Jenkens & Gilchrist®
A PROFESSIONAL CORPORATION

A SUMMARY
OF THE
FINAL HIPAA PRIVACY REGULATIONS:
Everything You Need To Know
But Did Not Know What To Ask!

www.jenkens.com

FEBRUARY 2001

TABLE OF CONTENTS

A Summary of the HIPAA Privacy Regulations:
Everything You Need To Know But Did Not Know What To Ask!

A SUMMARY OF THE FINAL HIPAA PRIVACY REGULATIONS:

EVERYTHING YOU NEED TO KNOW BUT DID NOT KNOW WHAT TO ASK!

Jenkens & Gilchrist

History And General Overview Of The Rules

On December 20, 2000, the United States Department of Health and Human Services ("HHS") released the long awaited final rule on Standards for Privacy of Individually Identifiable Health Information. (The rules were actually published in the Federal Register on December 28, 2000.) These rules, which are commonly referred to as the HIPAA Privacy Rules ("Privacy Rules"), are extremely complex and extensive. They constitute 1500 pages of material and more than 350 pages of the Federal Register, and once fully implemented, will have a dramatic impact upon the operation of virtually every health care provider, insurer (including self insured plan of employers for their employees), and health care clearinghouses (such as third party administrators of self-insured plans) as well as their business affiliates such as attorneys, accountants, and other consultants. Virtually every entity in the health care field needs to begin planning how to implement these rules ***NOW***!

The Privacy Rules, which are explained in detail, below, are one part of a "suite of rules" adopted by HHS to implement the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA, also commonly referred to as the Kennedy Kassebaum bill after its initial sponsors, Senators Ted Kennedy and Nancy Kassebaum, is principally known as a law that mandated the portability of health insurance. However, among its lesser known contents, HIPAA established standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care providers, and health care clearinghouses who transmit information electronically with respect to these transactions. The same provisions direct HHS to develop standards to protect the security, confidentiality and integrity of individually identified health care information. The Preamble describes the purpose of these provisions:

> "Congress called for steps to improve 'the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.' To achieve that end, Congress required [HHS] to promulgate a set of interlocking regulations establishing standards and protections for health information systems."

The Privacy Rules are one segment of this set. In August 2000 HHS published a final rule addressing Standards for Electronic Transactions that generally govern the transmission of information relating to health care insurance claims, payment and enrollment. Proposed rules have also been published governing standards for establishing security of electronic

information systems, a unique identifier for employers to use in electronic heath care transactions, and a unique identifier for providers for such transactions. Rules governing three other areas have yet to be proposed. Specifically with respect to the Privacy Rules, as part of HIPAA, Congress mandated HHS to submit to the Congress recommendations for protecting the rights of individuals who are the subject of individually identified health information, and, if Congress failed to enact legislation with respect to the privacy of such information by August 1999, the agency was to adopt standards by rule. That mandate, and Congress' failure to act, is the genesis of these rules.

Until the publication of these rules, the protection of privacy of health care information has largely been left to the individual states. The final HIPAA Privacy Rules now provide a national standard and set national requirements for the protection of private health information. However, there is no one mechanism for implementation mandated. Rather, the implementation of the rules is "scaled" to allow covered entities to implement the rules in a practical way that takes into account the size and nature of their business. Additionally, although the statute says that the Privacy Rules preempt State law, there is an exception where the standards in State law are more stringent.

The impact and importance of the Privacy Rules is demonstrated by the fact that the agency received more than 52,000 comments on the proposed rules. Additionally, the agency conducted numerous meetings with a variety of interest groups in the process.

Violations of the rules give rise to both criminal and civil penalties. These penalties range in dimension from fines of $100 per violation or $25,000 per year for a covered entity for unintentional violations, to criminal penalties of fines of up to $250,000 and 10 years imprisonment per offense if the purpose of the offense is to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. There are varying penalties in between depending upon the level of intent. Additionally, it is not inconceivable that enterprising plaintiffs attorneys will turn to tort law to seek redress for violations.

By regulatory amendment published on February 28, 2001, the effective of the rules was changed to April 14, 2001, but covered entities and their business affiliates have two years after that date to comply. However, because of the degree of effort and expense that covered entities and their business partners are likely to experience in complying with these rules, providers, plans, clearinghouses, and business affiliates need to understand these rules and begin the process of implementing these rules now. What follows below is a section-by-section analysis of the final HIPAA Privacy Rules.

HIPAA Section 164.502
The General Rule Concerning Uses and Disclosures of Protected Health Information

The final HIPAA Privacy Rules start off with a "general rule" concerning the use and disclosure of protected health information by covered entities. The general rule is found in Section 164.502 of the final rules and it requires covered health care providers who have ***a***

direct treatment relationship with an individual to obtain a general "consent" from the individual in order ***to use or disclose protected health information about the individual for treatment, payment and health care operations.*** The details on who must obtain such consents and the requirements the consents must meet are found in § 164.506 which is summarized in more detail below.

The consents required under HIPAA are intended to balance both the covered provider's need to use or disclose protected health information for treatment, payment, and health care operations, and also the individual's interest in understanding and making an informed consent to such uses and disclosures of information by the covered provider. HIPAA's general rule also includes various degrees of formality in the consents which range from very informal verbal agreements to more specific and highly detailed written consents and authorizations. Verbal agreements are intended to accommodate situations where it is neither appropriate to remove from the individual the ability to control the protected health information nor appropriate to require formal, written permission to share such information. Two common examples of when it is permissible to use "verbal agreements" are for purposes of collecting information for use in the "facility directory," e.g., information provided by a hospital receptionist to someone looking for the patient, and disclosure of the patient's health information to family members, such as a spouse, parent, child or close friend. However, the health care provider must inform the patient in advance of its intent or desire to use or disclose this information and give the patient the opportunity to prohibit or object or otherwise restrict the use and disclosure of the information. For example, the patient must be given the opportunity to opt out of being listed in the hospital's directory or be allowed to tell the hospital that it can disclose information to the patient's spouse, but not the patient's brother.

The new HIPAA regulations also require covered providers ***to accommodate reasonable requests by patients about how the covered provider communicates with the individual.*** For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual at his or her place of employment, or to send communications to another designated address. ***Covered providers must accommodate the request unless it is unreasonable.*** Similarly, the final rule permits individuals to request that health plans communicate with them by alternative means, and the health plan must accommodate such a request if it is reasonable and the individual states that disclosure of the information could endanger the individual. The specific provisions relating to confidential communications are covered under Section 164.522 and are summarized in greater detail below.

For use or disclosure of information other than as more specifically described in Section 164.510, HIPAA requires more formal written consents and authorizations from the patient. The details on who must obtain such consents and authorizations and what such documents must contain as well as the exceptions to the rule are discussed in detail in connection with Section 164.508 of the new rules. These documents are intended to provide individuals with concrete information and control over the uses and disclosures of protected health information about themselves.

There are also situations in which consent of the patient is not required at all. These are generally in support of important public policy purposes such as, for example, controlling the spread of contagious diseases, facilitating defective product recalls and prevention of child abuse. A complete summary of these and other exceptions to the general rule are found in connection with the discussion of Section 164.512.

The final rule also includes provisions ***that require*** a covered entity to disclose protected health information. Specifically, the mandatory disclosure is required when individuals request access to information about themselves, and when disclosure is compelled by the Department of Health and Human Services (DHHS) for determining compliance with and enforcement of HIPAA regulations.

Section 164.502 also states that in some cases a person other than the actual patient must be treated the same as the patient in terms of obtaining agreements, consents and authorizations to use and disclose health information. Generally those include the personal representatives of deceased individuals (including executors and administrators of the patient's estate), persons with powers of attorney to make health care decisions for a patient (such as through a living will), parents, guardians or others who stand in *"loco parentis"* for either minor or incapacitated adult patients.

As with any general rule there are numerous exceptions many of which will be discussed in greater detail below. However, in the case of abuse, neglect or endangerment situations, the hospital or other covered entity can elect to not to treat the parent or guardian as a covered individual if the entity providing treatment has a reasonable belief that (1) the patient has been the victim of abuse or neglect; (2) the person who caused the abuse or neglect is the person seeking to make the health care decisions, e.g., parent, spouse, guardian, and that by allowing this person to make the health care decisions could endanger the patient or (3) that the hospital or other covered HIPAA entity in the exercise of its professional judgment decides it is not in the best interest of the patient to treat that person as the individual's "personal representative" under these rules.

With respect to an unemancipated minor, a parent may act on behalf of an unemancipated minor in making decisions related to health care. A covered entity must treat such person as a personal representative under this rule with respect to protected health information relevant to such personal representation. However there are three (3) exceptions to this general rule. These exceptions occur if: (1) the minor consents to a health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (2) the minor may lawfully obtain such health care service without the consent of a parent, and the minor, a court, or another person authorized by law consents to such health care service; or (3) a parent assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service. Under these exceptions, HIPAA does not provide a minor with the authority to act under the rule unless the state has given them the ability to

obtain health care without consent of a parent, or the parent has assented. In addition, the HIPAA regulations ***do not supersede state law where the state law authorizes or prohibits disclosure of protected health information to a parent.*** This rule does not affect parental notification laws that permit or require disclosure of protected health information to a parent.

Another important aspect of the general rule is that only the *"minimum necessary"* information may be disclosed to third parties, even with a consent or agreement. In other words, a covered entity cannot reveal more than the third party needs to know for a particular purpose. For example, a third party billing company who prepares and sends bills for a hospital or medical clinic may need to know the patient's home address and the dates he or she was treated in the hospital or clinic, but not the fact that the patient was being treated for a brain tumor. There are exceptions to this general rule. The *"minimum necessary"* requirement does not apply to disclosures made to another health care provider for treatment, e.g., a general practice physician who refers the patient to a specialist may disclose any and all protected health information to the specialist. Other exceptions to the "minimum necessary" standard include disclosures made to the individual patient or to the Department of Health and Human Services when it investigates whether or not the entity has violated HIPAA or when disclosures are required by law, such as in a child abuse or neglect case.

The *"minimum necessary"* standard also applies to the authority of a personal representative who is authorized to act on behalf of the patient particularly to one whom the patient has given the representative a power of attorney or who has been named in a "living will" as having authority to act on behalf of the patient. For example, if the scope of a person's authority to make health care decisions for an individual is limited to decisions regarding treatment for a head injury, such person is a personal representative and must be treated as the individual with respect to protected health information related to the treatment of the head injury. However, such a person ***is not*** the personal representative of the individual with respect to ***all protected health information*** about the individual, and therefore, a covered entity may not disclose the fact that the patient has liver cancer if it is not relevant to the treatment of the head injury. Obviously, if the written power of attorney or living will is more broadly drafted to specifically include all types of health problems, then disclosure of additional information to the personal representative of the patient would not run afoul of the HIPAA general rule.

If protected health information is "de-identified," in accordance with the procedures specified Section 164.514, then such information may be fully disclosed to any other party for any purpose unless the information is or can be re-identified with the individual patient. Therefore, if patient names and other identifying information are removed from the records, e.g., addresses, Social Security and driver's license numbers, phone numbers, *etc.*, and the records are given random account numbers, e.g., patient number 123456, then disclosure of the specific health information is permissible unless the disclosure also includes a key or mechanism that could be used to re-identify the specific patient.

With regard to "business associates" of a covered health care entity, HIPAA requires a business associate contract not only when the covered entity discloses protected health

information to a business associate, but also when the business associate creates or receives protected health information on behalf of the covered entity. The nature and specific terms of such contracts are expressly covered under Section 164.504. A more detailed summary of this provision appears below.

There are specific exceptions to the "general rule" in Section 164.502 which allow for the disclosure of protected health information by so-called "Whistleblowers." Whistleblowers are employees of a covered health care entity, subcontractors, or other persons associated with a business associate. A covered entity is not in violation of the requirements of the general rule against non-disclosure of protected health information when a member of its workforce or a business associate discloses protected health information to: (i) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity; (ii) an appropriate health care accreditation organization; or (iii) an attorney for the Whistleblower in order to determine the Whistleblower's options with respect to whistle blowing.

Furthermore, the covered entity will not be in violation of this rule, provided that the Whistleblower believes in good faith that the covered entity has engaged in conduct which is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the covered entity potentially endanger one or more patients, workers or the public.

Finally, the provisions of Section 164.502 state that a covered entity is not in violation of the rule when a workforce member of a covered entity who is the victim of a crime discloses protected health information to law enforcement officials about the suspect of the crime. For example, if a hospital employee is the victim of an attack, whether inside or outside of the hospital premises, e.g., at a nearby restaurant, but spots the perpetrator of the attack sometime later when the perpetrator seeks medical care at the hospital, the workforce member who was attacked may notify law enforcement of the perpetrator's location and other identifying information. In other words, the hospital employee can tell the police that the suspect is in the hospital emergency room being treated for a gunshot wound to the foot. However, a non-employee who was victimized by the same criminal suspect, but who happens to see the suspect in the hospital cannot have a hospital employee relay that same information to the police. The non-employee victim would have to contact police directly. With respect to disclosures by workforce members of the health care entity, however, the disclosure of protected health information about the suspect other than that described in Section 164.512(f)(2) of the final HIPAA rules is not permitted. A full summary of Section 164.512 appears below.

Section 164.504: Uses and Disclosures: Organizational Requirements Component Entities, Affiliated Entities, Business Associates and Group Health Plans.

This Section introduces new definitions related to the distinctions and standards applicable to organizations that may include component entities or perform functions subject

to HIPAA compliance. Also included are the definitions and standards applicable to business entities, affiliated entities and health plans.

Under this section, the rules attempt to differentiate health plan, covered health care provider and health care clearinghouse activities from other functions carried out by a single legal entity. The provisions at §§ 164.504(a)-(c) introduce the concept of a "hybrid entity" which is defined as "a single legal entity that is a covered entity and whose covered functions are not its primary functions." For purposes of a "hybrid entity," the rules apply only to the part of the entity that is the health care component. In analyzing the term "primary functions," the rules suggest that a common sense evaluation take place: "is most of what the covered entity does related to its health care functions?" If so, then the whole entity should be covered.

The health care component rules are designed for the situation in which the health care functions of the legal entity are not its dominant mission. For example, a multinational corporation composed of multiple subsidiary companies would not be a single legal entity, but a small manufacturing firm and its health clinic, if not separately incorporated, could be a single legal entity. Because some part of the legal entity meets the definition of a health plan or other covered entity, the legal entity as a whole could be required to comply with the rules. Recognizing that this may not be practical, the rules require that for such an entity, its compliance efforts should focus on the component that is actually performing the health care functions. Under such circumstances, the rules require that the covered entity erect firewalls to protect against the improper use or disclosure within or by the organization. See § 164.504(c)(2). This safeguard provision is consistent with the statutory requirement and extends to any covered entity that performs "non-covered entity functions" or operates or conducts functions of more than one type of covered entity.

Section 164.504(d) permits legally distinct covered entities that share common ownership or control to designate themselves, or their health care components, together to be a single covered entity. Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. Such organizations may promulgate a single shared notice of information practices and a consent form. For example, a corporation with hospitals in twenty states may designate itself as a covered entity and, therefore, be able to merge information for joint marketplace analyses. The requirements that apply to a covered entity also apply to an affiliated covered entity. For example, under the minimum necessary provisions, a hospital in one state could not share protected health information about a particular patient with another hospital if such a use is not necessary for treatment, payment or health care operations. The covered entities that together make up the affiliated covered entity are separately subject to liability under this rule. The safeguarding requirements for affiliated covered entities track the requirements that apply to health care components.

The rules in Section 164.504(e) are intended to extend from the covered entity to its contracted or business affiliates certain obligations related to the confidential treatment of

identifiable health information. Covered entities may disclose protected health information to persons that meet the rule's definition of business associate, or hire such persons to obtain or create protected health information for them, only if covered entities obtain specified satisfactory assurances from the business associate that it will appropriately handle the information. These assurances may be in writing, and under certain circumstances such as for government entities, may be implied.

A covered entity may disclose protected health information as necessary to permit the business associate to perform functions and activities for or on behalf of the covered entity. Satisfactory assurances must be obtained if a covered entity's business associate is also a covered entity. The contract must state the purposes for which the business associate may use and disclose protected health information, and must indicate generally the reasons and types of persons to whom the business associate may make further disclosures. For example, attorneys often need to provide information to potential witnesses, opposing counsel, and others in the course of their representation of a client. The business associate contract pursuant to which protected health information is provided to its attorney may include a general statement permitting the attorney to disclose protected health information to these types of people, within the scope of its representation of the covered entity.

A business associate will need to consider the purpose for which protected health information is being disclosed in determining whether the recipient must be bound to the restrictions and conditions of the business associate contract. When the disclosure is a delegation of a function, activity or service that the business associate has agreed to perform for a covered entity, the recipient who undertakes such a function steps into the shoes of the business associate and must be bound to the restrictions and conditions. When the disclosure is to a third party who is not performing business associate functions, activities or services for on behalf of the covered entity, but is the type of disclosure that the covered entity itself could make without giving rise to a business associate relationship, the business associate is not required to ensure that the restrictions or conditions of the business associate contract are maintained. For example, if a business associate acts as the billing agent of a health care provider, and discloses protected health information on behalf of the hospital to health plans, the business associate has no responsibility with respect to further uses or disclosures by the health plan.

These rules do not attempt to directly regulate business associates, however, but pursuant to the authority to regulate covered entities restrictions are imposed on the flow of information from covered entities to non-covered entities. Regardless, a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses. In the event the business associate is found to be in violation of these rules, if the covered entity is unable to cure a material breach of the business associate's obligation under the contract, it is expected to terminate the contract, when feasible.

The rules make special provisions for government agencies that by law cannot enter into contracts with one another or that operate under other legal requirements incompatible with some aspects of the required contractual satisfactory assurances. As provided under Section 164.504(c)(3) several methods other than a business associate contract will satisfy the requirement for satisfactory assurances under this section. First, when a government agency is a business associate of another government agency that is a covered entity, a memorandum of understanding between the agencies is sufficient to constitute satisfactory assurance for the purposes of this rule, if the memorandum accomplishes each of the objectives of the business associate contract. Where the covered entity is a government agency, the satisfactory assurances requirement is satisfied if other law contains requirements applicable to the business associate that accomplish each of the objectives of the business associate contract. Finally, there may be some circumstances where the relationship between covered entities and business associates is otherwise mandated by law.

The final rules substantially expand the exception for disclosure of protected health information for treatment. Rather than allowing disclosures without business associate assurances only for the purpose of consultation or referral, in the final rule covered entities may make any disclosure of protected health information for treatment purposes to a health care provider without a business associate arrangement. This provision includes all activities that fall under the definition of treatment.

The rules also create an exception for data aggregation in order to permit a business association to combine or aggregate protected health information received in its capacity as a business associate of different covered entities when it is performing this service.. This is an exception from the general requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity.

The rules do not require a business associate contract for a group health plan to make disclosures to the plan sponsor, to the extent that the health plan meets the applicable requirements of § 164.504(f). Further, for public programs such as the State Children's Insurance Program (SCHIP) and Medicaid, where eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or where the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and the joint activities are authorized by law, no business associate contract is required with respect to the collection and sharing of individually identifiable health information for the performance of the authorized functions by the health plan and the agency other than the agency administering the health plan.

The rules do not consider a financial institution to be acting on behalf of a covered entity, and therefore no business associate contract is required, when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care. A typical

consumer-conducted payment transaction is when a consumer pays for health care or health insurance premiums using a check or credit card. In these cases, the identity of the consumer is always included and some health information (e.g., diagnosis or procedure) may be implied through the name of the health care provider or health plan being paid. However, covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements described in the preamble to § 164.514.

Covered entities under HIPAA include health care clearinghouses, health care providers and health plans. Specifically included in the definition of "health plan" are group health plans (as defined in section 2791(a) of the Public Health Service Act) with 50 or more participants or those of any size that are administered by an entity other than the employer who established and maintains the plan. These group health plans may be fully insured or self-insured. Neither employers nor other group health plan sponsors are defined as covered entities. However, employers and other plan sponsors - particularly those sponsors with self-insured group health plans - may perform certain functions that are integrally related to or similar to the functions of group health plans and, in carrying out these functions, often require access to individual health information held by the group health plan. Under Employee Retirement Income Security Act of 1974 (ERISA), a group health plan must be a separate legal entity from its plan sponsor. ERISA requires the group health plan to identify a "named fiduciary," a person responsible for ensuring that the plan is operated and administered properly and with ultimate legal responsibility for the plan. If the plan documents under which the group health plan was established and is maintained permit, the named fiduciary may delegate certain responsibilities to trustees and may hire advisors to assist it in carrying out its functions. While generally the named fiduciary is an individual, it may be another entity. The plan sponsor or employees of the plan sponsor are often the named fiduciaries.

These rules also recognize plan sponsors' legitimate need for health information in certain situations while, at the same time, protecting health information from being used for employment-related functions or for other functions related to other employee benefit plans or other benefits provided by the plan sponsor. The rules do not attempt to directly regulate employers or other plan sponsors, but they do place restrictions on the flow of information from covered entities to non-covered entities.

The final rule permits group health plans, and allows them to authorize health insurance issuers or HMOs with respect to the group health plan, to disclose protected health information to plan sponsors if the plan sponsors voluntarily agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for plan administration functions performed on behalf of the group health plan which are specified in plan documents. The group health plan is not required to have a business associate contract with the plan sponsor to disclose the protected health information or allow the plan sponsor to create protected health information on its behalf, if the conditions of § 164.504(e) are met.

In order for the group health plan to disclose protected health information to a plan sponsor, the plan documents under which the plan was established and is maintained must be amended to: (1) describe the permitted uses and disclosures of protected health information; (2) specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of protected health information; and (3) provide adequate firewalls to: identify the employees or classes of employees who will have access to protected health information; restrict access solely to the employees identified and only for the functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance. Any employee of the plan sponsor who receives protected health information for payment, health care operations or other matters related to the group health plan must be identified in the plan documents either by name or function. Any disclosure to employees or classes of employees not identified in the plan documents is not a permissible disclosure. To the extent a group health plan does have its own employees separate from the plan sponsor's employees, as the workforce of a covered entity (i.e. the group health plan), they also are bound by the permitted uses and disclosures of this rule.

The certification that must be given to the group health plan must state that the plan sponsor agrees to: (1) not use or further disclose protected health information other than as permitted or required by the plan documents or as required by law; (2) ensure that any subcontractors or agents to whom the plan sponsor provides protected health information agree to the same restrictions; (3) not use or disclose the protected health information for employment-related actions; (4) report to the group health plan any use or disclosure that is inconsistent with the plan documents or this regulation; (5) make the protected health information accessible to individuals; (6) allow individuals to amend their information; (7) provide an accounting of its disclosures; (8) make its practices available to the Secretary for determining compliance; (9) return and destroy all protected health information when no longer needed, if feasible; and (10) ensure that the firewalls have been established.

A covered entity may as a single legal entity, affiliated entity, or other arrangement combine the functions or operations of health care providers, health plans and health care clearinghouses (for example, integrated health plans and health care delivery systems may function as both health plans and health care providers). The rule permits such covered entities to use or disclose the protected health information of its patients or members for all covered entity functions, consistent with the other requirements of this rule. The health care component must meet the requirements of this rule that apply to a particular type of covered entity when it is functioning as that entity; e.g., when a health care component is operating as a health care provider it must meet the requirements of this rule applicable to a health care provider. However, such covered entities may not use or disclose the protected health information of an individual who is not involved in a particular covered entity function for that function, and such information must be segregated from any joint information systems. For example, an HMO may integrate data about health plan members and clinic services to members, but a health care system may not share information about a patient in its hospital with its health plan if the patient is not a member of the health plan.

Sections 164.506, 164.508 and 164.532
Requirements For Patient Consents And Authorizations

These sections - requirements for consent, requirements for authorization and requirements for interim activities prior to the effective date of the regulations – should put to rest once and for all the idea that HIPAA privacy requirements will result in "Administrative Simplification".

The proposed rules prohibited covered entities from requiring individuals to sign authorizations for uses and disclosures of protected health information for treatment, payment, and health care operations, unless required by other applicable law. The final rule now includes specific requirements for authorizations, as well as specific requirements for consent to release protected health information. The requirement for consent and the requirement for authorization are alleged to not overlap, to apply in different circumstances and to differ substantially from one another. We will let the reader be the final judge of this goal.

The regulations state that 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 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. Most persons who obtain a consent will be health care providers; health plans and health care clearinghouses may also seek a consent. 65 Fed. Reg. 82462, 82509 (Dec. 28, 2000) (emphasis added).

However, an "authorization"

> . . . allows use and disclosure of protected health information for purposes *other than* treatment, payment, and health care operations. In order 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. (*Id.*, 82510, 82511) (emphasis added).

Generally speaking, if a consent is not obtained when required, then a covered health care provider may not use or disclose protected health information about the individual for purposes of treating the individual, obtaining payment for health care delivered to the

individual, or for the provider's health care operations. Obviously, this would cripple the health care provider, and thus obtaining a consent as detailed in the rules will become of paramount importance to covered health care providers.

Also, given the crippling results of a covered health care provider not obtaining consent, certain exceptions had to be included. A covered health care provider with an indirect treatment relationship (a consulting physician, for instance) will not have to obtain a consent to use protected health information. Also, protected health information created or received in three treatment situations are exempt from consent requirements – (1) emergency treatment; (2) where the provider is required by law to treat the individual, and (3) where there are substantial barriers to communicating with the individual and, in the exercise of professional judgment, the covered provider clearly infers from the circumstances the individual's consent to receive treatment.

Covered health care providers may condition the provision of treatment on receipt of a proper consent, and health plans may condition an individual's enrollment in the health plan on receipt of such a consent.

In a confusing nod to form over substance, the rules allow the combination of the consent form described in the rules with other legal consent forms, including an informed consent to receive treatment, but do not allow the combination of the consent form described in the rules with the notice of privacy practices that is required under a separate section of the rules. Additionally, other than in the case of research, consent forms may not be combined with authorizations as these are described in the rules and later in this document. Wouldn't it have been administratively simpler to allow one form to suffice for both a notice of privacy practices as well as for consent and authorization? Evidently it would not.

Additionally, if a single consent form is used for various types of consent, the specific consent for use and disclosure of protected health information must be visually and organizationally distinct from the other consents and must be separately signed and dated by the individual.

With all of this fuss over the consent requirements, the rules surprisingly do not contain a model consent to be utilized by covered health care providers. Instead, the rules describe the core elements of an effective consent. The following describes the core elements. The consent must:

1. Inform the individual that protected health information may be used and disclosed by the covered entity to carry out treatment, payment or health care operations;

2. Refer the individual to the covered entities notice about the uses and disclosures of information described in the consent and indicate that the individual has the right to review the notice prior to signing;

3. Inform the individual that they have the right to request restrictions on uses and disclosures of the information, even though the covered entity does not have to abide by the request;

4. Inform the individual that they have the right to revoke the consent in writing;

5. Include the individual's signature and date of the signature.

Conflicts between the terms of the consent document and any other written legal permission to use or disclose protected health information must be resolved by adhering to the more restrictive document. As described below, a covered health care entity may be presented with an authorization from the patient obtained by a third party, which is less restrictive than the consent the same patient has given the covered health care entity. The more restrictive consent language would trump the less restrictive authorization language and not allow the protective health information to be released to the extent it was not covered by the consent. The covered health care entity can resolve the conflict directly with the patient, so long as such a resolution is documented in writing.

Entities that participate in an organized health care arrangement may develop joint consent forms such that the obtaining of consent by one member of the arrangement is deemed to be consent for all members of the arrangement. Hospitals and their clinical laboratories are given as examples of such joint consent uses.

So what about authorizations? The rules seem to make a bright line distinction between consents and authorizations, as described above. Consents are utilized only when the use and disclosure of the protected health information is for treatment, payment, and health care operations. Authorizations are for everything else. Again, the proposed rules were very lenient in this area. No consent or authorization was needed for purposes of treatment, payment, or health care operations. The rules now give examples of areas in which an authorization would be required. These examples are as follows:

1. Marketing;

2. Pre-enrollment underwriting;

3. Employment determinations; and

4. Fundraising.

Psychotherapy notes are handled in a more specific manner, due to their sensitivity. A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes to carry out treatment, payment, or health care operations, but the covered entity must obtain the person's consent for the person who created the psychotherapy notes to use the

notes to carry out treatment and for the covered entity to use or disclose psychotherapy notes for conducting training sessions.

Authorizations may not be combined with consent documents, nor with any other document including any other written legal permission from the individual. Exceptions are created for purposes of clinical research. Also, authorizations may be revoked at any time, so long as the covered entity has taken no action in reliance on the authorization.

The rules generally prohibit covered entities from conditioning treatment and payment on the provision by the individual of an authorization, and from conditioning eligibility for benefits or enrollment in a health plan on obtaining an authorization. Exceptions include underwriting or risk-rating determinations and information necessary to determine payment of a claim, as well as information necessary for fitness-for-duty physical examinations for employers and pre-enrollment physicals for applicants for life insurance coverage.

Just as consents have core elements that must be included, so do authorizations. These core elements are as follows:

1. A description of the information to be disclosed;

2. The name or other specific identification of the person(s) or class of persons, authorized to use or disclosure the protected health information;

3. The name or other specific identification of the person(s) or class of persons to whom the covered entity is authorized to make the use or disclosure;

4. An expiration date or event;

5. State that the individual has the right to revoke an authorization in writing;

6. Inform the individual that when the information is used or disclosed pursuant to the authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by the rule;

7. The individual's signature and date of signature;

8. If signed by a representative, a description of the representative's authority or relationship to the individual;

If a covered entity requests an individual to provide an authorization to the covered entity for the covered entities own uses and disclosures, then the authorization must additionally contain the following elements:

1. Except for clinical trials, a statement that the covered entity may not condition treatment or payment on the individual's authorization;

2. A description of the purpose of the requested use or disclosure;

3. A statement that the individual may inspect or copy the information to be used or disclosed and may refuse to sign the authorization;

4. If the use or disclosure would result in direct or indirect remuneration from a third party, a statement that such remuneration would result;

5. Provide that a copy of the executed authorization is given to the individual.

Finally, medical research that involves the delivery of treatment to participants could potentially result in the requirement for two separate authorizations. One would be an authorization for the use and disclosure of protected health information to be created for the research that involves the treatment of the individual and the other would be for the use of existing protected health information for the research that includes treatment of the individual.

These two sections of the rules, 164.506 and 164.508 are both additionally subject to the transition provisions of section 164.532. The transition provisions essentially allow covered entities to rely on consents and authorizations obtained prior to the effective date of the rules, even if such consents and authorizations do not contain the mandatory elements contained in the rules. However, to the extent a covered entity is required to obtain a consent or an authorization pursuant to the new rules, then it must do so for any protected health information it creates or receives after the date by which the covered entity must comply with the rules. The intent here is to not require every covered entity to go out and make every patient sign a new consent or authorization form at once, simply because the rules became effective. Only if information is received or created after the effective date of the rules will the new consent and authorization provisions be required.

The rules in this section have some elements that are specific to health care providers such as hospitals, clinics and physicians and other elements that our specific to health care insurers and HMOs. While the above discussion covered rules which are generally common to both, the following discussion concerns provisions which are specific to insurance plans and HMOs.

The final rules provide that health care providers may condition treatment, and health care plans may condition enrollment in a health plan, on receipt of the individual's consent for use and disclosure of the protected health information. However, in the case of the health plan, the request for consent ***must be sought in conjunction with the enrollment process.***

Health plans may obtain a consent that would permit the health plan and its business associates to use and disclose protected health information that the health plan and its business associates created or received. According to the commentary in the rule, "[t]hat consent cannot, however, permit another covered entity (an entity that is not a business associate) to disclose protected health information to the health plan or to any other person."

Furthermore, with regard to health plan pre-enrollment underwriting activities, it is noteworthy in the commentary that:

> if an individual applies for new coverage with a health plan in the non-group market and the health plan wants to review protected health information from the individual's covered health care providers before extending an offer of coverage, the individual must first authorize the covered providers to share the information with the health plan. If the individual applies for renewal of existing coverage, however, the health plan would not need to obtain an authorization to review its existing claims records about that individual, because this activity would come within the definition of health care operations and be permissible.

A group health plan and a health insurance issuer that provide benefits with respect to a group health plan in certain circumstances may disclose summary health information to a plan sponsor for the purpose of obtaining premium bids. This activity qualifies as a health care operation activity, an activity that is exempt from the authorization requirement.

The rule specifically provides that a covered entity, with certain exceptions, may not condition eligibility for benefits or enrollment in a health plan on an individual's willingness to provide an authorization. Health plans, on the other hand, are permitted to condition eligibility for benefits and enrollment in the health plan on receipt of an authorization. Health plans also are permitted to condition payment of specified benefit claims (excluding any psychotherapy treatment claims) upon receipt of an individual's authorization for the health plan to obtain from another covered entity protected health information. The limitation on this provision is that the information must be necessary to determine payment of the claim.

In addition, when a covered entity provides treatment for the sole purpose of providing information to a third party, the treatment may be conditioned upon receipt of an authorization to use and disclose the protected health information related to that treatment. An example of this situation arises when a covered health provider contracts with a life

insurer to conduct medical examinations of the insurer's applicants. In these situations, the examining provider may require the applicants to authorize the release of the results of the physical examination to the life insurer. Absent receipt of such authorization, the provider may refuse to undertake the examination.

Section 164.510: Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object

In general, all covered entities must obtain an individual's verbal "agreement" before using or disclosing protected health information for facility directories, to persons assisting in the individual's care, and for other purposed described in this §164.510. To disclose or use protected health information in such manner, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure. Verbal agreements are appropriate in these types of circumstances and are intended to accommodate situations where it is neither appropriate to remove from the individual the ability to control the protected health information nor appropriate to require formal, written permission to share such information. In exceptional circumstances, where even this informal discussion cannot practicably take place, covered entities are permitted to make decisions regarding disclosure or use based on the exercise of professional judgment of what is in the individual's best interest.

A patient may opt-out of inclusion of personal information in a health care facility's directory. Covered health care providers – which in this case are health care facilities – may include patient information in their directory for the general public only if: (1) they inform incoming patients of their policies regarding the directory; (2) they give patients a meaningful opportunity to opt out of the directory listing or to restrict some or all of the uses and disclosures that can be included in the directory; and (3) the patient does not object to being included in the directory. A patient must be allowed, for example, to have his or her name and condition included in the directory while not having his or her religious affiliation included. The facility's notice and the individual's opt-out or restriction may be oral.

Under the final rule, subject to the individual's right to object, or known prior expressed preferences, a covered health care provider may disclose the following information to persons who inquire about the individual by name: (1) the individual's general condition in terms that do not communicate specific medical information about the individual (e.g., fair, critical, stable, etc.); and (2) location in the facility.

The rules also establish provisions for disclosure of directory information to clergy that are slightly different from those, above, which apply for disclosure to the general public. Subject to the individual's right to object or restrict the disclosure, the final rule permits a covered entity to disclose to a member of the clergy: (1) the individual's name; (2) the individual's general condition in terms that do not communicate specific medical information about the individual; (3) the individual's location in the facility; and (4) the individual's religious affiliation. A disclosure of directory information may be made to members of the clergy even if they do not inquire about an individual by name. Individuals are free to

determine whether they want their religious affiliation disclosed to clergy through facility directories.

The rules expand the circumstances under which health care facilities can disclose specified health information to the patient directory without the patient's agreement such as in the case of incapacity and emergency treatment

Section 164.510(b) is intended to allow disclosures directly related to a patient's current condition and should not be construed to allow, for example, disclosure of extensive information about the patient's medical history that is not relevant to the patient's current condition and that could prove embarrassing to the patient. In addition, if a covered entity suspects that an incapacitated patient is a victim of domestic violence and that a person seeking information about the patient may have abused the patient, covered entities should not disclose information to the suspected abuser if there is reason to believe that such a disclosure could cause the patient serious harm. In all of these situations regarding possible disclosures of protected health information about an patient who is not present or is unable to agree to such disclosures due to incapacity or other emergency circumstance, disclosures should be in accordance with the exercise of professional judgment as to the patient's best interest.

Covered entities may disclose to a person involved in the current health care of the individual (such as a family member, other relative, close personal friend, or any other person identified by the individual) protected health information directly related to the person's involvement in the current health care of an individual or payment related to the individual's health care. Such persons involved in care and other contact persons might include, for example: blood relatives; spouses; roommates; boyfriends and girlfriends; domestic partners; neighbors; and colleagues. Inclusion of this list is intended to be illustrative only, and it is not intended to change current practices with respect to: (1) involvement of other persons in individuals' treatment decisions; (2) informal information-sharing among individuals involved in a person's care; or (3) sharing of protected health information to contact persons during a disaster.

Covered entities may use or disclose protected health information to notify or assist in notification of family members, personal representatives, or other persons responsible for an individual's care with respect to an individual's location, condition, or death. These provisions allow, for example, covered entities to notify a patient's adult child that his father has suffered a stroke and to tell the person that the father is in the hospital's intensive care unit.

The rule includes separate provisions for situations in which the individual is present and for when the individual is not present at the time of disclosure. When the individual is present and has the capacity to make his or her own decisions, a covered entity may disclose protected health information only if the covered entity: (1) obtains the individual's agreement to disclose to the third parties involved in their care; (2) provides the individual with an opportunity to object to such disclosure and the individual does not express an objection; or

(3) reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. Situations in which covered providers may infer an individual's agreement to disclose protected health information pursuant to option (3) include, for example, when a patient brings a spouse into the doctor's office when treatment is being discussed, and when a colleague or friend has brought the individual to the emergency room for treatment.

When an individual is not present (for example, when a friend of a patient seeks to pick up the patient's prescription at a pharmacy) or when the opportunity to agree or object to the use or disclosure cannot practicably be provided due to the individual's incapacity or an emergency circumstance, covered entities may, in the exercise of professional judgment, determine whether the disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. For example, this provision allows covered entities to inform relatives or others involved in a patient's care, such as the person who accompanied the individual to the emergency room, that a patient has suffered a heart attack and to provide updates on the patient's progress and prognosis when the patient is incapacitated and unable to make decisions about such disclosures.

Section 164.512: Uses and disclosures for Which Consent and Authorization, or Opportunity to Agree or Object is Not Required

The new § 164.512 includes paragraphs on: uses and disclosures required by law; uses and disclosures for public health activities; disclosures about victims of abuse, neglect, or domestic violence; uses and disclosures for health oversight activities; disclosures for judicial and administrative proceedings; disclosures for law enforcement purposes; uses and disclosures about decedents; uses and disclosures for cadaveric donation of organs, eyes, or tissues; uses and disclosures for research purposes; uses and disclosures to avert a serious threat to health or safety; uses and disclosures for specialized government; and disclosures to comply with workers' compensation laws.

This section permits covered entities to comply with laws requiring the use or disclosure of protected health information, provided the use or disclosure meets and is limited to the relevant requirements of such other laws.

This rule does not affect what is required by other law, nor does it compel a covered entity to make a use or disclosure of protected health information required by the legal demands or reporting requirements listed in the definition of "required by law." Covered entities will not be sanctioned under this rule for responding in good faith to such legal process and reporting requirements. However, nothing in this rule affects, either by expanding or contracting, a covered entity's right to challenge such process or reporting requirements under other laws. The only disclosures of protected health information compelled by this rule are disclosures to an individual (or the personal representative of an individual) or to the Secretary for the purposes of enforcing this rule. However, uses and

disclosures permitted under this rule must be limited to the protected health information necessary to meet the requirements of the law that compels the use or disclosure.

Covered entities may disclose protected health information without individual authorization to a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability and to disclose protected health information not only to U.S. public health authorities but also, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

Covered entities may disclose protected health information to a person subject to the FDA's jurisdiction, for the following activities: to report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems, or biological product deviations, if the disclosure is made to the person required or directed to report such information to the FDA; to track products if the disclosure is made to a person required or directed by the FDA to track the product; to enable product recalls, repairs, or replacement, including locating and notifying individuals who have received products regarding product recalls, withdrawals, or other problems; or to conduct post-marketing surveillance to comply with requirements or at the direction of the FDA.

Covered entities may disclose protected health information to employers for inclusion in a workplace surveillance database only: with individual authorization; if the disclosure is required by law; if the disclosure meets the requirements of § 164.512(b)(v); or if the disclosure meets the conditions of another provision of this regulation, such as § 154.512(i) relating to research. Similarly, if a pharmaceutical company seeks to create a registry containing protected health information about individuals who had taken a drug that the pharmaceutical company had developed, covered entities may disclose protected health information without authorization to the pharmaceutical company pursuant to FDA requirements or direction. If the pharmaceutical company's registry is not for any of these purposes, covered entities may disclose protected health information to it only with patient authorization, if required by law, or if disclosure meets the conditions of another provision of this rule.

Covered entities may disclose protected health information to such individuals when the covered entity or public health authority is authorized by law to notify these individuals as necessary in the conduct of a public health intervention or investigation. A covered entity that is acting as a public health authority – for example, a public hospital conducting infectious disease surveillance in its role as an arm of the public health department – may use protected health information in all cases for which it is allowed to disclose such information for public health activities as described above.

The final rule includes a new paragraph, § 164.512(c), allows covered entities to report protected health information to specified authorities in abuse situations other than those involving child abuse and neglect. Disclosures of protected health information related

to child abuse continues to be addressed in the paragraph allowing disclosure for public health activities as described, above. State laws continue to apply with respect to child abuse.

The rule specifies three circumstances in which disclosures of protected health information is allowed in order to report abuse, neglect or domestic violence. First, it allows disclosure of protected health information related to abuse if required by law and the disclosure complies with and is limited to the relevant requirements of such law. Second, it allows covered entities to disclose protected health information related to abuse if the individual has agrees to such disclosure. Third, the rule allows covered entities to disclose protected health information about an individual without the individual's agreement if the disclosure is expressly authorized by statute or regulation and either: (1) the covered entity, in the exercise of its professional judgment, believes that the disclosure is necessary to prevent serious harm to the individual or to other potential victims; or (2) if the individual is unable to agree due to incapacity, a law enforcement or other public official authorized to received the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual, and that an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Those individual affected by the disclosure shall be so notified, verbally. However, the rule provides two exceptions to the requirement to inform the victim about a report to a government authority. First, a covered entity need not inform the victim if the covered entity, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm. Second, a covered entity may choose not to meet the requirement for informing the victim, if the covered entity actually would be informing a personal representative (such as a parent of a minor) and the covered entity reasonably believes that such person is responsible for the abuse, neglect, or other injury that has already occurred and that informing that person would not be in the individual's best interests.

This rule permits covered entities to disclose protected health information to health oversight agencies for oversight activities authorized by law, including audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight..

Covered entities may disclose protected health information pursuant to this provision in compliance with and as limited by the relevant requirements of legal process or other law. The rules permit such disclosures pursuant to a warrant, subpoena, or other order issued by a judicial officer that documented a finding by the officer.

The rule expands the circumstances under which limited information about suspects, fugitives, material witnesses, and missing persons may be disclosed, to include not only cases in which law enforcement officials are seeking to identify such individuals, but also cases in which law enforcement officials are seeking to locate such individuals.

The final rule modifies the conditions under which covered entities can disclose protected health information about victims. In addition, as discussed above, the final rule includes a new § 164.512(c), which establishes conditions for disclosure of protected health information about victims of abuse, neglect or domestic violence. The final rule requires covered entities to obtain individual agreement as a condition of disclosing the protected health information about victims to law enforcement, unless the disclosure is permitted under § 164.512(b) or (c) or § 164.512(f)(1). The required agreement may be obtained orally, and does not need to meet the requirements of § 164.508 of this rule (regarding authorizations). The rule waives the requirement for individual agreement if the victim is unable to agree due to incapacity or other emergency circumstance and: (1) the law enforcement official represents that the protected health information is needed to determine whether a violation of law by a person other than the victim has occurred and the information is not intended to be used against the victim; (2) the law enforcement official represents that immediate law enforcement activity that depends on such disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (3) the covered entity, in the exercise of professional judgment, determines that the disclosure is in the individual's best interests.

The rule permits covered entities to disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death if the covered entity has a suspicion that such death may have resulted from criminal conduct. In such circumstances consent of the individual is not available and it may be difficult to determine the identity of a personal representative and gain consent for disclosure of protected health information.

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, is permitted to disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to (1) the commission and nature of a crime, (2) the location of such crime or of the victim(s) of such crime, and (3) the identity, description, and location of the perpetrator of such crime. A disclosure is not permitted under this section if health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care. In such cases, disclosures to law enforcement would be governed by paragraph (c) of this section.

Covered entities are further permitted to disclose protected health information to coroners, medical examiners, and funeral directors as part of a new paragraph on disclosures related to death.

This rules also allow covered entities to disclose protected health information without individual authorization to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for donation and transplantation. This provision is intended to address situations in which an individual has not previously indicated whether he or she seeks to donate organs, eyes, or tissues (and

therefore authorized release of protected health information for this purpose). In such situations, this provision is intended to allow covered entities to initiate contact with organ and tissue donation and transplantation organizations to facilitate transplantation of cadaveric organs, eyes, and tissues.

The rules permits uses and disclosures of protected health information for research purposes under specified terms and conditions. These include:

1. Documentation must indicate that the privacy board has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests.

2. The final rule continues to permit the documentation of IRB or privacy board approval of a waiver of an authorization as required by § 164.508, to indicate that only some or all of the § 164.508 authorization requirements have been waived. In addition, the final rule clarifies that the documentation of IRB or privacy board approval may indicate that the authorization requirements have been altered.

3. The final rule requires that the covered entity obtain written agreement from the person or entity receiving protected health information under § 164.512(i) not to re-use or disclose protected health information to any other person or entity, except: (1) as required by law, (2) for authorized oversight of the research project, or (3) for other research for which the use or disclosure of protected health information would be permitted by this subpart.

4. The rule broadens the types of individuals who are permitted to sign the required documentation of IRB or privacy board approval.

5. The final rule permits the use and disclosure of protected health information for research without requiring authorization or documentation of the alteration or waiver of authorization, if the research is conducted in such a manner that only de-identified protected health information is recorded by the researchers and the protected health information is not removed from the premises of the covered entity.

6. With respect to research involving deceased individuals, the rule retains the exception for uses and disclosures for research purposes but in addition require that the covered entity take certain protective measures prior to release of the decedent's protected health information for such purposes. requires that the covered entity obtain representation that the use or disclosure is sought solely for research

on the protected health information of decedent, and representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. In addition, the final rule allows covered entities to request from the researcher documentation of the death of the individuals about whom protected health information is being sought.

7. In addition, when using or disclosing protected health information for reviews preparatory to research (§ 164.512(i)(1)(ii)) or for research solely on the protected health information of decedents (§ 164.512)(1)(iii)), the final rule clarifies that the covered entity may rely on the requesting researcher's representation that the purpose of the request is for one of these two purpose, and that the request meets the minimum necessary requirements of § 164.514. Therefore, the covered entity has not violated the rule if the requesting researcher misrepresents his or her intended use of the protected health information to the covered entity.

8. To the extent that a researcher provided treatment to persons as part of a research study, such researchers are to be treated as health care providers for purposes of that treatment, and the researcher must comply with all of the provisions of the rule that would be applicable to health care providers.

Covered entities are allowed to use or disclose protected health information without individual authorization – consistent with applicable law and ethics standards – based on a reasonable belief that use or disclosure of the protected health information was necessary to prevent or lessen a serious and imminent threat to health or safety of an individual or of the public. The final rule allows covered entities to use or disclose protected health information without an authorization on their own initiative in these circumstances, when necessary to prevent or lessen a serious and imminent threat, consistent with other applicable ethical or legal standards.

The rules permit, but do not require, covered entities to use or disclose protected health information, consistent with applicable law and standards of ethical conduct, in specific situations in which the covered entity, in good faith, believes the use or disclosure is necessary to permit law enforcement authorities to identify or apprehend an individual. Under paragraph (j)(1)(ii)(A) of this section, a covered entity may take such action because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have resulted in serious physical harm to the victim. The protected health information that is disclosed in this case is limited to the statement and to the protected health information included under the limited identifying and location information in § 164.512(f)(2), such as name, address, and type of injury. Under paragraph (j)(1)(ii)(B) of this section, a covered entity may take such action where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful

custody. A disclosure may not be made under paragraph (j)(1)(ii)(A) for a statement admitting participation in a violent crime if the covered entity learns the information in the course of counseling or therapy. Similarly, such a disclosure is not permitted if the covered entity learns the information in the course of treatment to affect the propensity to commit the violent crimes that are described in the individual's statements.

Certain government functions are subject to specific rules.

1. For full time military personnel, use and disclose of protected health information is permitted for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority had published by notice in the *Federal Register*. Under the final rule, foreign military personnel are not excluded from the definition of "individual." Covered entities will be able to use and disclose protected health information of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for U.S. Armed Forces personnel under the notice to be published in the *Federal Register*. Foreign military personnel do have the same rights of access, notice, right to request privacy protection, copying, amendment, and accounting as do other individuals pursuant to §§ 164.520-164.526 (sections on access, notice, right to request privacy protection for protected health information, amendment, inspection, copying) of the rule.

2. A covered entity that is a component of DOD or the Department of Transportation may disclose to DVA the protected health information of an Armed Forces member upon separation or discharge from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

3. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to other components of the Department that determine eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs.

4. The final rule does not except intelligence community employees and their dependents from the general rule requiring an authorization in order for protected health information to be used and disclosed.

5. The rule allows a covered entity to disclose protected health information to an authorized federal official for the conduct of lawful

intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority (e.g., Executive Order 1233). The rule further states that a covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons as authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons as authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

6. The final rule creates a narrower exemption for Department of State for uses and disclosures of protected health information (1) for purposes of a required security clearance conducted pursuant to Executive Orders 10450 and 12698; (2) as necessary to meet the requirements of determining worldwide availability or availability for mandatory service abroad under Sections 101(a)(4) and 504 of the Foreign Service Act; and (3) for a family member to accompany a Foreign Service Officer abroad, consistent with Section 101(b)(5) and 904 of the Foreign Service Act.

7. The rules permit covered entities to disclose protected health information about these individuals if the correctional institution or law enforcement official represents that the protected health information is necessary for these purposes.

Under HIPAA, workers' compensation and certain other forms of insurance (such as automobile or disability insurance) are "excepted benefits." Insurance carriers that provide this coverage are not covered entities even though they provide coverage for health care services. To carry out their insurance functions, these non-covered insurers typically seek individually identifiable health information from covered health care providers and group health plans. The final rules clarify the ability of covered entities to disclose protected health information without authorization to comply with workers' compensation and similar programs established by law that provide benefits for work-related illnesses or injuries without regard to fault. A covered entity may disclose protected health information regarding an individual to a party responsible for payment of workers' compensation benefits to the individual, and to an agency responsible for administering and /or adjudicating the individual's claim for workers' compensation benefits.

Section 164.514: Other Requirements Relating To Uses And Disclosures Of Protected Health Information

This section addresses a variety of situations for the appropriate request and release of personally identifiable health information. Preliminarily, § 164.514 defines the protected data to be sufficiently specific so as to either actually identify one single individual or to at lease provide a covered entity with a reasonable basis to believe the information can be used

to distinguish a particular person. A covered entity may determine that health information is not individually identifiable health information only in one of two ways:

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information;

2. A covered entity may use a "safe harbor" approach to demonstrate compliance with the standard. Under this approach, a covered entity is considered to have met the standard if it has removed all of a list of enumerated identifiers (as specified under the rule), and if the covered entity has no actual knowledge that the information could be used alone or in combination to identify a subject of the information.

As for re-identifying records, covered entities may use codes and similar means of marking records so that they may be linked or later re-identified, if the code does not contain information about the subject of the information (*e.g.*, the code cannot be a derivation of a person's social security number), and as long as the covered entity does not use or disclose the code for any other purpose. The covered entity is prohibited from disclosing the mechanism for re-identification, such as tables, algorithms, or other tools that could be used to link the code with the subject of the information.

The Final Rule also imposes a *"minimum necessary"* standard which covers the amount of protected health information which may be disclosed by covered entities. This was substantially modified from the proposed requirements. The rules impose differing standards on the *"minimum necessary"* requirement depending on who is requesting the information and for what purpose. The following are examples:

1. **Routine disclosures:** For any type of disclosure that is made on routine, recurring basis, a covered entity must implement policies and procedures that permit only the disclosure of the minimum protected health information necessary to achieve the purpose of the disclosure -- individual review of each disclosure is not required.

2. **Non-routine disclosures:** For non-routine disclosures, reasonable criteria for determining and limiting disclosure to only the minimum amount of protected health information necessary to accomplish the purpose is required. Covered entities must establish and implement procedures for reviewing these non-routine requests for disclosures on an individual basis in accordance with these criteria.

3. **Requests for protected health information from other covered entities:** When handling requests for protected health information from other covered entities made on a routine, recurring basis, the requesting covered entities' policies and procedures may establish standard protocols describing what information is reasonably necessary for the purposes and limiting their requests to only that information, in lieu of making this determination individually for each request. For all other requests, the policies and procedures must provide for review of the requests on an individualized basis. As the commentary indicates ***"A request for the entire medical record, absent such documented justification is a presumptive violation of this rule."***

4. **Reasonable reliance:** A covered entity may reasonably rely on the assertion of a requesting covered entity that it is requesting the minimum protected health information necessary for the stated purpose.

5. **Uses and disclosures for research:** In making a "minimum necessary" determination, a covered entity may reasonably rely on documentation from an appropriate requestor seeking the information for research purposes.

6. **Standards for electronic transmissions:** Covered entities are not required to apply the "minimum necessary" standard to the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions in the Transactions Rule.

Use of protected health information for marketing purposes is also covered by this section. Essentially, covered entities ***must obtain the individual's authorization before making uses or disclosures*** of protected health information for marketing. However, under the Final Rule, certain activities are not prohibited. A covered entity ***is not required to obtain an authorization*** to make a marketing communication to an individual that: (1) Occurs in a face-to-face encounter with the individual; (2) concerns products or services of nominal value; or (3) concerns the health-related products or services of the covered entity or of a third-party and the communication identifies the covered entity as the party making the communication. To the extent the covered entity receives direct or indirect remuneration from a third-party for making the communication, covered entity must state that fact except in the case of a general communication, such as a newsletter, which meets the requirements of the rule.

For purposes of fundraising on behalf of itself, a covered entity may use protected health information without individual authorization provided that it limits the information that it uses to demographic information about the individual and dates that it has provided service to the individual. Furthermore, ***fundraising materials must explain how the individual may opt-out*** of any further fundraising communications, and covered entities are required to honor such requests. A covered entity is permitted to disclose the limited health information to a business associate for fundraising on its own behalf. Finally, a covered

entity may disclose the information to a "institutionally related foundation" (as defined under section 501(c)(3) of the Internal Revenue Code).

Protected health information may be used or disclosed for underwriting and other activities related to the creation, renewal, or replacement of a contract of health insurance, or health benefits. Health plans receiving such information for these purposes may not use or disclose it for any other purpose, except as required by law, if the insurance or benefits contract is not place with the health plan.

Prior to any disclosure of protected health information under this rule, a covered entity ***must verify the identity and authority to access*** of the person requesting the protected health information, and documentation of the conditions of disclosure (*e.g.*, pursuant to an administrative subpoena). The covered entity must establish and use written policies and protocols, which may be standard, that are reasonably designed to verify the identify and authority of the requestor.

Section 164.520: Notice Of Privacy Practices For Protected Health Information

An individual has the right to adequate notice of the uses and disclosures of protected health information that may be made by a covered entity, and of the individual's rights, and the covered entity's duties, with respect to this information. Unlike the proposed Rule, no "model" notice is included in the Final Rule. DHHS intends to develop further guidance on notice requirements prior to the compliance date of the rule. However, the rule provides basic guidelines for drafting such notices. Those guidelines are:

1. A covered entity must provide a notice that is written in plain language.

2. Contains a header notice that states: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."**

3. Must contain a description of the types of uses that the covered entity is permitted to make for the purposes of treatment, payment and health care operations.

4. Must contain a description of the types of uses that the covered entity is permitted to make without an individual's written consent or authorization.

5. For each purpose described above, the description must describe the uses or disclosures that are prohibited by law, or are permitted by law.

6. If the covered entity intends to engage in the certain activities (*e.g.*, provide appointment reminders, information about treatment alternatives, contact the individual for the purpose of raising funds, disclose protected to health

information to the sponsor of a group health plan), the covered entity must fully describe these activities in the notice.

7. The notice must contain a statement of the individual's rights with respect to protected health information, along with a brief description of how the individual may exercise those rights.

8. Covered entities must state in their notice that they are required by law to maintain the privacy of protected health information, provide notice of their legal duties and privacy practices, and abide by the notice terms currently in effect. A covered entity must also provide a statement as to how it will notify individuals of decisions to change privacy practices.

9. Notices must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated. A description of how to file a complaint, along with a statement that the individual will not be retaliated against, is also required.

10. The notice must contain the name or title, and telephone number of the person to call for more information.

11. The notice must contain the date on which the notice is first in effect.

12. Additional optional elements are also covered under the rule.

All covered entities that are required to produce a notice, must produce the notice upon request of any person. The person does not have to be a current patient or enrollee. In its commentary, DHHS states that it intends the notice to be a public document that people can use in choosing between covered entities.

Health plans must provide the notice to all health plan enrollees (including participants and beneficiaries) as of the compliance date. After the compliance date, health plans must provide the notice to all new enrollees at the time of enrollment and to all enrollees within 60 days of a material revision to the notice.

Distribution requirements for the notice differ according to whether the covered health care provider has a direct, versus an indirect treatment relationship with an individual. ***Covered providers that have a direct relationship*** with individuals ***must provide notice to individuals as of the first delivery of service*** after the compliance date. This requirement applies whether the first service is delivered electronically or in person. Covered providers that maintain a physical service delivery site must prominently post the notice where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. ***Covered providers that have an indirect relationship with individuals are only required to produce the notice upon request.***

Legally separate covered entities may participate in an organized health care arrangement to comply with the notice requirements by producing a single notice that describes their combined privacy practices. Such joint notice must meet the implementation specifications required under the rule except that it may be altered to reflect that the notice covers more than one covered entity.

Covered entities ***must retain copies*** of the notice(s) that they issue in accordance with the administration requirements set out in § 164.530(j) of this rule.

This section also covers the general right of an individual to request that uses and disclosures of protected health information be restricted and the requirement for covered entities to adhere to restrictions to which they have agreed. ***A covered entity must document a restriction to which it has agreed.*** No specific form of documentation is required. Documentation must be retained for six years after the date it was created, or the date it was last in effect, whichever is later. However, ***a covered entity is not required to agree to the restriction.*** If a covered entity has agreed previously to the restriction, it may terminate its agreement to a restriction, if:

1. The individual agrees to the termination in writing.

2. The individual orally agrees to the termination and the oral agreement is documented. A note in the medical records or similar notation is sufficient.

3. The covered entity informs the individual that it is terminating its agreement to a restriction, except that it is only effective with respect to protected health information created or received after the individual has been notified.

This section also covers requests from individuals for their own private health information and how to deliver the information to the person. Covered entities ***must permit*** individuals to request that the covered entity provide confidential communications of protected health information about the individual and the they ***must accommodate*** reasonable requests by individuals to receive communications of protected health information from the covered entity by alternative means or at alternative locations. For instance, an individual that does not want a family member to know about a certain treatment may request that the provider communicate with the individual at the individual's place of work rather than at their residence.

The same general rule also applies to health insurance plans, however, health plans must accommodate reasonable requests if the individual clearly states that the disclosure of all or part of the protected health information could endanger the individual. In its commentary, DHHS gives the following example: "If an individual requests that a health plan send explanations of benefits about particular services to the individual's work rather than home address because the individual is concerned that a member of the individual's

household might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the request.

The reasonableness of a request made under this paragraph must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request and as otherwise provided under this section of the rule. ***A health care provider cannot require the individual to provide a reason*** for the request as a condition of accommodating the request. In fact, if an individual indicates that a disclosure could endanger the individual, they cannot further consider the individual's reason for making the request in determining whether or not it must accommodate the request.

Section 164.522: Rights To Request Privacy Protection For Protected Health Information.

Under Section 164.522(a) an individual is provided the right to request restriction of uses and disclosures of "private health information" as defined in Act. This permits an individual to request the restriction of "(A) uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and (B) disclosures under Section 164.510(b)." Once a covered entity agrees to such a restriction, it may not use or disclose such protected health information in violation of the restriction unless the requesting individual requires emergency treatment and such restricted private health information is necessary to provide such treatment. In such event, the covered entity "may use the restricted private health information or may disclose such information to a healthcare provider, to provide such treatment to the individual."

Notwithstanding the foregoing, a covered entity is not absolutely required to agree to a restriction. Essentially, a covered entity may refuse to restrict uses and disclosures, or restrict agreement to only certain aspects of an individual's request, if the covered entity is concerned for the quality of patient care in the future. Under the examples provided in the comments, such refusal to restrict can occur where (1) the covered entity believes the restriction is not in the patient's best medical interest, or (2) where the covered entity is concerned about implications on future treatment it can agree to use and disclose sensitive private health information for treatment purposes only, and agree not to disclose information for payment and operation purposes. Accordingly, covered entities are encouraged to discuss with individuals information that may be used or disclosed in emergencies.

In the event restricted private health information is disclosed to a healthcare provider for emergency treatment under Section 164.522(a)(1)(iii), the covered entity ***must*** request that the healthcare provider "not further use or disclose the information." Notwithstanding the foregoing, any restriction agreed to by a covered entity under Section 164.522(a) is not effective to prevent uses or disclosures permitted or required under Sections 164.502(a)(2)(i), 164.510(a) or 164.512.

Section 164.522(a) permits a covered entity to terminate its agreement to a restriction if (i) the requesting individual agrees to or requests the termination in writing; (ii) the

requesting individual orally agrees to termination as supported by documentation of the oral agreement; or (iii) the covered entity informs the requesting individual that its terminating its agreement to restrict the private health information, ***except*** such termination is only effective regarding private health information created or received after the covered entity has so informed the individual. Should a covered entity agree to a restriction, such entity must document the restriction in accordance with Section 164.530(j).

Under Section 164.522(b), a covered healthcare provider ***must permit*** individuals to request and ***must accommodate reasonable requests*** by individuals, to receive communications of private health information from the covered healthcare provider by alternative means or at alternative locations. In addition, a health plan ***must permit*** individuals to request, and ***must accommodate reasonable requests*** by individuals, to receive private health information communications from the health plan by alternative means or at alternative locations if ***"the individual clearly states that the disclosure or all or part of that information could endanger the individual."*** Essentially, this provision gives individuals the right to request that they receive communications from covered entities at an alternative address by an alternative means, regardless of the nature of the private health information involved. Such covered healthcare providers must accommodate reasonable requests and cannot require the individual to explain the basis for the request as a condition of accommodating same. Health plans, however, may require an individual to make a statement that disclosure of the private health information could endanger the individual, and health plans may condition accommodation on receipt of such statement. However, a covered entity may require the individual to request such confidential communication described in Section 164.522(b)(1) in writing. In addition, the covered entity may condition such provision of a reasonable accommodation on: "(A) when appropriate, information as to how payment, if any, will be handled; (B) specification of an alternative address or other method of contact."

Section 164.524 sets forth the standards and requirements for access of individuals to their private health information. An individual has a right of access to inspect, obtain a copy of their private health information in a designated record as long as such private health information is maintained in such designated record set, except for "(i) psycho therapy notes; (ii) information compiled in a reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; (iii) [private health information] maintained by a covered entity that is (a) subject to the clinical laboratory improvements amendments of 1988, 42 U.S.C. Section 263(a) to the extent the provision of access to the individual would be prohibited by law; or (b) exempt from the clinical laboratory improvements amendments of 1988, pursuant to 42 CFR Section 493.3(a)(2)."

Under Section 164.524, individual access without an opportunity to review ("unreviewable grounds for denial") are provided. Under certain circumstances, a covered entity may deny an individual access to their private health information without an opportunity to review if: (i) it is excepted from the right of access under Section 164.522(a)(1); (ii) the covered entity is a correctional institution or a covered healthcare provider acting under the direction of a correctional institution, where obtaining private health information by the inmate would jeopardize the health, safety, security, custody, or

rehabilitation of such individual or of other inmates or the safety of any employee or other person at the correctional institution transporting such inmate; (iii) when private health information is created or obtained by a covered healthcare provider in the course of research which includes treatment, access may be temporarily suspended for as long as the research is in progress, provided the individual has consented to such denial of access to participate in the research, and the covered healthcare provider has informed the individual of reinstatement of access upon completion of research; (iv) where access to private health information is contained in records subject to the Privacy Act, 5 U.S.C. Section 552(a), this may be denied under denial of the Privacy Act provided it meets the requirements of that law; and (v) were private health information obtained from someone other than the healthcare provider under promise of confidentiality and access "would be reasonably likely" to reveal the source of the information.

Unlike the aforementioned unreviewable grounds, a covered entity may deny an individual access ***with a right of review*** under the following circumstances: (i) where a licensed healthcare professional has determined in their professional judgment that the requested access is "reasonably likely" to endanger life or physical safety of such individual or another person; (ii) or the private health information references another person (other than a healthcare provider) and a licensed healthcare professional has determined in their professional judgment that the requested access is "reasonably likely" to cause substantial harm to the other person; or (iii) the request for access is made by the individual's personal representative and a licensed healthcare professional has determined and exercised in their professional judgment that such access by the personal representative is "reasonably likely" to cause substantial harm to the individual or another person.

Where a denial of access to private health information is reviewable under 164.524(a)(iii), the requesting individual has the right to have the denial reviewed by a licensed healthcare professional (who did not participate in the original decision to deny) that is designated by the covered entity to act as a reviewing official. The covered entity must comply with the determination of the reviewing official pursuant to Section 164.524(d)(4).

Regarding an individual's request for access, the covered entity must permit an individual to request access to inspect or obtain a copy of that individual's private health information maintained in a designated record set. Such request could be required to be in writing as long as the individual is informed of such requirement. Generally, the covered entity must act on a request for access no later than 30 days after receiving the request. Should the covered entity grant the request in whole or in part, it must inform the individual that the request is accepted and provide access to the private health information subject to the requirements of Section 164.524(c). Should the covered entity deny the request in whole or in part, a written denial must be provided in accordance with Section 164.524(d). In the event the requested private health information is not maintained or accessible to the covered entity on-site, the covered entity must permit access for inspection or copy by no later than 60 days from receipt of the individual's request. In the event the covered entity is unable to grant or deny access within the aforementioned 30-day time period, the covered entity may extend the time for such actions, no more than 30 days, provided that (1) the covered entity provides the

requesting individual with a written statement of the reasons for the delay within the time limit set by the rule, and provides the individual the date with which the request for action will be completed; and (2) no extension of time on such request for access can be granted.

Where the covered entity provides the individual with access to private health information, either in whole or in part, the covered entity must comply with very specific requirements. Essentially, the covered entity must provide the access requested by the individuals (inspection, obtaining a copy, or both) of their private health information and designated record sets if such private health information is maintained in more than one designated record set at more than one location – the covered entity need only produce the private health information once in response to the request. In addition, the covered entity must provide the requesting individual with access to the private health information "in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and individual." Notwithstanding the foregoing, the covered entity may provide the requesting individual with a ***summary*** of the requested private health information ***in lieu of access*** if (1) the individual agrees in advance to a summary or explanation; and (2) the individual agrees in advance to the fees imposed, if any, by such covered entity for such summary or explanation. Moreover, access must be provided to the requesting individual in a timely manner, including arranging for a convenient time and place to inspect or obtain a copy of requesting individual's private health information, or mailing a copy of the private health information pursuant to the individual's request. The covered entity may discuss scope, format and other aspects of the request as necessary to facilitate timely access. Lastly, where an individual requests a copy of private health information or agrees to a summary or explanation of private health information, the covered entity may impose a reasonable cost-based fee, provided that the fee includes only costs of (i) copying the private health information, (ii) postage, if mailed, and (iii) preparing an explanation or summary of the private health information if agreed to between the covered entity and the individual as aforementioned.

Where an individual is denied access to private health information (either in whole or in part), a covered entity must comply with a number of requirements. To the extent possible, the covered entity must give the individual access to any private health information requested, excluding private health information where the covered entity has the grounds to deny access. The covered entity must also provide timely written denial to the individual as set forth in Section 164.524(b)(2), explaining in plain language (1) the basis for the denial, (2) a statement of the individual's review rights under Section 164.524(a)(4), if applicable, including a description of how the individual may exercise their rights, and (3) a description of how the individual may complain to the covered entity pursuant to the complaint procedure set forth in Section 164.530(d) or to the Secretary pursuant to the procedures in Section 160.306. Such description must include name or title and telephone number of the contact person or office designated in Section 164.530(a)(1)(ii). If the covered entity does not maintain the private health information that is the subject of the individual request for access, yet the covered entity knows where such information is maintained, ***the covered entity must inform the individual where to direct the request for access.*** Where the

individual has requested review of a denial under Section 164.524(a)(4), the covered entity must designate the licensed healthcare official not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer the request to review to the designated reviewing official, who must make a determination within a reasonable period of time whether or not to deny access based on the standards set forth in Section 164.524(a)(3). Accordingly, the covered entity must provide written notice to the individual of the designated reviewing official's determination to take other action required by Section 164.524 to carry out such determination.

With respect to documentation, a covered entity must document (1) the designated record set subject to access by individuals, (2) the titles of the persons or offices responsible for receiving and processing individual requests for access.

Section 164.526: Amendment Of Protected Health Information

For as long as private health information is maintained in a covered entity designated record set, an individual has the right to have the covered entity amend private health information or record about such individual in the designated record set. such request may be denied by the covered entity if the covered entity determines that the private health information or record that is subject of the request (i) was not created by the covered entity (unless a reasonable basis is provided by the individual that the originator of the private health information is no longer available to amend the record set), (ii) is not part of the designated record set, (iii) is not available for inspection under section 164.524, or (iv) is accurate and complete.

Generally, a covered entity ***must*** permit an individual's request to amend private health information maintained and designated record set; however, the covered entity may require such request to be in writing, including reasons in support of the amendment, as long as the individuals are informed in advance of such requirements by the covered entity. Once received, the covered entity must act on such individual's amendment request within sixty (60) days. If the covered entity grants the amendment (either in whole or in part), it must take action as set forth in Section 164.526(c)(1), (2). If the covered entity denies the requested amendment (either in whole or in part), it must provide the individual with a written denial as set forth in Section 164.526(d)(1). If the covered entity is unable to act on the amendment within the sixty (60) day time period, such time may be extended an additional thirty (30) days if (1) the covered entity provides the requesting individual with a written statement of the reasons for delay and anticipated date for completing action on the request within the original sixty (60) day period, and (2) only one extension for such action on the amendment is granted.

Once a covered entity accepts an individual's request for amendment (either in whole or in part), the covered entity must comply with specific requirements. First, the covered entity, at a minimum, must identify the records in the designated record set affected by the amendment and append or otherwise provide a link to the location of the amendment. Further, the covered entity must comply with Section 164.526(b) by timely informing the

individual that the amendment is accepted, and obtain the individual's agreement to have the covered entity notify the relevant persons identified by the individual with which the amendment needs to be shared according to Section 164.526(c)(3). Moreover, the covered entity must make reasonable efforts to both inform and provide the amendment within a reasonable time to (i) those persons identified by the individual to receive the private health information and needing the amendment, (ii) persons (including business associates) known by the covered entity to possess private health information that is subject to the amendment who rely (or could foreseeably rely) on such information to the individual's detriment.

Where the covered entity denies the requested amendment (either in whole or in part) the covered entity must also comply with certain requirements. First, the covered entity must provide the requesting individual with a "timely, written denial" as set forth in Section 164.526(b)(2). The denial must contain in plain language, (i) the basis for the denial pursuant to Section 164.526(a)(2), (ii) notice of an individual's right to submit a written statement disagreeing with a denial and how to file same, (iii) where the individual does not submit written statement of disagreement, a statement that the individual may request the covered entity to provide the individual's request for amendment and the resulting denial in future disclosures of private health information that are subject to the amendment, and (iv) a description of how the individual may complain to the covered entity under the complaint procedure set forth in Section 164.530(d) or to the Secretary pursuant to procedures established in Section 160.306. This description must include the name or title, and telephone number, of the contact persons/office designated as set forth in Section 164.530(a)(1)(ii).

The regulations further permit an individual to submit a written statement disagreeing with a covered entity's denial of all or part of the requested amendment, and the basis of such disagreement; however, a covered entity may reasonably limit the length of such statement. In return, the covered entity may prepare a written rebuttal of the individual statement of disagreement, and must provide a copy of such rebuttal to the individual who has submitted the statement. For recordkeeping purposes, the covered entity must appropriately identify the record or private health information in the designated record set that is subject to the disputed amendment, and append or otherwise link (1) the individual's request for amendment, (2) the covered entity's denial of the request, (3) the individual statement of disagreement (if any), and (4) the covered entity's rebuttal (if any) to the designated record set.

Where an individual has submitted a statement of disagreement, the covered entity must include the material appended as set forth in Section 164.526(d)(4) or, at the covered entity's option, an accurate summary of the information, and any subsequent disclosure of private health information related to the substance of the disagreement. Where an individual has not submitted such written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of the information, with any subsequent disclosure of private health information only where the individuals requested such action in accordance with Section 164.526(d)(1)(iii). Where the aforementioned subsequent disclosures are made using a standard transaction under Section 162 that does not permit such additional material to be included in the disclosure, the covered

entity is permitted to separately transmit such material to the recipient of the standard transaction.

Where a covered entity is informed by another covered entity of an amendment of an individual's private health information under section 164.526(c)(3), the covered entity must amend such private health information in the designated record set as set forth in section 164.526(c)(1). The covered entity is also required to document the titles of persons or officers that are responsible for receiving or processing individual requests for amendments and retain such documentation as required by Section 164.530(j).

SECTION 164.528: Accounting Of Disclosures Of Protected Health Information

This section sets forth an individual's right to receive an accounting of disclosures of private health information made by a covered entity in the six (6) years prior to the date on which the accounting is requested. Notwithstanding such right to receive an accounting, such right excepts disclosures: (i) to carry out treatment, payment and health care operations pursuant to Section 164.502, (ii) to individuals of private health information about them as set in Section 164.502, (iii) for the facility's directory or to persons involved with the individual's care or other notification purposes as set forth in Section 164.510, (iv) for national security or intelligence purposes pursuant to Section 164.512(k)(2), (v) to correctional institutions or law enforcement officials as set forth in Section 164.512(k)(5), or (vi) that occurred prior to the compliance date for such covered entity. This right to receive an accounting of disclosures to a health oversight agency or law enforcement official may be temporarily suspended by the covered entity for the time specified by such agency or official if such agency or official provides the covered entity with a written statement that the accounting to the individual would be "reasonably likely to impede the agency's activities," and specifying the time required for such suspension. Where the agency or official statement is made orally, the covered entity must (1) document the statement (including identity of the agency or official making the statement), (2) temporarily suspend the individual's right to accounting of disclosures that are subject to the statement and (3) limit the temporary suspension for up to thirty (30) days from the date of the oral statement unless a written statement under Section 164.528(a)(2)(i) is submitted within such thirty (30) day period. Although an individual's right to receive an accounting of disclosures of private health information may cover up to six (6) years prior to the date on which the account is requested, an individual may request an accounting of disclosures for a lesser period of time.

Any written accounting by a covered entity must meet certain requirements. Unless otherwise provided in Section 164.520(a), the accounting must include disclosures of private health information that occurred in six (6) years, or any shorter time requested by the individual, prior to the date of the request for an accounting, ***"including disclosures to or by business associates of the covered entity."*** Such accounting must include for each disclosure (i) the disclosure date, (ii) the name of the entity or person who received the private health information and, where known, the address of such entity or person, (iii) a brief description of the disclosed private health information, (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis of disclosure, or in lieu of such statement,

(A) a copy of the individual's written authorization pursuant to Section 164.508, or (B) a copy of a written request for disclosure under Sections 164.502(a)(2)(ii) or 164.512, if any. If a covered entity has made multiple disclosures of private health information to the same person or entity were for a single purpose under Sections 164.502(a)(2)(ii) or 164.512 during the period covered by the accounting, or pursuant to a single authorization under Section 164.508, the accounting with respect to such multiple disclosures ***may*** provide (i) the information required in Section 164.528(b)(2) for the first disclosure during accounting, (ii) the frequency, period, or number of disclosures made during such accounting, and (iii) the date of the last disclosure during such accounting period.

Upon an individual's request for an accounting, the covered entity must act within sixty (60) days of receipt of the request as follows: (i) the covered entity ***must provide*** the individual with the requested accounting, or (ii) if the covered entity cannot provide the accounting with the time set forth above, ***the covered entity may extend the time up to thirty (30) days if*** (A) the covered entity provides a written statement of the reasons for the delay and date which the covered entity will provide the accounting, within the initial sixty (60) day period, and (B) the covered entity has only one such extension of time. The covered entity must provide the first accounting to the individual in any twelve (12) month period without charge. Thereafter, a covered entity may impose a "reasonable, cost-based fee" for each subsequent request for accounting by that individual within the twelve (12) month period if the covered entity informs the individual in advance of the fee and provides the individual an opportunity to withdraw or modify the request for a subsequent accounting to avoid or reduce the fee.

Regarding such accountings, a covered entity must document certain information and retain the documentation required by Section 164.530(j). First, such documentation must include information required to be included in an accounting under Section 164.528(b) for disclosures of private health information subject to accounting under Section 164.528(a). In addition, such documentation must include the written accounting provided to the individual under Section 164.528. Finally, the titles of persons or officers responsible for receiving and processing such individual request for accounting must be included within such documentation.

Section 164.530: Chief Privacy Officer and Privacy and Security Plans

Like compliance with fraud and abuse, and billing and collection, covered entities ***are required to have privacy and security plans (Program) and chief privacy officers.*** The biggest difference, though, is that the these are required as a matter of HIPAA law. In the compliance arena, the Office of Inspector General effectively required them by enforcement and guidance issued.

The key to success for any organization will be to create HIPAA Hero culture. In other words, a culture of compliance, a culture of privacy, a culture of respect for the privacy

and protection of protected health information. This could even be considered a culture of respect for each individual patient.

To be effective, the entire organization should be involved in the development, implementation and continuing utilization of the Program. Particularly important are the operations, technology, information systems, billing and collections, medical records, administration, quality improvement, utilization improvement, clinical care, accounting/finance and legal departments. Senior management is critical to the success of the Program.

Chief Privacy Officer (CPO): Like the corporate compliance officer (CCO), the CPO is responsible for the development and implementation of the policies and procedures. This person should command the respect of the persons in the various departments involved; should be meticulous; should understand the operations of the enterprise, especially including the health care aspect of the service or the entities customers. The CPO should also be sufficiently senior that the various departments will be responsive.

Privacy and Security Program: By the time the regulations are effective, each covered entity must have an effective privacy and security program in place. The minimum elements of the program are:

1. Designation of a Privacy Official or CPO.

2. Every member of the workforce (not just employees) must be trained on the policies and procedures on protected health information related to his or her function. The training must be included in orientation or within a reasonable period of time. Training must be repeated from time to time. Training on changes to the Program must occur. All training must be *documented*. Documentation should include both the fact of the training program and also who attended. While not required, consideration should be given to having individuals sign statements of learning and of compliance.

3. Safeguards must be in place to prevent both intentional and unintentional use or disclosure of private health information.

3. Detailed procedures must be documented. These procedures might parallel or be extracted from those in the corporate compliance plan.

4. Sanctions must be established for violation of the regulations or the policies and procedures and the policy should be uniformly applied. Actual sanctions will demonstrate an effective program.

5. Mitigate violations or their effects. The effect of any violation must be reduced or eliminated.

6. No retaliation may be tolerated against individuals exercising rights under the Program or the regulations, including filing complaints or acting as a whistleblower outside the entity.

7. No one may be required to waive their rights as a condition of treatment, payment, enrollments in a health plan, or eligibility for benefits.

8. Covered entities must have policies and procedures in place and updated. The Program should state that policies and procedures may be updated from time to time and retroactively. Otherwise, the procedures for changes are more complex. Notice of changes are required. But, if the Program is properly prepared, the changes may be retroactive.

9. Documentation: paper or electronic documentation or communication are permissible. Maintain records of all policies and procedures, changes and updates, complaints and investigations, resolution of complaints and investigations, etc. Finally, retain documentation for six years.

10. Group Health Plans do not have to comply with the first six and the ninth standards listed above *if*: (1) the plan provides health benefits solely through an insurance contract with a health insurer or HMO; (2) the health plan does not create or receive protected health information except summaries and enrollment/dis-enrollment.

The regulations make a brief and vague reference to a reporting obligation of covered entities. No requirements are set out. For now, it does not appear that any routine reports are required, but that could change in the future.

Not surprisingly, the Federal Government may initiate its own investigations, or it may follow-up on complaints. In either event, covered entities are required by the regulations to be cooperative. The key for covered entities will be to determine their procedures, including who will coordinate any requests for information and serve as the point person for the entity.

JENKENS & GILCHRIST ATTORNEY PROFILES

We are pleased to answer your questions and address specific issues related to the HIPAA Privacy Regulations. You may call or Email your HIPAA questions and concerns to any of the Jenkens & Gilchrist attorneys listed. *Thank you*.

Teri Bair
Shareholder
tbair@jenkens.com
713/951-3357

Ms. Bair, a pharmacist attorney, provides both general and specialized representation to a broad range of health care clients. Her experience involves preparation and review of corporate documents, mergers and acquisitions, state and federal legislative regulatory and reimbursement representation, physician practice management transactions and operational matters and health care system and provider operational matters with an emphasis on all pharmacy related matters.

Mike Cook
Shareholder
mhcook@jenkens.com
202/326-1500

Mr. Cook provides business, reimbursement, and regulatory guidance for health care providers of all types, with a special emphasis on acute and post acute providers. Prior to entering private practice, Mr. Cook represented Federal regulators of the Medicare and Medicaid programs as an attorney with the United States Department of Health and Human Services. Since leaving government, Mr. Cook has represented health care providers for more than twenty years, addressing issues and solving problems under Medicare, Medicaid and other government sponsored programs, and involving managed care payors, as well as addressing strategic planning, and business issues. Mr. Cook is a founding member of J&G's internal HIPAA Privacy Task Force, has been included in Who's Who in American Law, publishes and speaks widely on topics involving the health care industry, sits on a number of advisory task forces and editorial boards for health care related trade associations and publications, and was named by McKnight's Long Term Care News as one of the most influential people in the country on long term care.

Sheryl Dacso
Of Counsel
sdacso@jenkens.com
713/951-3332

Dr. Dacso specializes in health care innovation and strategic planning with emphasis on managed care, e-health strategies and complex transaction negotiation and dispute resolution. Her experience includes general health care, medical and hospital law with special interest in rural health care delivery systems. She is an AHLA certified mediator/negotiator for resolution of disputes and renegotiation of managed care and business relationships. Dr. Dacso's experience also includes design and implementation of recruitment and retention arrangements and representation of alternative health care delivery providers such as ambulatory care facilities, including freestanding surgery centers. Dr. Dacso has worked with large health care systems, governmental organizations and managed care organizations to mediate complex legal and operational issues.

Kenneth Gordon
Shareholder
kgordon@jenkens.com
214/855-4740

Mr. Gordon provides general and specialized representation of healthcare providers and vendors of all types. He regularly works with both laws and practical considerations involved with strategic planning; privacy and security compliance and analysis; health care fraud and abuse analysis, compliance and defense, including internal reviews; hospital operational matters; medical staff relations; physician, hospital and other integrated provider networks; clinics and other arrangements; group medical/practices; joint ventures; third-party reimbursement; patient consent; specialty issues; and managed care and network systems and arrangements.

Thomas Kulik
Associate
tkulik@jenkens.com
214/855-4728

Mr. Kulik focuses his practice upon intellectual property transactions, concentrating on the acquisition, development, protection and licensing of domestic and international intellectual property rights under copyright, trademark, patent and trade secret law. Mr. Kulik's extensive expertise includes the evolving law of the Internet, with particular emphasis on Internet privacy and e-commerce.

Robert Liles
Senior Attorney
rliles@jenkens.com
202/326-1593

Mr. Liles' practice focuses on health care fraud and regulatory matters. He served as an Assistant United States Attorney in the Southern District of Texas, Houston office, where he handled False Claims Act matters and cases. He was subsequently detailed to the Executive Office for United States Attorneys in Washington, D.C. as its first national Health Care Fraud Coordinator. In this capacity, he advised Assistant United States Attorneys in the 94 United States Attorneys' offices on civil and criminal health care fraud issues.

Jeffrey Look
Associate
jlook@jenkens.com
214/855-4380

Mr. Look focuses his practice on trademark law. His experience includes handling trademark application prosecutions, oppositions, infringement litigation matters, and Internet domain name dispute matters.

Iden Martyn
Of Counsel
lmartyn@jenkens.com
202/326-1523.

Mr. Martyn's practice focuses on health care fraud defense, regulatory compliance, and lobbying. Prior to joining Jenkens and Gilchrist, Mr. Martyn litigated criminal and civil matters as an Assistant United States Attorney for almost ten years, and most recently served as Counsel to the Subcommittee on Crime of the House Judiciary Committee (on detail from DOJ). In that role he provided counsel and support to the Subcommittee and full Judiciary Committee on issues relating to the development of criminal justice public policy.

Susan Murphy
Shareholder
smurphy@jenkens.com
713/951-3362

Ms. Murphy provides both general and specialized health law counsel to a variety of health care providers and entities. She has extensive experience in antitrust, federal and state remuneration issues and managed care network development and contracting. A significant portion of her practice focuses on physician practice management and ancillary network transactions, group practice development and integration, physician-hospital arrangements and joint ventures.

David Ralston
Associate
dralston@jenkens.com
713/951-3367

Mr. Ralston practices as a health care transactions lawyer with substantial experience in the merger and acquisition of various nationally recognized health care entities. He also represents clients before various regulatory bodies, including the Texas State Board of Medical Examiners and the Texas Pharmacy Board.