HIPAA

WHAT THE "H" DO I DO NOW?

Presented by

Michael H. Cook, Esq.

Jenkens & Gilchrist, A Professional Corporation

1919 Pennsylvania Avenue, N.W., Suite 600

Washington, D.C. 20006

(202) 326-1585 (phone)

(202) 326-1555 (fax)

mhcook@jenkens.com

To

HIPAA IMPLEMENTATION CASE STUDIES

LONG TERM CARE AND HOME HEALTH AGENCIES

THE HIPAA SUMMIT WEST

JUNE 20-22, 2001

THE HYATT EMBARCADERO CENTER

SAN FRANCISCO, CALIFORNIA

This outline is for informational purposes only and does not constitute legal advice. Anyone seeking legal advice should consult his or her own counsel.

Standards for Privacy of Identifiable Health Information[1]

I. Background:

A. History (65 *Fed Reg.* 82462, 82463)

1. Under Title II, Subtitle F, ' 261-264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, titled "Administrative Simplification," 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.

2. Under HIPAA, if Congress failed to enact privacy legislation prior to August 1999, the Department of Health and Human Services was tasked with promulgating these privacy regulations.

3. On August 17, 2000, the first regulation in this set, "Standards for Electronic Transactions," 65 *Fed. Reg.* 50312, was published.

4. This regulation establishes Standards for Privacy of Individually Identifiable Health Information.

5. Rules establishing a unique identifier for employers to use in electronic health care transaction, a unique identifier for providers for such transactions, and a rule establishing standards for the security of electronic information systems, have been proposed.

B. ' 160.101 - Statutory basis and purpose (65 *Fed. Reg.* 82462, 82463)

1. This regulation has three major purposes:

---

[1]Special thanks to Robert W. Liles, Senior Attorney, for his efforts in preparing this outline. Robert can be reached in J&G's Washington, D.C. office at (202) 326-1593, or at rliles"jenkens.com.

a. Protect and enhance the rights of consumers by providing access to their health information and controlling inappropriate use of that information.

b. Improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and organizations and individuals committed to the delivery of health care.

c. Improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection.

II. Part 160, Subpart A B General Provisions:

A. ' 160.102 - Applicability (65 *Fed. Reg.* 82462, 82475)

1. Under both the proposed Rule and the Final Rule, the subchapter (Parts 160, 162, and 164) applies to health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the subchapter.

B. ' 160.103 - Definitions (65 *Fed. Reg.* 82462, 82475, 82798)

1. Business associate (65 *Fed. Reg.* 82462, 82475, 82798):

a. Under the Final Rule, a "business association" occurs when the right to use or disclose the protected health information belongs to a covered entity, and another person is using or disclosing the protected information (or creating, obtaining and using the protected health information) to perform a function or activity on behalf of the covered entity.

b. It also occurs when a covered entity creates a business associate relationship if the provision of the service involves the disclosure of protected health information to the service provider.

c. The provision of specified services give rise to a business associate relationship if the performance of the service involves disclosure of protected health information by the covered entity to the business associate. Specified services include legal, actuarial, accounting , consulting, management, administrative accreditations, data segregation, and financial services.

d. In general, actions relating to the protected health information of an individual undertaken by a business associate are considered to be actions of the covered entity (although the covered entity is subject to sanctions under this Rule only if it has knowledge of the wrongful activity and fails to take the required actions to address the wrongdoing.

e. Business associate contracts are only required for cases in which:

(1) the covered entity is disclosing information to someone that will use the information on behalf of the covered entity,

(2) when the other person will be creating or obtaining protected health information on behalf of the protected entity,

(3) or when the business associate is providing the specified services to the covered entity and the provision of those services involves the disclosure of protected health information by the covered entity to the business associate.

(a) For example, when a health care provider discloses protected health information to health plans for payment purposes, no business associate relationship is established. While the covered provider may have an agreement to accept discounted fees for services provided to health plan members, neither entity is acting on behalf of, or providing a service to the other.

(b) Similarly, where a physician or other provider has staff privileges at a health institution, neither the physician nor the institution is a business associate based solely on staff privileges since neither party is providing functions or activities on behalf of the other. However, if the institution is providing services (e.g., billing services) for the physician, a business associate relationship may exist.

(4) Covered entities are permitted to disclose protected health information to "oversight agencies" (e.g., HCFA) that act to provide oversight of federal programs and the health care system. These oversight agencies are not performing

services on behalf of the covered entities and are thus not business associates of the covered entities.

(5) Covered entities do not have to enter into a business associate contract with a person or organization that merely acts as a conduit for protected information (*e.g.*, USPS, certain private couriers or their electronic equivalents). A conduit transports but does not have access to information. Moreover, no disclosure is intended by the covered entity and the probability of disclosure is very small.

(6) Financial institutions, acting on behalf of a covered entity, processing consumer-conducted financial transactions, is not a business associate.

2. Covered entity (65 *Fed. Reg.* 82462, 82476, 82799):

a. Covered entities include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred to in section 1173(a)(1) of the Act.

b. Health care providers who do not submit HIPAA transactions in standard form become covered by this Rule when other entities, such as a billing service or hospital, transmit standard electronic transactions on their behalf.

c. Where a public entity is required by law to administer a health plan jointly with another entity (*e.g.*, joint administration of Medicare+Choice between HCFA and the issuer offering the plan), we consider each agency to be a covered entity with respect to the health plan functions it performs.

3. Health care (65 *Fed. Reg.* 82462, 82477, 82799):

a. Health care means the "care, services, or supplies related to the health of an individual". Health care includes the following:

(1) Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

4. Health care clearinghouse (65 *Fed. Reg.* 82462, 82477, 82799):

a. A public or private entity, including billing services, repricing companies, community health management information systems or community health information systems, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

b. In order to fall within this category, a covered entity must perform the clearinghouse function on health information received from some other entity.

(1) Affiliates may perform clearinghouse functions for each other without triggering the definition of "clearinghouse" if the conditions in ' 164.504(d) are met.

5. Health care provider (65 *Fed. Reg.* 82462, 82477, 82799):

a. A provider of services (as defined in section 1861(u) of the Act, a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s), and any other person who furnishes, bills, or is paid for health care in the normal course of business.

6. Health information (65 FR 82462, 82478, 82799):

a. Any information, whether oral or recorded in any form or medium, that:

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

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

7. Health plan (65 *Fed. Reg.* 82462, 82478, 82799):

a. An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

C. ' 160.104 Modifications (65 *Fed. Reg.* 82462, 824800):

1. The Secretary may adopt a modification to a standard or implementation specification no more frequently than once every 12 months. However, during the first year, the Secretary may adopt a modification at any time after the standard is initially adopted, if the Secretary determines that modification is necessary to permit compliance with the standard or implementation specification.

III. Part 160, Subpart B - Preemption of State Laws:

A. ' 160.203 General Rule and Exceptions (65 *Fed. Reg.* 82462, 82480, 82801):

1. ' 1178 of the Act establishes a "general rule" that state law provisions that are contrary to the provisions or requirements of Part C of Title XI or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements.

2. Under the Final Rule, this general rule applies unless:

a. The Secretary determines are necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery, and other purposes;

b. The state law has as its principal purpose the "regulation of the manufacture, registration, distribution, dispensing, or control of any controlled substances", as defined under 21 U.S.C. 802, or under state law.

c. The state law relates to the privacy of individually identifiable health information and is more stringent than the federal requirements.

d. The state law provides for the reporting of public health concerns (*e.g.,* disease) or for the conduct of public health surveillance, investigation, or intervention.

e. The state law requires a health plan to report or provide access to information for the purpose of management audits, financial audits, program monitoring, and evaluation, or the licensure or certification of facilities or individuals.

B. § 160.204 Process for requesting exception determinations (65 *Fed. Reg.* 82462, 82801):

1. Requests to except a provision of state law from preemption may be submitted to the Secretary by the state's "chief elected official". Until a determination is made, the standard stays in effect.

C. § 160.205 Duration of effectiveness of exception determinations (65 Fr 82462, 82801):

1. Exceptions granted remain in effect until either the state law or the federal standard materially change such that the grounds for the exception no longer exists, or the Secretary revokes the exception.

IV. Part 160, Subpart C B Compliance and Enforcement:

A. § 160.304 Principles for achieving compliance (65 *Fed. Reg.* 82462, 82801):

1. The Secretary will seek the cooperation of covered entities in obtaining compliance with the requirements of these standards. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the these requirements.

B. § 160.306 Complaints to the Secretary (65 Fr 82462, 82801):

1. Right to file a complaint: A person who believes that a covered entity is not complying with the privacy requirements may file a complaint with the Secretary.

2. Requirements for filing complaints: Complaints must be filed in writing (either on paper or electronically). The complaint must name the covered entity that has allegedly committed a violation and must describe the acts or omissions are the basis of the complaint. It must be filed within 180 days of when the complainant knew or should have known that the act or omission occurred (unless the Secretary waives the time limit).

3. Investigation: The Secretary may investigate complaints filed under this section. Such investigations may include a review of pertinent policies, procedures, or practices of the covered entity and the circumstances regarding the alleged acts or omissions concerning compliance.

C. § 160.308 Compliance reviews (65 *Fed. Reg.* 82462, 82802):

1. The Secretary may conduct compliance reviews to determine if covered entities are complying with applicable requirements.

D. § 160.310 Responsibilities of covered entities (65 *Fed. Reg.* 82462, 82802):

1. Provide records and compliance reports: Covered entities must keep records and submit compliance reports in a manner and on a schedule that will be determined by the Secretary.

2. Cooperate with complaint investigations and compliance reviews: If the Secretary undertakes an investigation of compliance review of a covered entities' policies, procedures, or practices, the covered entity must cooperate.

3. Permit access to information:

a. A covered entity must permit the Secretary access during normal business hours. Access must be given to facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with applicable requirements. If the Secretary believes that records may be destroyed, the covered entity must provide access at any time, without notice.

b. If any information is in the possession of another agency, institution, or person who refuses to furnish the information, the covered entity must certify the efforts they have made to obtain the information.

c. Protected health information obtained by the Secretary in connection with an investigation or compliance review, will not be re-disclosed except as authorized by this statue or otherwise required by law.

E. § 160.312 Secretarial action regarding complaints and compliance reviews (65 *Fed. Reg.* 82462, 82802):

1. Resolution where noncompliance is indicated: If an investigation or compliance review discloses a failure to comply, the Secretary will inform the covered entity (and notify the complainant if the matter arose form a complaint), in writing, and attempt to resolve the matter informally. If the Secretary determines that the matter cannot be resolved informally, the Secretary will issue written findings documenting the non-compliance.

2. Resolution when no violation is found: If no violations are found, the Secretary will notify the covered entity (and the complainant, if applicable) in writing of this determination.

V. Part 164 -- Security and Privacy, Subpart E -- Privacy of Individually Identifiable Health Information:

A. § 164.500 Applicability (65 *Fed. Reg.* 82462, 82488, 82803):

1. As discussed in the commentary, under the proposed Rule, the standard would not have applied to information that was never electronically maintained or transmitted by a covered entity. Under the Final Rule, the scope of protection has been extended to all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes individually identifiable health information in paper records that never has been electronically stored or transmitted.

B. § 164.501 Definitions (65 *Fed. Reg.* 82462, 82491, 82803):

1. Health care operations (65 *Fed. Reg.* 82462, 82491, 82803):

a. Includes any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities.

(2) Reviewing the performance, competence or qualifications of health care professionals, health plans, and students.

(3) Underwriting and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

(5) Business planning and development (*e.g.*, cost-management and planning related analyses; formulary development; payment methods).

(6) Business management and general administrative activity, including compliance implementation, customer service, resolution of internal grievances, due diligence, creating de-identified health information, fund-raising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in section 164.514(e)(2).

2. Health oversight agency (65 *Fed. Reg.* 82462, 82491-2, 82803):

a. In the preamble to the proposed proposed Rule, a number of examples of health oversight agencies that conduct oversight activities relating to the health care system are listed. Some include: Offices of Inspectors General of federal agencies; the Department of Justice; state Medicaid fraud control units; Defense Criminal Investigative Services; the HHS Office for Civil Rights; and the HHS, Food and Drug Administration. The Final Rule added the Department of Justice's civil rights enforcement activities, and EEOC's civil rights enforcement activities.

b. Under the Final Rule, "health oversight agency" is defined as an agency or authority of the United States, a state or territory, including persons or entities acting under a grant of authority from a contract with such agencies, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights for which health information is relevant.

c. The definition of health oversight agency does not include private organizations such as private-sector accrediting groups. Accreditation organizations are performing health care operations on behalf of health plans and covered health care providers. As a result, in order to obtain protected health information without an individual's authorizations, they must enter into business associate agreements with health plans and covered providers. Similarly, coding committees, that help government agencies that are health plans make coding and payment decisions are performing health care payment functions and must enter business associate agreements in order to receive protected health information from

the covered entity (absent individual's authorization for such disclosure).

3. Individually identifiable health information (65 *Fed. Reg.* 82462, 82491, 82804):

   a. The definition under the Final Rule remains largely unchanged from that originally proposed. Under the Final Rule, "individually identifiable health information" is information that is a subset of the term "health information", described above. It includes:

      (1) Information created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

      (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual, and (ii) there is a reasonable basis to believe that the information could be used to identify the individual.

4. Law enforcement official (65 *Fed. Reg.* 82462, 82493, 82804):

   a. The Final Rule recognizes that law enforcement officials are empowered to prosecute cases as well as to conduct investigations and civil or criminal administrative proceedings. It also recognizes that when an investigation begins, it is not always clear if the law has been violated. The Final Rule describes law enforcement investigations and official proceedings as inquiring into a potential violation of law. It also describes law enforcement related civil, criminal, or administrative proceedings as arising from alleged violations of law.

5. Marketing (65 *Fed. Reg.* 82462, 82493, 82804):

   a. The proposed Rule did not include a definition of "marketing." In the Final Rule, it is defined as a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service. The definition does not limit the type or means of communication.

b. Exceptions to the definition encompass oral communications or written communications in which the covered entity does not receive direct or indirect remuneration from a third party for making the communication. Exceptions:

(1) The purpose of the first exception in to avoid interfering with communications made to individuals about their health benefits. Covered entities may use or disclose protected health information when discussing topics such as the benefits and services available under a health plan, the payment that may be made for a product or service, which providers offer a product or service, and whether a provider is part of a network or whether (and what amount of) payment will be provided with respect to the services of particular providers.

(2) The purpose of the second exception is to avoid interfering with communications made to individuals about their treatment or about the management of their treatment. Health care providers are free to use or disclose protected health information as part of a discussion of its products and services, or the products and services of others, and to prescribe, recommend, or sell such products or services, as part of the treatment of an individual.

6. Organized health care arrangement (65 *Fed. Reg.* 82462, 82494, 82804):

a. This term was not covered in the proposed Rules. HHS include it in the Final Rules to describe certain arrangements in which participants need to share protected health information about their patients to manage and benefit the enterprise. Five basic arrangements are described in the rule. While they may vary in legal structure, a key component of these arrangements is that the individuals who obtain services from them have an expectation that these arrangements are integrated and that they jointly manage their operations.

b. A common example of this type of organized arrangement is the hospital setting, where a hospital and a physician with staff privileges together provide treatment to the individual. Participants in these settings need to be able to share health information freely.

7. Protected health information (65 *Fed. Reg.* 82462, 82496, 82805):

a. Under the proposed Rule, "protected health information" only included information that is or has been electronically submitted. The Final Rule removed this limitation and expanded the definition to encompass all individually identifiable health information transmitted or maintained by a covered entity, regardless of form.

C. § 164.502 Uses and disclosures of protected health information: general rules (65 *Fed. Reg.* 82462, 82498, 82805):.

1. Standard (65 *Fed. Reg.* 82462, 82498, 82805):

a. As in the proposed Rule, under the Final Rule, the general standard remains that covered entities may <u>not</u> use or disclose protected health information except as permitted or required by the rule. Moreover, HHS made substantial changes to the conditions under which uses and disclosures are permitted under the rule. As discussed in the commentary:

(1) Covered health care providers who have a direct treatment relationship with an individual are required 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.

(2) In general, as under the proposed Rule, other covered entities are permitted to use and disclose protected health information to carry out treatment, payment, or health care operations without obtaining such consent.

(3) Covered entities must, as under the proposed Rule, obtain the individual's authorization in order to use or disclose psychotherapy notes for most purposes.

(4) 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 § 164.510. 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.

b. Covered entities may disclose protected health information to the individual who is the subject of that information without any condition. This includes "personal representatives" of individuals as provided in § 164.502(g).

c. covered entity may use or disclose protected health information for other lawful purposes if the entity obtains a written "authorization" from the individual, consistent with the provisions of § 164.508. Unlike "consents", "authorizations" are specific and detailed. They are intended to provide the individual with concrete information about, and control over, the uses and disclosures of protected health information about themselves.

d. Under the Final Rule, a covered entity is required to disclose protected health information in only two instances:

(1) To an individual requests access to information about himself.

(2) When disclosures are compelled by the Secretary for compliance and enforcement purposes.

2. Standard: minimum necessary (65 *Fed. Reg.* 82462, 82499, 82805):

a. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose.

b. Minimum necessary does not apply to:

(1) Disclosure to or requests by a health care provider for treatment.

(2) Uses or disclosures made to the individual.

(3) Disclosures made to the Secretary in accordance with this rule.

(4) Uses or disclosures that are required by law.

(5) Uses or disclosures that are required for compliance with this chapter.

3. Standard: uses and disclosures of protected health information subject to an agreed upon restriction. (65 *Fed. Reg.* 82462, 82499, 82806):

   a. The Final Rule retains an individual's right to request restrictions on uses or disclosures for treatment, payment or health care operations and prohibits a covered entity from using or disclosing protected health information in a way that is inconsistent with the agreed upon restriction between the covered entity and the individual.

   b. Individuals have the right to request restrictions of all covered entities.

4. Standard: uses and disclosures of de-identified protected health information (65 *Fed. Reg.* 82462, 82499, 82806):

   a. A covered entity may use protected health information to create de-identified information, whether or not the de-identified information is to be used by the covered entity. Deidentified information is not subjects to the requirements of these rules unless it is re-identified. Disclosure of a "key" or mechanism that could be used to re-identify such information constitutes disclosure of protected health information.

5. Standard: disclosures to business associates (65 *Fed. Reg.* 82462, 82499, 82806):.

   a. A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

6. Standard: deceased individuals (65 *Fed. Reg.* 82462, 82499, 82806):

   a. Under the proposed Rule, privacy protections would cover protected health information of an deceased individual for two years following the date of death. This was extended under the Final Rule. Covered entities are now required to protect health information about deceased individuals for as long as the covered entity maintains the information.

7. Standard: personal representatives (65 *Fed. Reg.* 82462, 82501, 82806):

a. A covered entity must treat a person that meets the requirements of a "personal representative" as the individual. Disclosure to a personal representative is only mandatory if disclosure to the individual was mandatory.

b. In its commentary, HHS states that it will "continue to allow covered entities to use their discretion to disclose certain protected health information to family members, relatives, close friends, and other persons."

8. Standard: confidential communications (65 *Fed. Reg.* 82462, 82501, 82806):

a. Covered providers must accommodate reasonable requests by patients as to how the covered provider communicates with the individual. For instance, an individual who does not want a family member to know about a certain treatment may ask that the provider call him or her at work rather than at home.

9. Standard: uses and disclosures consistent with notice (65 *Fed. Reg.* 82462, 82501, 82807):

a. Covered entities cannot use or disclose information in a manner that is inconsistent with their notice of information practices.

10. Standard: disclosures by whistleblowers and workforce member crime victims (65 *Fed. Reg.* 82462, 82501, 82806):

a. A covered entity is not in violation of the requirements of this rule when a member of its workforce or a business associate of the covered entity discloses protected health information to:

(1) A health oversight agency or public health authority authorized by law to investigate or oversee the relevant conduct.

(2) An appropriate health care accreditation organization.

(3) An attorney, for the purpose of determining his or her options with respect to whistleblowing.

D. § 164.504 Uses and disclosures: organizational requirements (65 *Fed. Reg.* 82462, 82502, 82807):

1. Standard: health care component (65 *Fed. Reg.* 82462, 82502, 82807):

   a. 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 university may have an on-site clinic that provides health services to its students. In such a case, the clinic would be a covered entity but the university may have no other involvement in the provision of health care. In such a situation, as a practical matter, it makes sense for the entity to focus its compliance efforts in the component that is actually performing health care functions (i.e. the clinic).

   b. The Final Rules provide that for a hybrid entity, the rules apply only to the part of the entity that is the health care component. Thus the covered entity must construct a "firewall" to protect against the improper use or disclosure of protected health information within or by the organization.

2. Standard: affiliated covered entities (65 *Fed. Reg.* 82462, 82503, 82808):

   a. The requirements that apply to a covered entity also apply to an affiliated covered entity. For instance, a hospital in one state could not share protected health information about a patient with another hospital if such a use is not necessary for treatment, payment or health care operations.

3. Standard: business associate contracts (65 *Fed. Reg.* 82462, 82504, 82808):

   a. A covered entity is not in compliance with the rule if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract , unless the covered entity took reasonable steps to cure the breach or end the violation, and if such steps were unsuccessful.

   b. A covered entity 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.

c. The regulation specifies the elements of what constitutes satisfactory assurances.

d. Covered entities have responsibilities when such assurances are violated by a business associate.

e. In its commentary, HHS notes that a master business associate contract or MOU that otherwise meets the requirements regarding specified satisfactory assurances meets the requirements with respect to all signatories.

4. Standard: requirements for group health plans (65 *Fed. Reg.* 82462, 82507, 82808):

a. Under the Final Rule, group health plans are permitted to authorize health insurance issuers or HMOs 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 the plan documents. The group health plan is not required to have a business associate contract with the plan sponsor to disclose protected health information or allow the sponsor to create protected health information if the conditions of § 164.504(e) are met.

b. Plan documents will need to be amended to describe the permitted uses and disclosures of protected health information, specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that the plan documents have been amended and that the sponsor agrees to certain conditions regarding use and disclosure, and provide adequate firewalls.

5. Standard: requirements for a covered entity with multiple covered functions (65 *Fed. Reg.* 82462, 82507, 82809):

a. The Final Rule recognizes that 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.

E. § 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations. (65 *Fed. Reg.* 82462, 82509, 82810):

1. *Consent vs. Authorization* (65 *Fed. Reg.* 82462, 82509):

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 clearinghouses may also seek a consent.

b. An "authorization" allows the 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 in writing 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 (See § 164.508) , a covered entity may not refuse to treat someone based on the fact that they refuse to sign an authorization.

2. Standard: consent requirement (65 *Fed. Reg.* 82462, 82509, 82810):

a. A covered entity must obtain an individual's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.

b. A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations if the covered health care provider has an indirect relationship with the individual.

c. A covered health care provider may, without prior consent, use or disclose protected health information created or received to carry out treatment, payment, or health care operations:

(1) In emergency care situations, if the covered health care provider attempts to obtain consent as soon as reasonable possible.

(2) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts but is unable to obtain consent.

(3) If a covered health care provider attempts to obtain consent but is unable to do so due to communication barriers and in the covered health care provider's professional judgment, the individual's consent is clearly inferred from the circumstances.

3. Implementation specifications: general requirements (65 *Fed. Reg.* 82462, 82511, 82810):

a. Under the Final Rule, a covered health provider is permitted to condition the provision of treatment on the receipt of an individual's consent for the covered provider to use and disclose protected health information to carry out treatment, payment, and health care operations. Covered providers may refuse to treat individuals who do not consent to uses and disclosures for these purposes.

b. A similar provision is provided for health plans.

c. A consent provision may not be combined in a single document with the notice requirements of § 164.520.

d. A consent for use or disclosure may be combined with other types of written legal permission from the individual (*e.g.*, informed consent for treatment) if the consent:

(1) Is visually and organizationally separate from the other legal permission.

(2) Is separately signed and dated.

4. Implementation specifications: content requirements (65 *Fed. Reg.* 82462, 82511, 82810):

   a. A consent must be written in plain language.

   b. It must inform the individual that protected health information may be used or disclosed to carry out treatment, payment or health care operations.

   c. It must refer the individual to the covered entity's notice for additional information about the uses and disclosures of information described in the consent. It must also indicate that the individual has the right to review the notice prior to signing the consent.

   d. It must notify the individual that they have the right to request restrictions on uses and disclosures. While the covered entity does not have to agree to the request, but it if does agree, it is binding on the covered entity.

   e. The consent must indicate that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance on the consent.

   f. It must be signed and dated.

5. Implementation specifications: defective consents (65 *Fed. Reg.* 82462, 82511, 82810):

   a. There is no "consent" within the meaning of the rule, if a completed document lacks a required element or if the individual has revoked the consent.

6. Standard: resolving conflicting consents and authorizations (65 *Fed. Reg.* 82462, 82512, 82810):

   a. Under the rule, when the terms of a covered entity's consent conflict with the terms of another legal permission from the individual to use or disclose protected health information, the covered entity must adhere to the more restrictive document.

7. Standard: joint consents (65 *Fed. Reg.* 82462, 82513, 82811):

a. Covered entities that participate in an organized health care arrangement may develop a joint notice and a joint consent in which the individual consents to the uses and disclosures of protected health information by each of the covered entities in the arrangement. If any one of the covered entities included in the joint consent obtains the individual's consent , the requirement is met for all other covered entities to which the consent applies.

F. § 164.508 Uses and disclosures for which an authorization is required (65 *Fed. Reg.* 82462, 82513, 82811):

1. Standard: authorizations for uses and disclosures (65 *Fed. Reg.* 82462, 82513, 82811):

a. As in the proposed Rule, the Final Rule requires that covered entities have authorization from individuals prior to using or disclosing protected health information for any purpose not otherwise permitted or required by the rule. Specifically, except for psychotherapy notes, covered entities are not required to obtain the individual's authorization to use or disclose protected health information to carry out treatment, payment and health care operations.

b. Covered entities are bound by the statements provided on the authorization; use or disclosure by the covered entity for purposes inconsistent with the statements made in the authorization constitute a violation of the rule.

c. Examples of specific applications:

(1) Marketing: Covered entities must obtain the individual's authorization before using or disclosing protected health information for marketing purposes. The definition of "marketing" is covered at § 164.501.

(2) Pre-enrollment underwriting: Covered entities must obtain the individual's authorization to use or disclose protected health information before making eligibility or enrollment determinations relating to underwriting or risk rating determinations.

(3) Employment determinations: As in the proposed Rule, covered entities must obtain the individual's authorization to use or disclose protected health information before

making employment determinations (*e.g.*, authorization is required to disclose the results of a pre-employment physical).

(4) Fundraising: Authorization is not required when a covered entity uses or discloses demographic information and information about the dates of health care provided to an individual for the purpose of raising funs for its own benefit, nor when it discloses such information to an institutionally related foundation to raise funds for the covered entity. Any use or disclosure that falls outside of § 164.514(f) requires authorization.

2. Implementation specifications: general requirements; valid and defective authorizations (65 *Fed. Reg.* 82462, 82515-17, 82811-12):

a. Required elements of a valid authorization:

(1) Description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion, including: the name of the person(s) authorized to make the requested use or disclosure; the name(s) to whom disclosure may be made; the expiration date that relates to the individual or the purpose of the use or disclosure; a statement of the individual's right to revoke the authorization; a statement regarding re-disclosures; signature; date.

(2) The authorization must be written in plain language.

(3) Additional elements may be required, if applicable, as described in § 164.508, paragraphs (d), (e), or (f).

(b) An authorization is defective if:

(1) The expiration date has passed.

(2) The authorization has not been filled out completely.

(3) The authorization is known to have been revoked.

(4) The authorization lacks a required element.

(5) Any material information in the authorization is known to be false.

3. Prohibition on conditioning treatment, payment, eligibility, or enrollment (65 *Fed. Reg.* 82462, 82516):

a. The basic approach taken in the proposed Rule was adopted, and refined, in the Final Rule. In addition to the general prohibition on conditioning treatment and payment, covered entities are also prohibited (with certain exceptions) from conditioning eligibility for benefits or enrollment in a health plan on obtaining an authorization. This extends to all authorizations, not just those for use or disclosure of psychotherapy notes.

b. This prohibition is intended to prevent covered entities from coercing individuals into signing an authorization for use or disclosure that is not necessary to carry out the primary services that the covered entity provides to the individual. For example, a covered provide cannot refuse to treat an individual because the individual refused to authorize a disclosure to a pharmaceutical manufacturer for the purpose of marketing a new product.

G. § 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object (65 *Fed. Reg.* 82462, 82521, 82812):

1. Standard: use and disclosure for facility directories (65 *Fed. Reg.* 82462, 82521, 82812):

a. Under the Final Rule, health care facilities may include patient information in their directory 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 information that can be disclosed.

(3) The patient does not object to being included in the directory.

b. Both a facility's notice and the individual's opt-out or restriction may be oral.

c. Subject to the individual's right to object, a health care provider may disclose the individual's general condition (*e.g.*, fair, critical, stable, etc.) and their location in the facility to persons who inquire

about the individual by name. Absent an individual's objection, an individual's religious affiliation may be disclosed to members of the clergy.

2. Standard: uses and disclosures for involvement in the individual's care and notification purposes (65 *Fed. Reg.* 82462, 82521, 82812):

a. 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 other person identified by the individual) protected health information directly related to the person's involvement in the current health care of the individual.

H. § 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (65 *Fed. Reg.* 82462, 82524, 82813):

1. Standard: uses and disclosures required by law (65 *Fed. Reg.* 82462, 82524, 82813):

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

b. Should the use or disclosure involve one or more of the national priority purposes described elsewhere in this section (*e.g.*, domestic violence, for judicial proceedings, or for law enforcement purposes), such uses or disclosures must conforms with the requirements set out in those provisions.

2. Standard: uses and disclosures for public health activities (65 *Fed. Reg.* 82462, 82525, 82813):

a. Covered entities may disclose protected health information for the certain public health activities as described in the rule.

3. Standard: disclosures about victims of abuse, neglect or domestic violence (65 *Fed. Reg.* 82462, 82524, 82814):

a. Under the Final Rule, covered entities may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect or domestic

violence. Three circumstances are identified when this these disclosures may be made:

(1) When required by law.

(2) When the individual has agreed to the disclosure.

(3) Without the individual's agreement if the disclosure is expressly authorized by statute or regulation and either:

(a) the covered entity, in its professional judgment, believes that the disclosure is necessary to prevent serious harm to the individual or others, or

(b) if the individual is unable to agree due to incapacity, if other requirements are also met under the statute.

4. Standard: uses and disclosures for health oversight activities (65 *Fed. Reg.* 82462, 82528, 82814):

a. A covered entity may disclose protected health information to a health oversight agency (as defined under § 164.501) for oversight activities authorized by law, including

(1) Civil, administrative, or criminal investigations.

(2) Inspections.

(3) Licensure or disciplinary actions.

(4) Civil, administrative, or criminal proceedings or actions.

(5) Other activities necessary for the appropriate oversight of:

(a) The health care system

(b) Government benefit programs for which health information is relevant to beneficiary eligibility.

(c) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards.

(d) Entities subject to civil rights laws for which health information is necessary for determining compliance.

b. Under the proposed Rule, there was considerable, and often confusing, overlap between "law enforcement" and "health oversight." Under the Final Rule, an investigation or activity is not considered health oversight for purposes of the rule if:

(1) The individual is the subject of the investigation or activity, and

(2) The investigation or activity does not arise out of and is not directly related to (a) the receipt of health care, (b) a claim for public benefits related to health, or (c) qualification for, or receipt of public benefits or services where a patient's health is integral to the claim for benefits or services. **[Note: in its commentary, HHS states that for purposes of the rule, (a) through (c) relate to investigations of health care fraud]**.

(3) Where an individual is the subject of the investigation and the investigation does not relate to issues (a) through (c) above, the rule regarding disclosure for law enforcement purposes (§ 164.512(f)) applies.

5. Standard: disclosures for judicial and administrative proceedings (65 *Fed. Reg.* 82462, 82529, 82814):

a. This section addresses when a covered entity is permitted to protected health information in response to requests that are made for protected health information in the course of judicial or administrative proceedings (*e.g.*, non-party hospital receives a subpoena for medical records in a automobile tort case).

b. Under the Final Rule, covered entities are permitted to disclose protected health information in a judicial or administrative proceeding if the request for such information is made pursuant to a court order, order from an administrative tribunal, subpoena, discovery request, or other lawful process, by a party to the proceeding.

(1) If the request is made pursuant to an order or subpoena from a court or administrative tribunal, a covered entity may disclose the information without additional process.

(2) Absent an order of, or subpoena by a court or administrative tribunal, a covered entity may respond to a subpoena, discovery request, or other lawful process, by a party to the proceeding only if the covered entity obtains either (a) satisfactory assurances that reasonable efforts have been made to the give the individual whose information has been requested notice of the request; or (b) satisfactory assurances that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information.

6. Standard: disclosures for law enforcement purposes (65 *Fed. Reg.* 82462, 82531, 82815-16):

a. Under the Final Rule, a covered entity may disclose protected health information for a law enforcement purpose, to a law enforcement official in the following circumstances:

(1) Pursuant to process and as otherwise required by law: As required by laws includes (but is not limited to) the reporting of certain types of wounds (*e.g.*, gunshot wounds) or other physical injuries. It also covers compliance with court orders, warrants, court-ordered subpoena, summons issued by a judicial officer, a grand jury subpoena, an administrative request, including an administrative subpoena or summons, civil or authorized investigative demand, or similar process. Information sought must be material to a legitimate law enforcement inquiry and must be limited in scope to the extent reasonably practicable in light of its purpose.

(2) Limited information for identification and location purposes: A covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. In addition to basic information (*e.g.*, name, address, date and place of birth, etc.), the covered entity may disclose a description of physical characteristics. There are limitations on providing some types of health information such as DNA, body fluids, etc.

(3) Victims of a crime: A covered entity may disclose protected health information in response to a law

enforcement official's request for such information about an individual who is, or is suspected to be, a victim of crime, as long as the victim agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance (as permitted under the rule).

(4) Decedents: A covered entity may 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.

(5) Crime on premises: A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of a criminal conduct that occurred on the premises of the covered entity.

(6) Reporting crime in emergencies: A covered entity providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure is necessary to alert law enforcement to the commission and nature of a crime, the location of a crime or of victims, or identity, description, and location of the perpetrator.

7. Standard: uses and disclosures about decedents (65 *Fed. Reg.* 82462, 82534, 82816):

a. Under the Final Rule, covered entities are permitted to disclose protected health information to coroners and medical examiners for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.

b. A covered entity may also disclose protected health information to funeral directors, as necessary to carry out their duties. If necessary for them to carry out their duties, this information may be disclosed in reasonable anticipation of an individual's death.

8. Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes (65 *Fed. Reg.* 82462, 82534, 82816):

a. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantations of organs, eyes, or tissues.

9. Standard: uses and disclosures for research purposes (65 *Fed. Reg.* 82462, 82535-38, 82816):

a. Under circumstances specified in the rule, a covered entity may use or disclose protected health information for research, regardless of the source of funding for such research.

10. Standard: uses and disclosures to avert a serious threat to health or safety (65 *Fed. Reg.* 82462, 82538-39, 82817):

a. A covered entity may, consistent with applicable laws and standards of ethical conduct, use or disclose protected health information, if the covered entity believes in good faith that the use or disclosure:

(1) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

(2) Is necessary for law enforcement authorities to identify or apprehend an individual.

b. A disclosure may not be made under paragraph (j)(1)(ii)(A) of the rule for a statement admitting participation in a violent crime if the covered entity learns the information in the course of counseling or therapy.

11. Standard: uses and disclosures for specialized government functions (65 *Fed. Reg.* 82462, 82539, 82817):

a. A covered entity may use or disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission [requires the military authority to publish a separate notice in the Federal Register].

12. Standard: disclosures for workers' compensation (65 *Fed. Reg.* 82462, 82539, 82817):

a. A covered entity may use or disclose the protected health information as authorized by and to the extent necessary to comply

with the laws relating to worker's compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

I. § 164.514 Other requirements relating to uses and disclosures of protected health information (65 *Fed. Reg.* 82462, 82542, 82818):

1. Standard: de-identification of protected health information (65 *Fed. Reg.* 82462, 82542-43, 82818):

a. The Final Rule explicitly adopts the statutory standard as the basic regulatory standard for whether health information is identifiable health information under the rule. Information is not individually identifiable under the rule if it does not identify the individual, or if the covered entity has no reasonable basis to believe it can be used to identify the individual.

2. Implementation specifications: requirements for de-identification of protected health information (65 *Fed. Reg.* 82462, 82543, 82818):

a. 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.

3. Implementation specifications: re-identification (65 *Fed. Reg.* 82462, 82543, 82819):

a. 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 .

b. 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.

4. Standard: minimum necessary requirements (65 *Fed. Reg.* 82462, 82543, 82819):

a. The Final Rule is substantially modified from the proposed requirements. Under the Final Rule, for all uses and many disclosures and requests for disclosures from other covered entities, it is required that covered entities implement policies and procedures for "minimum necessary" uses and disclosures.

b. Implementation of such policies and procedures is required in lieu of making the "minimum necessary" determination for each separate use or disclosure.

(1) Uses of protected health information: A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties (along with the categories of protected health information to which such persons will need access). A covered entity must make reasonable efforts to limit the access of such persons or classes of persons to protected health information.

(2) Disclosures of protected health information: 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. 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: 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.

5. Standard: uses and disclosures of protected health information for marketing (65 *Fed. Reg.* 82462, 82545, 82819):

a. The general rule is that 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.

b. 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 states that fact; except in the case of a general communication (such as a newsletter) meets the requirements of the rule.

6. Standard: uses and disclosures for fundraising (65 *Fed. Reg.* 82462, 82546, 82820):

a. A covered entity may use protected health information without individual authorization for fundraising on behalf of itself, 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.

b. Fundraising materials must explain how the individual may opt-out of any further fundraising communications, and covered entities are required to honor such requests.

c. A covered entity is permitted to disclose the limited health information to a business associate for fundraising on its own behalf.

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

7. Standard: uses and disclosures for underwriting and related purposes (65 *Fed. Reg.* 82462, 82546, 82820):

a. 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.

b. 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.

8. Standard: verification requirements (65 *Fed. Reg.* 82462, 82546, 82820):

a. Prior to any disclosure under this subpart, 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).

b. 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.

J. § 164.520 Notice of privacy practices for protected health information (65 *Fed. Reg.* 82462, 82547, 82820):

1. Standard: notice of privacy practices (65 *Fed. Reg.* 82462, 82547, 82820):

a. 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.

2. Implementation specifications: content of notice (65 *Fed. Reg.* 82462, 82548-50, 82821):

a. Unlike the proposed Rule, no "model" notice is included in the Final Rule. HHS intends to develop further guidance on notice requirements prior to the compliance date of the rule.

b. The basics:

(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.

c. 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.

d. 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.

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

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

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

3. Implementation specifications: provision of notice (65 *Fed. Reg.* 82462, 82551, 82821-22):

a. 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, HHS states that it intends the notice to be a public document that people can use in choosing between covered entities.

b. Under the Final Rule, 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.

c. Distribution requirements differ according to whether the covered health care provider has a direct, versus an indirect treatment relationship with an individual.

(1) 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.

(2) Covered providers that have an indirect relationship with individuals are only required to produce the notice upon request.

4. Implementation specifications: joint notice by separate covered entities (65 *Fed. Reg.* 82462, 82552, 82822):

a. 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.

5. Implementation specifications: documentation (65 *Fed. Reg.* 82462, 82551, 82822):

a. 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.

K. § 164.522 Rights to request privacy protection for protected health information (65 *Fed. Reg.* 82462, 82552, 82822):

1. Standard: right of an individual to request restriction of uses and disclosures (65 *Fed. Reg.* 82462, 82552, 82822):

a. Under the Final Rule, HHS retained 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.

b. A covered entity is not required to agree to the restriction.

c. A covered entity 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.

d. A covered entity that agrees to a restriction must the restriction in accordance with the administrative requirements set out in § 164.530(j).

2. Standard: confidential communication requirements (65 *Fed. Reg.* 82462, 82553, 82823):

a. Covered entities must permit individuals to request that the covered entity provide confidential communications of protected health information about the individual. Moreover, 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.

b. Covered health care provider versus health plan: Covered health care providers must accommodate all reasonable requests. Health plans must accommodate all 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, HHS 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 (*e.g.*, the named insurer) might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the request."

c. 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.

d. 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.

L. § 164.524 Access of individuals to protected health information (65 *Fed. Reg.* 82462, 82554, 82823):

1. Standard: access to protected information (65 *Fed. Reg.* 82462, 82554, 82823):

a. General rule: As in the proposed Rule, under the Final Rule, individuals have a right to access to protected health information that is maintained in a "designated record set." This right applies to health plans, covered health care providers, and health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity.

b. Protected health information not used to make decisions about individuals: Under the Final Rule, individuals have a right of access to any protected health information that is used, in whole or in part, to make decisions about individuals. For example, protected health information may be used to determine whether or not an insurance claim will be paid. As a result, the individual would have a right of access to the information. However, protected health information kept in information systems used for other purposes (*e.g.*, quality control or peer review analysis) may not be used to make decisions about individuals. In these situations, the individual will not have a right of access to the protected health information.

c. Duration of the right of access: Covered entities must provide access to individuals for as long as the protected health information is maintained in a designated record set.

d. Exceptions to the right of access: There are three types of information to which individuals do not have a right of access, even if they are kept in a designated record set. They are:

(1) Psychotherapy notes.

(2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(3) Certain protected health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988. Covered entities may, but are not required to, provide access to this information.

e. Unreviewable grounds for denial: Under the Final Rule, a number of grounds are listed for denying access to records, without providing an individual with a right to have the denials reviewed. The grounds include, but are not limited to: they involve psychotherapy notes; information compiled in anticipation of civil, criminal, or administrative proceedings; are involved in ongoing research activities; the protected health information is contained in records that are subject to the Privacy Act and providing access would violate the Privacy Act.

f. Reviewable grounds for denial: A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed in the following circumstances:

(1) A licensed health care professional determined the inspection and copying was reasonably likely to endanger the life or physical safety of the individual or another person.

(2) The information was about another person and (other than a health care provider) and a licensed health care professional determined the inspection and copying was reasonably likely to cause substantial harm to that other person.

(3) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to the individual's personal representative is likely to cause substantial harm to the individual or another person.

g. Review of a denial of access: If access is denied based on one of the three reviewable grounds listed above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny.

2. Implementation specifications: requests for access and timely action (65 *Fed. Reg.* 82462, 82556, 82823):

a. Requests for access: A covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. Covered entities may require individuals to make the request in writing.

b. Timely action required by the covered entity: A covered entity must act on a reviewable request from an individual no later than 30 days after receipt of the request.

3. Implementation specifications: Provision of access (65 *Fed. Reg.* 82462, 82556, 82824):

a. If a covered entity accepts a request, and provides an individual with access to protected heath information (in whole or in part), the covered entity must:

(1) Provide the access requested: Individuals have a right to inspect, copy, or both. If the same information is kept in more than one designated record set, the covered entity is only required to produce the information once per request for access.

(2) Form of access requested: A covered entity must provide the information in a form or format requested if it is readily producible in such a form or format. For example, if the information is available electronically and the individual wants an electronic copy, the covered entity must accommodate the request if possible. If the information is not available in the form requested, the covered entity must produce a readily readable hard copy of the information or another jointly agreed format. If the individual agrees (and agrees to pay any associated fees), the covered entity may provide access to a summary of information rather than all protected health information in designated record sets.

(3) Time and manner of access: A covered entity must provide the access requested in a timely manner, and arrange for a mutually convenient time and place for the individual to inspect the protected health information or obtain a copy. It the individual asks that the copy be mailed, the mailing fees may be assessed by the covered entity.

(4) Fees: A covered entity may charge a reasonable, cost-based fee for copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made, this would include the cost of the computer disk. Covered entities may not charge for retrieving and handling the information or for processing the request. Fees for copying and postage may also be assessed. If an individual requests an explanation or summary and agrees in advance to any associated costs, the covered entity may charge for the summary or explanation as well. Nothing in the rule affects current practices with regard to the fees charged by one covered entity when sending copies of records to another covered entity for treatment purposes.

4. Implementation specifications: Denial of access (65 *Fed. Reg.* 82462, 82557, 82824):

a. Making other information available: A covered entity that denies access (in whole or in part), must, to the extent possible, give the individual access to any other protected health information requested, after excluding the information that the covered entity has claimed a ground for denying access.

b. Basis for denial: The covered entity must provide a timely, written denial that is in plain language. The denial must contain the following: the basis for the decision; a statement of the individual's review rights along with a description of how the individual may exercise such rights; and a description of how to complain to the covered entity (including the name, and phone number of the contact person or office), or to the Secretary about the denial decision.

c. Other responsibility: If the covered entity does not maintain the requested protected health information, but knows where it is maintained, it must inform the individual where to contact for access.

5. Implementation specifications: Documentation (65 *Fed. Reg.* 82462, 82824):

a. A covered entity must document the designated record sets that are subject to access by individuals and the tiles of persons or offices responsible for receiving and processing requests for access by individuals.

M. § 164.526 Amendment of protected health information (65 *Fed. Reg.* 82462, 82558, 82824):

1. Standard: right to amend (65 *Fed. Reg.* 82462, 82558, 82824):

a. An individual has the right to have a covered entity amend protected health information in a designated record set for as long as the protected health information is maintained in the designated records set.

b. A covered entity may deny a request for amendment if the covered entity did not create the protected health information or record that is the subject of the request for amendment. One exception: if the originator of the protected health information is no longer available to act on the requested amendment, the covered entity must

address the request as though the covered entity had created the information.

2. Implementation specifications: requests for access and timely action (65 *Fed. Reg.* 82462, 82558, 82825):

   a. A covered entity may require that an individual submit a request for amendment in writing and provide a reason in support of the request.

   b. An entity must act on a request for amendment within 60 days after receipt of the request. If the covered entity is unable to act on the request for amendment within the time period, it may exercise a 30 day extension.

3. Implementation specifications: accepting the amendment (65 *Fed. Reg.* 82462, 82558, 82825):

   a. If a covered entity accepts an individual's request for amendment, it must make the proposed amendment. At a minimum, it must identify the records in the designated record set that are affected by the amendment and append them or otherwise provide a link to the amendment. Covered entities are not required to expunge any protected health information, but they may do so if it is consistent with other laws and the covered entity's record-keeping practices.

   b. In its commentary, HHS states that a covered entity must obtain an individual's permission before sharing amended information with certain persons. If the individual agrees, the covered entity must make reasonable efforts to provide a copy of the amendment within a reasonable time to:

      (1) Persons the individual identifies as having received protected health information and needing the amendment.

      (2) Persons, including business associates, that the covered entity knows may have unamended information and who may have relied, or could foreseeably rely, on the information to the detriment of the individual.

4. Implementation specifications: denying the amendment (65 *Fed. Reg.* 82462, 82559, 82825):

   a. A covered entity that denies a request for amendment (in whole or in part), must provide the individual a timely, written denial. The denial must be in plain language and should cover the basis for the

denial and discuss the individual's right to submit a written statement disagreeing with the denial along with information on how to file such a statement. The written denial must also provide a statement on how future disclosures will be handled if the individual chooses not to submit a statement of disagreement. Instructions for complaining about the denial to the covered entity or to the Secretary must also be provided.

b. An individual may submit a statement of disagreement (of reasonable length) to the covered entity.

c. A covered entity may prepare its own written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, a copy must be given to the individual.

d. As appropriate, the covered entity must keep proper recordkeeping of a request for amendment, amendments made, statements of disagreement submitted, and rebuttal statements issued.

e. When handling future disclosures, a covered entity must provide either the material that has been appended or (at the election of the covered entity), an accurate summary of such information.

5. Implementation specifications: documentation (65 *Fed. Reg.* 82462, 82559, 82825):

a. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain documentation and required under the administrative requirements of the rule.

N. § 164.526 Accounting of disclosures of protected health information (65 *Fed. Reg.* 82462, 82559, 82826):

1. Standard: right to an accounting of disclosures of protected health information (65 *Fed. Reg.* 82462, 82559, 82826):

a. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity (including disclosures by or to a business associate of the covered entity), for the six years prior to the date on which the accounting is requested. The accounting may be for purposes other than treatment, payment, and health care operations. This right to an accounting is subject to certain exceptions.

b. An individual may request an accounting of disclosures for a time period of less than six years of the date of the request.

c. In addition to treatment, payment and health care operations, several other exceptions (e.g., disclosures made for the facility's directory or for national security purposes) are listed in the rule.

d. Notably, a covered entity must suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for a time period specified by the agency or official, if the agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities.

2. Implementation specifications: content of the accounting (65 *Fed. Reg.* 82462, 82560, 82826):

a. A covered entity must provide the individual with a written accounting that meets the following requirements:

(1) It must include the disclosures made in the six years prior to the date of the request (unless a shorter period is requested).

(2) The accounting must include (i) the date of the disclosure, (ii) the name of the entity or person who received the protected information and their address, if known.

(3) A brief description of the protected information disclosed.

(4) A brief statement of the of the purpose of the disclosure that reasonably informs the individual or the basis of the disclosure.

3. Implementation specifications: provision of the accounting (65 *Fed. Reg.* 82462, 82559, 82826):

a. A covered entity must act upon an individual's request for an accounting no later than 60 days after receipt of such a request.

b. If the covered entity is unable to provide the accounting within 60 days, they may extend the time period for response for an additional 30 days provided that (i) they provide the individual with a written statement of the reasons for the delay and provide the date by which the covered entity will provide the accounting.

c. A covered entity must provide the first accounting to an individual in any 12 month period without charge. A reasonable, cost-based fee may be charged for each subsequent request for an accounting by the same individual within the same 12 month period, provided that the covered.

4. Implementation specifications: documentation (65 *Fed. Reg.* 82462, 82561, 82826):

a. A covered entity must document and retain documentation of the information required to be included in an accounting. The covered entity must also retain a copy of any accounting provided and must document the titles of persons or offices responsible for receiving and processing requests for an accounting.

O. § 164.526 Administrative requirements (65 *Fed. Reg.* 82462, 82561, 82826):

1. Standard: personnel designations

a. A covered entity must designate a privacy officer who is responsible for the development and implementation of the policies and procedures of the entity.

b. As discussed in the commentary of the rule, in the case of affiliated entities:

(1) If a subsidiary is defined as a separate covered entity under the rule, then a separate privacy officer and contact person is required.

(2) If several subsidiaries are designated as a single covered entity, then together they need have only a singe privacy officer and contact person.

(3) If several covered entities share a notice for services provided on the same premises, the notice need designate only one privacy official and contact person for the information collected under that notice.

c. A covered entity must also designate a contact person or office who is responsible for receiving complaints under this section of the rule.

d. Although not specifically addressed in the Final Rule, in the accompanying commentary, HHS indicates that the contact can be,

but is not required to be, the person also designated as the privacy official.

2. Standard: training (65 *Fed. Reg.* 82462, 82561, 82826):

   a. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information as necessary for members of the workforce to carry out their functions within the covered entity. As indicated in the commentary, documentation that training has been provided should be maintained.

   b. The training must be provided to existing members of the workforce no later than the compliance date for the covered entity.

   c. Training for new employees must be provided "within a reasonable period of time after the person joins the covered entity's workforce."

3. Standard: safeguards (65 *Fed. Reg.* 82462, 82561, 82827):

   a. A covered entity must have appropriate administrative, technical and physical safeguards in place to protect the privacy of protected health information.

4. Standard: complaints to the covered entity (65 *Fed. Reg.* 82462, 82561, 82827):

   a. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures under this rule or its compliance with these policies and procures.

5. Standard: sanctions (65 *Fed. Reg.* 82462, 82561, 82827):

   a. Under the Final Rule, a covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.

6. Standard: mitigation (65 *Fed. Reg.* 82462, 82562, 82827):

   a. To the extent practicable, a covered entity must mitigate the harmful effects (that is known) of any use or disclosure of information that is made (by the covered entity itself or its business associates) in violation of the covered entity's policies and procedures, or this subpart.

7. Standard: refraining from intimidating or retaliatory acts (65 *Fed. Reg.* 82462, 82563, 82827):

    a. A covered entity may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against individuals or other persons for filing a complaint under this section; testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing; or opposing any act of policy that the individual or person believes is unlawful.

8. Standard: waiver of rights (65 *Fed. Reg.* 82462, 82563, 82826):

    a. A covered entity may not require that an individual waive their rights under this section as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

9. Standard: policies and procedures (65 *Fed. Reg.* 82462, 82563, 82827:

    a. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of the subpart.

    b. As the commentary discussed, the policies and procedures must be reasonably designed, taking into account the size of the covered entity and the nature of the activities undertaken by the covered entity that relate to protected health information.

    c. Changes to policies and procedures must be made promptly as necessary and appropriate to comply with changes in the law.

10. Standard: documentation (65 *Fed. Reg.* 82462, 82563, 82828):

    a. A covered entity must maintain documentation of its policies and procedures required by this regulation in writing. Any other communication, action, activity or designation that must be documented under this regulation must also be in writing.

    b. The term "writing" includes electronic storage. Paper records are not required.

    c. Covered entities must retain any documentation required under this rule for at least six years from the date of the creation of the documentation, or the last date that the document was in effect, whichever comes last.

11. Standard: group health plans (65 *Fed. Reg.* 82462, 82563, 82828):

a. A group health plan that provides benefits solely through an issuer or HMO, and that does not create, receive, or maintain information other than summary health information or information regarding enrollment or disenrollment, is not subject to the requirements of this section regarding designation of a privacy official and contact person, workforce training, safeguards, complaints, mitigation, or policies and procedures.

b. Such a group is only subject to the requirements of this section documentation with respect to its plan contents.

P. § 164.532 Transition procedures (65 *Fed. Reg.* 82462, 82564, 82828):

1. Standard: effect of prior consents and authorizations (65 *Fed. Reg.* 82462, 82564, 82828):

a. A covered entity may continue to use or disclose protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with the "consent" or "authorization" sections of the rule.

2. Implementation specification: requirements for retaining effectiveness of prior consents and authorizations (65 *Fed. Reg.* 82462, 82563, 82828):

Q. § 164.534 Compliance dates for initial implementation of the privacy standards (65 *Fed. Reg.* 82462, 82565, 82829 as amended at 66 Fed. Reg. 12433, 12434.):

1. A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

2. A health plan must comply with the applicable requirements of this subpart as follows:

a. Health plans other than small health plans: April 14, 2003.

b. Small health plans: April 14, 2004.

c. Health care clearinghouses: April 14, 2003.

R. Office for Civil Rights: statement of delegation of authority (65 *Fed. Reg.* 82381):

1. The Director, Office for Civil Rights (with authority to re-delegate) is granted the following authorities by the Secretary, HHS:

a. The authority under section 262 of HIPAA, Public law 104-191, as amended, to the extent that these actions pertain to the "Standards for the Privacy of Individually Identifiable Health Information", to (i) impose civil monetary penalties under section 1176 of the Social Security Act, for a covered entity's failure to comply with certain requirements and standards, and (ii) make exception determinations concerning when provisions of state laws that are contrary to the federal standards are not preempted by the federal provisions.

b. The authority under section 264 of HIPAA, to administer the regulations "Standards for the Privacy of Individually Identifiable Health Information", 45 CFR Part 164, as these requirements pertain to Part 164, and to make decisions regarding the interpretation and enforcement of these Standards and Administrative Requirements.

S. Penalties for violation:

1. The Final Rule does not cover penalties for non-compliance or for knowing violations of the regulation. Civil and criminal penalties are set forth in the HIPAA statute.

a. Civil violations: No more than $100 per person, per violation, or no more than $25,000 per person for violations of a single standard within a calendar year. 42 U.S.C §1320d-5.

b. Criminal violations: Providers who "knowingly" obtain or disclose individually identifiable health information may be fined no more than $50,000 and/or imprisoned for up to one year. In addition, if the offense is committed under "false pretenses", a fine of not more than $100,000, and/or imprisonment for up to 5 years may be assessed. If the offense is committed with intent to sell, transfer or use the privacy information for commercial advantage, personal gain or malicious harm, a fine of not more than $250,000 and/or imprisonment of up to 10 years may be assessed. 42 U.S.C §1320d-6.