect of health plan administration. The Health Reform Act of 1996 is formally titled the Health Insurance Portability and Accountability Act of 1996 (H.R. 3103), and is informally referred to as “HIPAA”. The law is principally a tax act that amends and adds sections to the Internal Revenue Code. In order to conform to the Code changes, this Act concurrently amended ERISA, the Public Health Services Act, and other pertinent law, and thus modified many aspects of group health coverages.

The Departments Labor, Treasury, and Health and Human Services were entrusted to work together on issuing coordinated implementation rules and enforcement procedures. Temporary, interim, and final regulations providing further guidance and information on the law’s requirements

have been issued sporadically since HIPAA was signed into law on August 21, 1996.

Under ERISA, plan participants and beneficiaries can sue plan fiduciaries who violate the requirements. The Secretary of Labor can also sue to remedy ERISA violations. Under the Internal Revenue Code, the IRS can impose an excise tax **up to \$100 for each day, for each responsible entity, for each individual with respect to whom such a failure occurs**. The maximum penalty is the lesser of 10% of the amount due under the \$100 per day rule or \$500,000. Under state law, the states are responsible for enforcing HIPAA with insurers and HMO's. However, if the states refuse or fail to take enforcement action, the U.S. Secretary of Health & Human Services may assume that responsibility. Sanctions, including monetary penalties, can be imposed on insurers and HMO's.

II. PORTABILITY -WHO MUST COMPLY?

Portability rules are established for group-to-group and group-to-individual markets. Portability is encouraged and achieved through a variety of mechanisms, including prohibitions on discrimination in eligibility, limits on exclusions due to health status, and limits on the use of pre-existing conditions exclusions and waiting periods.

In general, HIPAA applies to "group health plans" and to "health insurance issuers" who offer coverage to "group health plans". A "group health plan" is an employee welfare benefit plan that provides medical care to employees or their dependent directly or through insurance, reimbursement or otherwise. Note that this definition does include group health plans insured through a carrier, as well as plans that are self-insured or self-funded. A "health insurance issuer" is defined as an insurance company, insurance service or insurance organization (including an HMO) that is licensed under state law to engage in the business of insurance and is subject to state

law.

Employers with 2 or more participants in a group health plan who are current employees must comply. Single-employer plans, multiple-employer welfare arrangements (MEWA's), collectively bargained plans, church plans, and government plans affected by the act. However, state and local governments may elect to be excluded from the rules.

In general, HIPAA does not apply to certain coverage in relation to those listed as "excepted benefits". Excepted Benefits are those which are benefits under one or more of the following:

- Coverage only for accident or disability income insurance
- Coverage issued as a supplement to liability insurance
- Liability insurance (including general liability and automobile liability)
- Workers' compensation coverage
- Automobile medical payment insurance
- Credit-only insurance
- Coverage for on-site medical clinics
- Other coverage where medical care is secondary or incidental to other benefits
- Benefits provided under a separate policy for long-term care, nursing home care, home health care, and other similar limited benefits
- Limited-scope dental or vision expense benefits
- Coverage only for specified disease or illness, hospital indemnity, or other fixed indemnity insurance
- Medicare supplemental health insurance and other supplemental coverage.

HIPAA portability rules may or may not apply to FSA's, some Dental plans, and/or EAPs', depending upon the facts and circumstances of the coverage.

III. SPECIAL ENROLLMENTS

Plans must provide a description of the special enrollment rights on or before an employee is first offered the opportunity to enroll in the plan. Also, plans must provide a description of special enrollment rights to those who decline coverage.

Special Enrollment Rights are provided for:

- Individuals who lose their coverage in certain specified situations

- Individuals who become a new dependent through marriage, birth, adoption, placement for adoption, or due to court order.
- If an eligible Employee and/or Dependent declined coverage under the Plan when initially eligible because of other health coverage, application for coverage may be made when involuntary loss of other group coverage or a change in Family status occurs.

The special enrollment rights may apply with respect to an Employee, a Dependent of an Employee or both. The special enrollment period begins on the date of the event, the individual must be allowed at least 30 days for special enrollment due to an involuntary loss of eligibility of an Employee and/or affected Dependents under another Group Health Plan or through a Health Insurance Issuer offering group health insurance coverage resulting from:

- legal separation or divorce;
- death;
- termination of employment;
- reduction in work hours;
- all employer contributions for the coverage were terminated; or
- COBRA continuation coverage under the other plan has been exhausted.

An individual does not have to elect COBRA continuation coverage or exercise similar continuation rights in order to preserve the right to special enrollment. However, an individual does not have a special enrollment right if the individual loses the other coverage as a result of the individual's failure to pay premiums/contributions or for termination of coverage for cause (such as making a fraudulent claim or an intentional misrepresentation of a material fact in connection with the Plan).

Loss of eligibility for an Employee and/or affected Dependents coverage under a governmental plan such as Medicare, Medicaid, or CHAMPUS coverage. A change in Family status due to:

- marriage;
- birth of a Child; or

- adoption or Placement for Adoption of a Child; or
- court order.

The special enrollment rules allow an eligible Employee to enroll when he marries or has a new Child (as a result of marriage, birth, adoption, Placement for Adoption, or court order). A Spouse of a Participant can be enrolled separately at the time of marriage or when a Child is born, adopted, placed for adoption, or court ordered. The Spouse can be enrolled together with the Employee when they marry or when a Child is born, adopted, placed for adoption, or court ordered. A Child who becomes a Dependent of a Participant as a result of marriage, birth, adoption, Placement for Adoption, or court order can be enrolled when the Child becomes a Dependent. Similarly, a Child who becomes a Dependent of an eligible Employee as a result of marriage, birth, adoption, Placement for Adoption, or court order can be enrolled if the Employee enrolls at the same time. Individuals who enroll under these special enrollment conditions are not considered Late Entrants.

The Effective Date of coverage for those individuals timely enrolled during a special enrollment is *no later than*:

- for loss of eligibility under a Group Health Plan, another group Health Insurance Issuer offering group health insurance coverage, or a governmental plan such as Medicare, Medicaid or CHAMPUS coverage, the first day of the calendar month following the date of application; or
- for a marriage, the first day of the calendar month following the date of application; or
- for a birth, the date of birth; or for an adoption or Placement for Adoption, the date of the adoption or placement; or for a court order, the date of the court order or the date coinciding with the Employee's Effective Date, whichever is later.

IV. GUARANTEED AVAILABILITY

HIPAA requires that health insurance issuers who offer coverage in the individual market must guarantee issue, without any pre-existing condition exclusions to *eligible individuals* (as

defined). Furthermore, individual market health insurance issuers are required to renew existing individual market health insurance policies (at the insured's option). The individual market health insurance portability provisions do not apply to the previously-listed "excepted benefits" that are not an integral part of the plan. Individual market health insurance issuers are state licensed insurance companies, insurance services, and insurance organizations (including HMO's).

The primary responsibility for implementation and enforcement of these requirements lies with the states. However, CMS (formerly HCFA) has the right to enforce implementation if a state substantially fails to act. States can either enforce the federal HIPAA requirements or implement an alternative mechanism that will achieve the goal of providing access to individual health insurance coverage without imposing pre-existing condition exclusions. Individuals eligible for the portability provisions are those that meet the following:

- Had health insurance coverage for at least 18 months (states may enact a shorter period) with no significant break in coverage (63 days or more; states may enact a longer period);
- The most recent coverage was through an employment-related group health plan, *regardless of the amount of time covered* (even if just for one day). This does not include a conversion policy available at the end of a COBRA continuation period.
- Is not currently eligible for Medicare, Medicaid, or covered under any other health insurance;
- Has exhausted available COBRA continuation or other similar continuation coverage (including state-mandated continuation).

IV. HEALTH STATUS NONDISCRIMINATION RULES

Regulations have been issued that provide guidance on the nondiscrimination provisions based on health factors. Generally, under HIPAA, a group health plan or group health insurance issuer is prohibited from denying an individual eligibility for benefits based on a health factor, and from charging an individual higher premiums than a similarly situated individual based on any health factor. Furthermore, a plan may not deny eligibility or charge a higher premium because an

individual is confined to a hospital. The regulations also provide that a plan generally may not impose an “actively-at-work” clause. In addition, eligibility of premium charge cannot be based on any individual’s ability to engage in normal life activities.

The regulations do allow a plan to limit or exclude benefits, but only if such limitation or exclusion is applied uniformly to all similarly situated individuals. The limitation or exclusion cannot be directed at individual participants based on any health factor. Health factors are: health status, medical condition (including both physical and mental illnesses), claims experience, receipt of health care, medical history, genetic information, evidence of insurability, and disability.

A plan or issuer may impose limits or exclude benefits for a specific disease or condition, or limit or exclude benefits based on a determination of whether the benefits are experimental or not medically necessary ONLY IF the benefit limitation or exclusion is applied uniformly to all similarly situated individuals. Also, annual, lifetime or other limits may be imposed, and the plan may require satisfaction of a deductible, copayment, coinsurance or other cost-sharing requirements in order to obtain a benefit, but only if the limits or requirements are applied uniformly to all similarly situated individuals.

A person cannot be excluded from a plan for engaging in certain recreational activities (such as motorcycling, snowmobiling, ATV operation, etc.). These are known as “source of injury” restrictions. However, a plan can exclude benefits for injuries sustained as a result of various recreational activities *if* the accident did not result from any medical condition (mental and/or physical) or from domestic violence.

Although a plan or insurer generally may not impose an “actively at work” or “actively at life” clause that would deny eligibility or benefits or charge an individual a higher premium, there

are some exceptions. An Actively-at-work clause is permissible if individuals who are absent from work are treated (for purposes of health coverage) as if they are actively at work. Therefore, plan provisions that delay enrollment until an individual is actively at work on a day following a waiting period are prohibited unless the individual is considered "actively-at-work" if the absence is due to any health factor. Additionally, the regulations provide an exception for the first day of work. Under the exception, an individual may be required to actually begin work (for at least one day) before coverage becomes effective.

HIPAA's nondiscrimination provisions do not prevent health plans or issuers from establishing wellness incentives to encourage participants to participate in health promotion and disease prevention programs and to attain specific outcomes. These incentives may take the form of discounts or rebates, or of modifications to applicable copayments or deductibles. Alternatively, HIPAA's provisions do prohibit plans from imposing a "penalty" for unhealthy activities.

In general, bona fide wellness programs must offer a limited reward or discount. The reward may be a premium discount, a rebate of premium or contribution, a waiver of all or part of a cost-sharing mechanism (such as deductibles, copays or coinsurance), or the absence of a surcharge. The reward may not exceed a specified percentage of the cost of employee-only coverage under the health plan (based on the total amount of employer and employee contributions for the employee's benefits package).

The wellness program must be reasonably designed to promote good health and disease prevention (e.g., the program offers reduced premiums to participants who achieve a cholesterol count of under 200). To meet this requirement, individuals must have the opportunity to qualify for the program's reward at least once a year. A plan that bases a reward or penalty on health factors

present when the individual first enrolls in the health plan is not reasonably designed to promote health or prevent disease.

The reward must be available to all similarly situated employees. If it is unreasonably difficult or medically inadvisable for a participant to satisfy the initial program standard, the program must provide a reasonable alternative standard. Plans do not have to establish reasonable alternatives before the program begins—they can develop alternatives after being informed of a participant's difficulty in meeting the original standard. Alternative standards must take into account the participant's relevant health factors.

V. PREEXISTING CONDITION EXCLUSION RESTRICTIONS

Under the Act, group health plans may impose limited preexisting condition restrictions on coverage provided to new enrollees, including employees and dependents. Individuals must be given written notification of the plan's preexisting condition limitations and waiting periods at the time of enrollment. The notification must include information on the individual's right to request a Certificate of Creditable Coverage, and a statement that the current plan or issuer will provide assistance in obtaining such a certificate if necessary.

Furthermore, if the plan decides to impose a preexisting condition exclusion on an individual, the individual must be given written notice of the plan's determination, the period for which the exclusion applies, the basis for the determination (including the source and substance of any information on which the plan relied), and the plan's appeal procedures (and these must include the right to submit additional evidence of creditable coverage).

Plans may refuse or limit coverage for a new enrollee for up to 12 months (18 months for a late enrollee) for a health condition that was treated or diagnosed in the six months before

enrollment. The exclusion period must be reduced by the number of days of prior creditable health coverage (unless there has been a break of more than 63 days).

In no event will a Pre-existing Condition Exclusion apply to the following:

- Pregnancy;
- Genetic Information in the absence of a diagnosis or other care or treatment of the condition related to the genetic diagnosis;
- A Newborn, an adoptee under the age of 18, or a Child under the age of 18 Placed for Adoption with the Participant, so long as the Child is enrolled in the Plan within thirty-one (31) days after birth, adoption, or Placement for Adoption, (whichever is applicable), pursuant to the provisions set forth in the "Eligibility for Coverage" Section of the Plan.

For purposes of the Pre-existing Condition provision, (1) "Enrollment Date" means the first day of coverage under the Plan or, *if earlier*, the first day of the Waiting Period under the Plan (if applicable); and (2) the Pre-existing Condition Exclusion period will be reduced by the days of Creditable Coverage, excluding any Creditable Coverage incurred prior to a "Significant Break in Coverage". The term "Significant Break in Coverage" means a period of more than 63 days during which an individual has no type of Creditable Coverage. This term does not include any Waiting Period (or affiliation period for HMO's) under the Plan or any other plan or insurance coverage.

V. Creditable Coverage

Creditable coverage includes prior coverage under a group health plan (including COBRA/continuation coverage), HMO, individual health plan, public health plan, Medicaid or Medicare, military and non-military government plan, Indian Health Services medical plan, a state health risk pool, and the Peace Corps Health Plan. Coverages previously listed as "excepted benefits" are not included when determining creditable coverage.

Creditable coverage is count in days, and is counted backwards from the employee's first date of *employment* (for new employees), or the first day of *coverage* (for special or late enrollees).

Days in a waiting period with no coverage are not creditable coverage, nor are these days taken into account when determining a significant break in coverage (a break of 63 days or more).

To demonstrate evidence of Creditable Coverage, individuals must present to the plan administrator a Certificate(s) of Creditable Coverage, issued by the prior plan(s) or insurance carrier(s), or, in the absence of such Certificate(s), such other evidence of health coverage as may be required by the plan administrator, including but not limited to, copies of claim forms, explanations of benefits, pay stubs reflecting premium payments, and summary plan descriptions. If necessary, the plan administrator will assist an individual in obtaining the Certificate(s) of Creditable Coverage.

Any individual who terminates coverage is eligible for a Certificate of Creditable Coverage. A Certificate of Creditable Coverage will indicate how many days of creditable coverage an individual had under a prior eligible plan. It is not required that separate certificates be issued for each covered person in a family, if the information is identical for each individual. However, if the information is different, it can still be included on the same Certificate if it provides all the required information for each individual.

Certificates of Creditable Coverage must be provided as follows:

- For a covered individual who is a qualified beneficiary entitled to elect COBRA continuation coverage, the Certificate must be provided no later than when a notice is required to be provided for a qualifying event under COBRA. Further, if the individual does elect COBRA, a second Certificate must be provided within a reasonable period of time after coverage ceases. The second certificate only has to cover the period of COBRA coverage.
- For a covered individual who is not a qualified individual entitled to elect COBRA, the certificate must be provided within a reasonable time after coverage terminates.
- Certificates must also be provided upon request any time requested within 24 months after coverage ceases, as soon as reasonable possible after the request is received.

The health plan and the insurance company (if applicable) are jointly responsible for

providing Certificates of coverage. If either provides the Certificate, the requirement is considered satisfied. Insured plan may totally transfer this responsibility to the insurance company by contract.

VII. HIPAA PRIVACY REGULATIONS

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 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 became 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>.

A. 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.

1. “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).

2. 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.

3. “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).

B. DISCLOSURE OF PHI

1. 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.

2. 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.

3. 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.

4. 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).

C. 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.

D. 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.

E. 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.

F. 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.

G. 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.

G. 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.

H. 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

I. 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.