Final Rule for Standards for Privacy of Individually Identifiable Health Information

Analysis by the American Health Information Management Association Policy and Government Relations Team

Amid fanfare that included a presidential address, the Department of Health and Human Services (DHHS), released the final rule [Rule or Privacy Rule] for "Standards for Privacy of Individually Identifiable Health Information" in December 2000. The rule, which has been controversial since its beginnings, is the second administrative simplification regulation to be released as a result of the 1996 Health Insurance Portability and Accountability Act (HIPAA) Public Law 104-191.

AHIMA's analysis will cover the rule itself, any expected effects on health information management (HIM), and resources for further information, training, and implementation. HIM professionals should note that the rule contains both procedural and "legal" requirements and has a compliance date two years after its effective date. The rule is also substantially different than that proposed by DHHS in November 1999. Given the controversy and attention this rule continues to receive, it is very possible that there could be changes to the rule before it is actually implemented. While it would not be prudent to wait to begin implementing this Rule readers are encouraged to regularly monitor AHIMA's Web site for any developments, changes, delays, or additions that might occur over the next few years. AHIMA will continue to keep you posted.

While this analysis highlights much of the 367 pages in the final rule, it is not a substitute for a close review of the entire rule. The rule was written by a large group of federal staff members with both complementary and contrasting styles. Many parts of the Rule are very detailed and somewhat confusing. This analysis attempts to provide a nonlegal perspective on such language. There are points within the Rule where this analysis drops or ignores a section because it essentially says: "The rule is to obey the Rule." On the other hand, where appropriate, this analysis contains the exact wording of the Rule in quotations, because the language is what will be used to hold a covered entity accountable.

The actual rule itself is only 31 pages long, but given the detail and legal aspects of the regulation, it will be important to review all sections closely. The final rule was published essentially in four sections:

- Pages 65FR82462—82565 cover background, history, and a section-by-section review of the proposed and final rule. The review assists with specific detail, on any single section of the final rule.
- Pages 65FR82565—82758 cover general comments, section-by-section. Here the discussion responds to more than 50,000 commentaries (grouped). For this particular Rule, this section is well worth your reading time and also provides details that explain the "why" behind some of the final Rule's sections.
- Pages 65FR82758—82798 cover the final regulatory impact analysis. The Secretary of the Department of Health and Human Services (Secretary) is suggesting that the overall costs of implementation will cost the healthcare[1] industry $17.6 billion dollars over ten years. This

section will create significant discussion in the months to come. You will have to decide if you agree with the amounts in question, but this section does provide some thinking about what activities must be implemented over the next several years.

- Pages 65FR82798—82829 cover the final Rule language. Our commentary is primarily based on this section. The language and content constitutes what covered entities must comply with.

This Analysis Includes:

- Information Regarding the Rule Publication

- Effective Dates

- What the Rule Covers

  Application to Specific Entities
    Health Care Provider
      Direct treatment relationship
      Indirect treatment relationship
    Health Care Clearinghouse
    Health Plan
    Business Associate

  Definitions

  Preemption of State [and other] Law[s]
    "Contrary" and "More Stringent"

  Uses and Disclosure of Protected Health Information: General Rules
    Minimum Necessary
    Organized Health Care Arrangement
    Payment

  Uses and Disclosures of De-Identified Protected Health Information
    Uses and Disclosures to Create De-Identified Information
    De-Identification of PHI
    Disclosures to Business Associates
    Rules Related to Individuals or Parties
    Uses and Disclosures Consistent With Notice
    Disclosures by Whistleblowers and Workforce Member Crime Victims
      Disclosures by Whistleblowers
      Disclosures by Workforce Members Who Are Victims of a Crime

  Uses and Disclosures: Organizational Requirements
    Hybrid Entities
    Affiliated Covered Entities

Business Associate Contracts
Requirements for Group Health Plans
Requirements for a Covered Entity with Multiple Covered Functions

Consent for Use or Disclosures to Carry Out Treatment, Payment, or Health Care Operations
Consent Requirement
Resolving Conflicting Consents and Authorizations
Joint Consents

Uses and Disclosures for Which an Authorization Is Required
Authorizations for Uses and Disclosures
Psychotherapy Notes

Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
Use and Disclosure for Facility Directories
Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes
Use and Disclosure for Disaster Relief Purposes

Use and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required
Uses and Disclosure Required by Law
Uses and Disclosure for Public Health Activities
Disclosure About Victims of Abuse, Neglect or Domestic Violence
Uses and Disclosures for Health Oversight Activities
Disclosures for Judicial and Administrative Proceedings
Disclosure for Law Enforcement Purposes
Uses and Disclosures About Decedents
Uses and Disclosures for Research Purposes
Uses and Disclosures to Avert a Serious Threat to Health or Safety
Uses and Disclosure for Specialized Government Functions
Correctional Institutions and Other Law Enforcement Custodial Situations
Disclosure for Workers' Compensation
Presidential Executive Order: To Protect the Privacy of Protected Health Information in Oversight Investigations

Other Requirements Relating to Uses and Disclosures of Protected Health Information
Uses and Disclosures of PHI for Marketing
Uses and Disclosures for Fundraising
Uses and Disclosures for Underwriting and Related Purposes
Verification Requirement

Notice of Privacy Practices for Protected Health Information
Notice of Privacy Practices—Right to Notice

Rights to Request Privacy Protection for Protected Health Information

Right of an Individual to Request Restriction of Uses and Disclosures of PHI
Confidential Communication Requirements

Access of Individuals to Protected Health Information
Access to PHI—Right of Access

Amendment of Protected Health Information
Right to Amend

Accounting of Disclosures of Protected Health Information
Right to an Accounting of Disclosures of PHI

Administrative Requirements
Personnel Designations—*Privacy Officer*
Training
Safeguards
Complaints to the Covered Entity
Sanctions
Mitigation
Refraining From Intimidating or Retaliatory Acts
Waiver of Rights
Policies and Procedures
Changes to Policies or Procedures
Change in Law
Documentation
Group Health Plans

Modifications

Transition Provisions
Effect of Prior Consents and Authorizations

Compliance and Enforcement

Complaints to the Secretary

Secretarial Action Regarding Complaints and Compliance Reviews

- Reaction to AHIMA's Previous Comments
- Background and History
- Resources

Information Regarding the Rule Publication

Titled "Standards for Privacy of Individually Identifiable Health Information," the Rule can be found in the *Federal Register,* Vol. 65, No. 250, Pages 82462-82829, published on Thursday, December 28, 2000. Two companion notices were published in the *Federal Register:*

- Tuesday, December 26, 2000—Executive Order 13181 "To Protect the Privacy of Protected Health Information in Oversight Investigations" (65FR81321)[2], and
- Friday, December 29, 2000—"Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000" (65FR82944).

Copies of the *Federal Register* can be purchased individually from the Superintendent of Documents. However, it will take several weeks to receive a copy.[3] A much easier way to obtain a copy is to access the *Federal Register* and Government Printing Office Web site at http://www.access.gpo.gov/su_docs/fedreg/a001228c.html. Downloading the Rule requires the use of Adobe Acrobat Software, which is available for free at the GPO Web Site http://www.access.gpo.gov/su_docs/aces/aces140.html The software is safe to download and use. Access to the Rule will also be available at other Web sites listed in the "resource" section of this analysis.

Similar access to the two companion documents can be found at:
http://www.access.gpo.gov/su_docs/fedreg/a001226c.html for the Executive Order and
http://www.access.gpo.gov/su_docs/fedreg/a001229c.html for the Technical Corrections.

Effective Dates

While this final Rule was published on December 28, 2000, it's effective date, originally posted as February 26, 2001, now stands as April 14, 2001. The change in dates was due to a technical error made by DHHS that was not corrected until mid-February. Congress could technically rescind or change the legislation sustaining the Rule. While there has been much debate on the Rule, it does not appear that the effective date will be changed at this writing.

Presuming that the Rule's effective date is not delayed, the implementation dates, or "compliance by" dates will be (§164.534) April 14, 2003 for all covered entities except those designated as "small health plans,"[4] whose "compliance by" date will be February 26, 2004.

What the Rule Covers

Application to Specific Entities

Essentially, the Rule (§160.102) covers the three entity groups mentioned specifically in HIPAA and in the previously published Transactions and Code Sets (TCS) rule. The "covered entities" are:

- Health plans
- Clearinghouses
- Providers

The Rule further states (§164.500) that "except as otherwise provided herein, the standards, requirements, and implementation specifications of this..[Rule]..apply to covered entities with respect to protected health information [PHI]."

It must be noted however that §164.104 on applicability states: "Except as otherwise provided, the provisions of this part apply to covered entities: health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act [HIPAA].

{This section is causing some debate, but the common interpretation, at this point in time, is that the Rule's requirements with respect to privacy, depend on whether a covered entity is performing any of the electronic transactions identified in HIPAA, directly or indirectly. It is possible that there are some entities not involved in any of the HIPAA electronic transactions, and are therefore not covered by this rule. The number of such entities (most likely healthcare providers) is considered very low and could change at any time if one or more plans require electronic transactions.}

The Privacy Rule depends greatly on the definitions and functions of these covered entities (§160.103) and entities that are indirectly covered by the Rule. Therefore it is important to review the applicable definitions contained in the Rule.

Covered Entities

Healthcare Provider

The *covered entity* definition remains fundamentally the same (65FR82799 & 82476) . For *healthcare provider*(s) it is noted that such a provider "transmits any health information in electronic form in connection with a transaction covered by" HIPAA. Note that while this definition qualifies which providers are covered, later in the Rule it is clarified that *all* individually identifiable health information, no matter its media, is covered under the Rule. Furthermore, it is important to remember that entities cannot become uncovered by shifting electronic transactions to a business associate. To assist providers in clarifying their status, the preamble of the rule also details the definition of a healthcare provider (65FR82478), while the final rule language only provides statutory reference.

Healthcare providers are also defined in this Rule by their treatment relationship. ***Direct treatment relationship*** (§164.501) is defined to mean "a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship." ***Indirect treatment relationship*** (§164.501) is defined as "a relationship between an individual and a health care provider in which:

- The health care provider delivers health care to the individual based on the orders of another health care provider; and
- The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual."

Several examples of these definitions are included in the preamble to the Rule (65FR82492).

Healthcare Clearinghouse

The Rule (§160.103) provides a new definition for ***health care clearinghouse:*** "a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and 'value-added' networks and switches, that does either of the following functions:"

- "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"
- "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."

The Rule (§164.500) also clarifies the role or roles of healthcare clearinghouse and when they become covered entities. The Rule notes that "health care clearinghouses must comply with the standards, requirements, and implementation specification as follows:

- When a health care clearinghouse creates or receives protected health information (PHI) as a business associate of another entity" it must comply with the Rule "except that a clearinghouse is prohibited from using or disclosing PHI other than as permitted in the business associate contract under which it created or received the PHI."
- When the healthcare clearinghouse is acting as a covered entity "including the designation of [a] health care component of a covered entity."
- "When relating to uses and disclosures for which consent, individual authorization, or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing PHI other than as permitted in the business associate contract under which it created or received the PHI."

Note that in this instance, information is exchanged with another entity. Some of these functions could be done in-house and therefore would not constitute a clearinghouse function. In the Rule's preamble (65FR82477), the Secretary details that some entities that are often considered clearinghouses will not be considered covered entities. "Telecommunication entities that provide connectivity or mechanisms to convey information such as telephone companies and Internet Service Providers, are not health care clearinghouses as defined in the rule, unless they actually carry out the functions outlined" above. Value-added networks and switch services likewise fall into entities that probably are not covered.

{The clearinghouse issue is important. Clearinghouses could, based on the applicability references above, define if a health plan or provider is covered under this Rule. Page 65FR82488 also provides some additional information.}

Health Plan

The definition of *health plan* remains essentially the same as in HIPAA and the NPRM.[5] There are, however, a few categories added due to the Balanced Budget Act (BBA) or failure to include them in the past, such as high-risk health insurance pools. The Rule has significant impact on health plans and their sponsors or customers, so it is important to note some of the exclusions from the definition such as:

- Group health plans with less than 50 participants that are not administered externally from the employer as defined by ERISA;

- Workers compensation plans; and
- Certain liability plans and government agencies.

Business Associate

Business Associate is defined (§160,103—65FR82798) by its relationship to one of the covered entities and the functions that it performs in that relationship (or independently). An entity that is a business associate in one case could also be one of the three covered entities in another.

With respect to a covered entity or an "organized health care arrangement," a business associate is a person:

- Who is not a member of the workforce of the covered entity.
- Performs a function or activity involving the use or disclosure of individually identifiable health information, including (but not limited to) one or more of the following:
  - Claims processing or administration,
  - Utilization review,
  - Quality assurance,
  - Billing,
  - Benefit management,
  - Practice management,
  - Repricing,
  - Legal,
  - Actuarial,
  - Accounting,
  - Consulting,
  - Data aggregation,
  - Management,
  - Administrative,
  - Accreditation,
  - Financial services, or
  - Any other function or activity covered by the Rule.

This should not be considered an exhaustive list. Clearly, for HIM professionals, we can add functions such as transcription, coding, and release of information to the business associate list.

All entities will have to examine their relationships and functions to determine when they might become a business associate. In the NPRM this entity was called a "business partner." The Rule changes "clarify that the business association occurs when the right to use or disclose the PHI belongs to the covered entity, and another person is using or disclosing the PHI (or creating, obtaining, and using the PHI) to perform a function or activity on behalf of the covered entity." The Rule also clarifies that "providing specified services to a covered entity creates a business associate relationship if the provision of the service involves the disclosure of PHI to the services provider."

It will be important for all suspected covered entities and business associates to closely review their current and future relationships and functions. Such a review, in questionable situations, may need a legal review as well. For instance, the Secretary points out that "the mere fact that

two covered entities participate in an organized health care arrangement does not make either of the covered entities a business associate of the other covered entity."

The preamble, or section-by-section review, discusses the business associate relationship in detail (65FR82475-82476). Included in this discussion are situations where two covered entities are working together, though their relationship may not be as business associates. Key to this discussion is that of a physician or other provider that has staff privileges at an institution. The Secretary notes, "neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other." The discussion goes on to note that parties often have a variety of functions, some of which could be as business associates, such as when or if the institution becomes the billing agent for the physician. (See Disclosures to Business Associates and Business Associate Contracts)

Definitions

Definitions play a key role in the Privacy Rule, and there are a number of definitions provided in the final rule: §160.103 (65FR82798), §160.202 (65FR82800), §164.501 (65FR82803), and §164.504 (65FR82802). Due to their detail, several of the definitions are important components in and of themselves. Key among these definitions (not provided above) are:

- **Common Control** (§164.504): "exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

- **Common Ownership** (§164.504): "exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity."

- **Contrary** (§160.202) means: "when used to compare a provision of State law to a standard requirement, or implementation specification adopted" in this Rule. In such situations:
  - "(1) A covered entity would find it impossible to comply with both the State and federal requirements; or
  - (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA, "as applicable."

- **Correctional Institution** (§164.501): "means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center…for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody…." This definition was added to the rule to support the rule as it addresses *inmates (*"a person incarcerated in or otherwise confined to a correctional institution"). The expanded definition (65FR80803) defines who oversees the institution and "other persons" housed in such facilities.

- **Covered Functions** (§164.501): "means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse." The preamble review (65FR82489) of this definition notes some of the functions that would not be considered as "covered."

- **Data Aggregation** (§164.501): a new definition that "means, with respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities." This definition when applied effectively allows an entity to use data for a variety of what are now common business practices.

- **Designated Record Set** (§164.501) sets the tone for some of the activities and information that is cover in the Rule. It "means:
  - (1) A group of records maintained by or for a covered entity that is:
    - (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
    - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan: or
    - (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - (2) For purposes of [this rule] the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

- **Disclosure** (§164.501): "means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."

- **Health Care** [or healthcare] (§160.103): "means care, services, or supplies related to the health of an individual," including but not limited to the following:
  - (1) "Preventive, 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.

  The preamble (65FR82477) also provides additional government-type definitions of what is included in health care. A key change in the definition is the addition of "assessment" to the list of services under this definition.

- **Health Care Component** (§164.504): means that "components of a covered entity that perform covered functions are part of the health care component" and/or "another component of the covered entity is part of the entity's health care component to the extent that it performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of that component that performs covered functions if the two components were separate legal entities and the activities involve the use or disclosure of PHI that such other component creates or receives from or on behalf of the component that performs covered functions."

- **Healthcare Operations** (§164.501): "means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates
  - (1) Conducting quality assessment and improvement activities…; population-based activities….; and related functions that do not include treatment [full definition at 65FR82803-82804]
  - (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs.….
  - (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care ….
  - (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - (5) Business planing and development….; and
  - (6) Business management and general administrative activities of the entity including … management activities…customer service…resolution of internal grievances…due diligence…"

  {This very long and detailed definition can be found at 65FR82803-82804 and is discussed at length at 65FR82489-82491.}

- **Health Information** (§160.103) a key definition defined as: "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."

  {Note that health information can be oral or recorded. As the Rule plays out, there is the possibility that protected information could be released in oral form. This makes the job of ensuring privacy much more difficult. Also, note that this definition will play a key role in the expansion of this rule beyond electronic health information.}

- **Health Oversight Agency** (§164.501): "means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, 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 laws for which health information is relevant."

- **Hybrid Entity** (§164.504): "means a single legal entity that is a covered entity and whose covered functions are not its primary functions."

- **Individual** (§164.501): "means the person who is the subject of PHI." This definition was changed to eliminate confusion with personal representative, which is defined below. The background discussion on this definition (65FR82492-82493) notes that some records can potentially refer to more than one individual."

- **Individually Identifiable Health Information** (§164.501): "is information that is a subset of health information, including demographic information collected from an individual, and:
  - (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

- **Implementation Specification** (§160.103) is a term used throughout the Rule and means: "specific requirements or instructions for implementing a standard." (see below)

- **Law Enforcement Official** (§164.501): "means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision or a State or territory, or an Indian tribe, who is empowered by law to:
  - (1) Investigate or conduct an official inquiry into a potential violation of law; or
  - (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law."

- The **marketing** definition and concept are receiving much attention. There is a sizable discussion on this issue in the Rule's preamble (65FR82493-82494). The Rule (§164.501) states that **marketing**: "means to make 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." (see more on marketing below****)

- **More Stringent** (§160.202): "means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted " under HIPAA and in the section on Security and Privacy, a sate law that meets one of a number of six criteria (see discussion on Contrary and More Stringent in Preemption below).

- **Plan Administration Functions** (§164.504): "means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan, and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor."

- **Protected Health Information** (§164.501): "means individually identifiable health information…that is:
  - (i) Transmitted by electronic media;

- (ii) Maintained in any medium described in the definition of electronic media …[under HIPAA], or
- (iii) Transmitted or maintained in any other form or medium."

Excluded from *PHI* is education records covered by the Family Educational Right and Privacy Act and other educational records covered under 20 U.S.C. 1232g((a)(4)(B)(iv). Under HIPAA, electronic media means the mode of electronic transmission including the Internet, Extranet, leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disc media." (65FR82496)

In the preamble discussion (65FR82496) the Secretary also discusses that this definition is "set out in this form to emphasize the severability of this provision….we believe we have ample legal authority to cover all individually identifiable health information transmitted or maintained by covered entities." The definition has been structured so that "if a court were to disagree with our [DHHS's] authority in this area, the rule would still be operational, albeit with respect to a more limited universe of information."

- **Psychotherapy Notes** (§164.501): "means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

  Besides content, the key to the definition of *psychotherapy notes* is the requirement that they are *separate* from other information and records. If such *notes* are maintained in another or with another record, they are no longer covered by this definition. This definition is significant in the discussion of consents and authorizations (below).

- **Public Health Authority** (§164.501): "means an agency or authority…or a person or entity acting under a grant of authority from or contact with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." (65FR82805).

- **Relates to the Privacy of Individually Identifiable Health Information** (§160.202) means: "with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial law."

- **Required by Law** (§164.501): a new definition key to the Rule's compliance, this "means a mandate contained in law that compels a covered entity to make a use or disclosure of PHI and that is enforceable in a court of law. *Required by law* includes, but is not limited to court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a

governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand, Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits."

{It is important to note that in its discussion of this definition (65FR82497) DHHS states: "nothing in this rule compels a covered entity to make a use or disclosure required by the legal demands or prescriptions listed in this [definition] clarification or by any other law or legal process, and a covered entity remains free to challenge the validity of such laws and processes.}

- **Research** (§164.501): "means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

  This definition is taken from the "Common Rule" which is the Federal Policy for the Protection of Human Subjects at 45 CFR part 46, subpart A. The term "generalizable knowledge" is not defined in the Rule, but in the preamble (65FR82497) it is defined as "knowledge related to health that can be applied to populations outside of the population served by the covered entity."

- **Standard** (§160.103) in this Rule means: "a rule, condition, or requirement:
  - (1) Describing the following information for products, systems, services or practices: (i) Classification of components, (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or
  - (2) With respect to the privacy of individually identifiable health information."

- **State** (§160.103) becomes an important definition in this Rule due to the preemption sections. Here *state* "refers to one of the following:
  - (1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.
  - (2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam."

- **State Law** (§160.202): "means a constitution, statute, regulation, rule common law, or other State action having the force and effect of law.

- **Summary Health Information** (§164.504): "means information that may be individually identifiable health information, and that:
  - (1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan;" and
  - (2)" From which specific identifiers defined in the Rule have been deleted with some exceptions for aggregated zip codes."

- **Transaction** (§160.103): "means the transmission [called "exchange" in the NPRM] of information between two parties to carry out financial or administrative activities related to health care" including the transactions as defined in the HIPAA final rules for Transactions and Code Sets.[6]

- **Treatment** (§164.501): "means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. The preamble contains a significant discussion on *treatment* (65FR82497).

- **Use** (§164.501): "means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."

- **Workforce** (§160.103) has significant meaning in the Rule and "means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." It should be noted that in the Rule there are times when personnel employed by a business associate could be considered part of the "workforce."

Preemption of State [and other] Law[s]

{The preemption of state law remains one of the more controversial issues with Privacy. Parties generally disagreed on three specific issues. First, various groups that include AHIMA support complete preemption to establish a uniform national standard for the release and disclosure of health information. The standard would be a federal "ceiling" where states could not enact more stringent laws. Second, a number of groups support the creation of a federal "floor" of protections where a federal standard would exist but states would have the ability to pass something stronger. Finally, various groups believe that the federal government has no constitutional authority to enact any type of federal privacy rule. This is the "states rights" position.

HIPAA was limited in its ability to preempt state laws. The legislative language specifically provided for establishing a federal "floor" of protections where states can enact more stringent health information privacy protections. Therefore, the December 28, 2000 Rule did not solve the preemption issue in accordance with AHIMA's position. The Rule, in accordance with HIPAA's legislative language, created a federal "floor" of protections.}

General Rule and Exception

The Rule states (§160.203) that "a standard, requirement, or implementation specification adopted under the [Rule] that is contrary to a provision of State law preempts the provision of State law." This general rule applies, except if one or more of the following conditions is met:

- "A determination is made by the Secretary [See: Exception Determinations below] that the provision of State law:
  - Is necessary;
    - To prevent fraud and abuse related to the provision of or payment for health care;

- To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- For State reporting on health care delivery costs; or
- For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under…[other parts of this Rule]…, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

- Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law." [65FR82801]

{This determination will be made by the Secretary after receiving a request to exempt from a state. Until such an exempt is approved, the preemption of the state law exists. The following three points do not require a request from the state.}

- "Relates to the PHI and is more stringent than a standard, requirement, or implementation specification adopted under…[this Rule]."
- "Provides for the reporting of disease or injury child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention [under procedures established by such law]."
- "Requires a health plan to report, or to 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."

Process for Requesting Exception Determinations

The Rule (§160.204) indicates that a request to exempt a provision of state law from preemption may be submitted to the Secretary. The request must be submitted through the chief elected official of the state or his or her designee. The request must be in writing and include the following information:

- The state law for which the exception is requested;
- The particular standard, requirement, or implementation specification [in this Rule] for which the exception is requested;
- The part of the standard or other provision [of the Rule] that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
- How healthcare providers, health plans, and other entities would be affected by the exception;
- The reasons by which the State law should not be preempted by the federal standard, requirement, or implementation specification [of this Rule], including how the State law meets one or more of the criteria [first listed under "general rule and exception" above].
- Any other information the Secretary may request in order to make the determination.

Requests for exception must be submitted to the Secretary. "Until the Secretary's determination is made, the standard, requirement, or implementation specification under this [Rule] remains in effect." The Secretary's determination …"will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the [acceptable under the Rule] criteria has been met."

{As this Rule is newly published, it is unclear to what extent, and how, the Secretary will allow public comment into the decisions allowed here. Other modifications under HIPAA essentially include advisory bodies and published requests for comments. This may be the case, but, currently, this is not spelled out.

Since exceptions to exemption and all the preemption issues are statewide, HIM professionals and covered entities interested in the impact of the Rule with state law should be working with state associations and the state's attorney general or similar officer to review situations where conflicts might exist. Federal legislation may also be forthcoming that would add to or decrease what aspects of the Rule are open to preemption.}

Duration of Effectiveness of Exception Determinations

Once an exception is granted by the Secretary, it remains in effect until either the state law or the federal standard, requirement, or implementation specification [of this Rule] that provided the basis for the exception is materially changed, such that the ground for the exception no longer exists. The Secretary can also revoke the exception based on a determination that the ground supporting the need for the exception no longer exists.

{Relation to Other Federal Laws:

The Rule does not generally refer to other federal statutes and regulations. In the preamble to the Rule (65FR82481) there is an extended discussion with regard to potential overlaps. In this discussion DHHS suggests that there should be few conflicts, and that many times one rule might state may while another states must; leading to a situation where must overides may and, according to DHHS, therefore resolves the conflict. Readers should note that this same situation exists between the Rule and some state laws as well.

In the discussion on other federal statutes and regulations that interact with the Rule, DHHS lists several situations were federal statutes might be considered overlapping. We list them here for your benefit, although we will not provide any analysis regarding the potential interaction. The rules listed include (we note the 65FR page where discussion occurs):

- *The Privacy Act of 1974 (5 U.S.C.)—65FR82482*
- *The Freedom of Information Act (5 U.S.C.)—65FR82482*
- *Federal Substance Abuse Act—Confidentiality Requirements (42 U.S.C.)—65FR82482*
- *Employee Retirement Income Security Act of 1974 (ERISA) (29 U.S.C.)—65FR824883*
- *The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.)—65FR82483*
- *Gramm-Leach-Bliley (Pub.L. 106 -- 102)—65FR82483*
- *Various federally funded health programs' requirements—65FR82484*
- *Food, Drug, and Cosmetic Act(FDA) (21 U.S.C.)—65FR82484*
- *Clinical Laboratory Improvement Amendments (CLIA)(42 U.S.C.)—65FR82485*
- *Other Mandatory Federal or State Laws—65FR82485*
- *Federal Disability Nondiscrimination Laws—65FR82485*
- *US Safe Harbor Privacy Principles—65FR82486}*

"Contrary" and "More Stringent"

The definitions for *contrary* and *more stringent* were listed above. *Contrary* is specified when comparing a state law to a standard, requirement, or implementation specification under this Rule, the covered entity would find it impossible to comply with both requirements and or "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub.L. 104-191, as applicable." (HIPAA).

The term *more stringent* comes into play (§160.202) when a State law meets one or more of the following criteria with respect to:

- **Use or Disclosure** -- The State law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this Rule with two exceptions:
  - The disclosure is required by the Secretary to determines a covered entity's compliance with the Rule, or
  - The disclosure is to the individual who is the subject of information.
- **Rights of an Individual** -- who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that nothing in this [Rule] may be construed to preempt any state law to the extent that it authorizes or prohibits disclosure of PHI about a minor to a parent, guardian, or person acting in *loco parentis* of such minor.
- **Information to be Provided to an Individual** -- who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
- **Form or Substance of an Authorization or Consent --** for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.
- **Recordkeeping or Requirement Relating to Accounting of Disclosures --** provides for the retention or reporting of more detailed information or for a longer duration.
- **Any other Matter** -- provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

{Patently, this preceding section is very legalistic. Covered entities will need to work with their state associations and representatives of the state to determine if there are situations that ought to be defined and determine, with regard to "more stringent," so that such issues are identified and resolved as soon as possible.}

Uses and Disclosure of Protected Health Information: General Rules

Standard: General

DHHS takes the approach to privacy-based on who, when, and under what circumstances protected health information (PHI) can and cannot be used. To further clarify the Rule's intent, it has been written as a series of standards. The standards for Use and Disclosure will be presented, for the most part, in the order they appear in the final rule. [65FR82805]

Permitted Use and Disclosure of Protected Health Information

The Rule indicates at section 164.502 a variety of situations where a covered entity can use or disclose PHI, and it covers when a covered entity is required to disclose PHI. Each situation points to other sections of the Rule, which are listed throughout situations explained below.

Standard: Minimum Necessary

[When] Minimum Necessary Applies

The Rule introduces the concept of minimum necessary as applied to the use, disclosure, and request for PHI. The Rule (§164.502(b)) states that "when using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [65FR82805 & 65FR82819]

{This was one of the items specifically addressed by AHIMA's comments to DHHS. AHIMA members expressed concerns over requests for disclosure that typically asked for more PHI than was actually needed. It appears that this comment was heard.}

[When] Minimum Necessary Does Not Apply:

The requirement for minimum necessary does not apply to:

- Disclosure to or a request by a healthcare provider for treatment purposes.
- Uses or disclosures made to or by the individual, except when certain authorizations exist (see Uses and Disclosures for Which an Authorization Is Required), access is limited (see Access of Individuals to Protected Health Information), or other prohibitions exist (see Accounting of Disclosures of Protected Health Information).
- Disclosures made in response to a request from the Secretary to investigate or determine the covered entity's compliance.
- Uses or disclosures are required by law (see Uses and Disclosures for Which Consent, Authorization, or Opportunity to Agree or Object Is Not Required).

Specification: Minimum Necessary Use Requirements

With respect to the uses of PHI, a covered entity must make reasonable efforts (§164.514) to identify:

- Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties;
- (For each such person or class of persons) the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Once such identification takes place, a covered entity is expected to make reasonable efforts to limit the access of such persons or classes identified with respect to the category or categories of the PHI.

{Significant concern was levied, especially by consumer groups, that too many persons had access to medical records and PHI. This access and the need for access varies from entity to entity. This part of the Privacy rule will require coordination with the HIPAA security rules when they are released. Covered entities will have to look at all classes of employees, volunteers, and so forth and determine policies and procedures -- and even computer access requirements -- for access to PHI information, and when. The Rule does not dictate who should have what access; that will vary by entity. Each entity, however, will have to document its decisions and will be expected to enforce its policies and procedures.}

Specification: Minimum Necessary Disclosures

Again, with respect to PHI, a covered entity (§164.514) is expected to:

- Develop and implement reasonable "policies and procedures ("which may be standard protocols") that limit the PHI disclosed "on a routine and recurring basis" to the amount reasonably necessary to achieve the purpose of the disclosure."
- Develop reasonable "criteria designed to reasonably limit the items of PHI disclosed to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria."

A covered entity is permitted to assume that a request is for the minimum necessary information when:

- Making disclosures to public officials is permitted, (see Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required) "the public official represents that the information requested is the minimum necessary for the stated purpose(s);"
- "The information is requested by another covered entity;"
- "The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s);" or
- "Documentation or representations that comply with the applicable requirements for" authorizations that "have been provided by a person requesting the information for research purposes."

Specification: Minimum Necessary Requests

A covered entity (§164.514) must limit any request for PHI to that "which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities." When such a request is made on a "routine and recurring basis" a covered entity [in this case the requestor] must develop and implement policies and procedures ("which may be standard protocols") that "limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made." When the request is not routine or recurring, the covered entity is expected to review the (each) request "to determine that the PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made."

{Note that when PHI is exchanged between covered entities, it is the requestor that is given the responsibility of determining what is minimally necessary. This could affect the ongoing dialogue between healthcare plan/payers and providers, that will not be resolved until most of the HIPAA electronic transactions are fully in use within the industry.}

Specification: Other Content Requirement

Finally, the Secretary reiterates that a "covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request."

{As we continue the discussion on use, disclosures, and requests, it is appropriate to cover two other elements that are in the Rule, "organized health care arrangement" and "payment."}

Organized Healthcare Arrangement

"Organized health care arrangement is defined (§164.501) as meaning:

- A clinically integrated care setting in which individuals typically receive health care from more than one health care provider, and
- An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
  - Hold themselves out to the public as participating in a joint arrangement, and
  - Participate in joint activities that include at least one of the following:
    - *Utilization review*, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    - *Quality assessment and improvement activities*, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - *Payment activities,* if the financial risk for delivering health care is shared in part or in whole by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk;
- A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance insurer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
- A group health plan and one or more other group health plans, each of which are maintained by the same plan sponsor; or,
- The group health group health plan described just above and health insurance issuers or HMO with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans."

Payment

Payment means:

- "The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care;" and
- "The activities of these plans or providers related to the individual to whom health care is provided and including , but not limited to:
  - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost-sharing amounts), and adjudication or subrogation of health benefit claims;
  - Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    - Name and address:
    - Date of birth;
    - Social security number;
    - Payment history;
    - Account number; and
    - Name and address of the health care provider and/or health plan."

Uses and Disclosures of De-Identified Protected Health Information

Standard: Uses and Disclosures to Create De-Identified Information

The Rule (§164.502(c)) states "a covered entity may use PHI to create information that is not individually identifiable health information or disclose PHI only to a business associate for such purpose, whether or not the de-identified information is to by used by the covered entity." (65FR82806)

Uses and disclosures of De-Identified Information

"Health information that meets the standard and implementation specifications for de-identification [see below] is considered not to be individually identifiable health information" and is therefore "de-identified." "The requirements of this ..[Rule]..do not apply to information that has been de-identified," If however, there is the use of a code or other means to identify the information, the information is then considered covered by the Rule.

De-Identified Information

DHHS specifies (§164.514) how health information can be shared without an authorization when it discusses its standard for "de-identification of PHI under its "Other Requirements" section. [65FR82818]

Standard: De-Identification of PHI

"Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."

Specification: Requirements for De-Identification of PHI

The Rule presents alternatives to ensure that information is de-identified. The first option (called a "safe harbor" in the preamble) is for the covered entity to strip the information of certain data listed in the rule including:

- Names of the individual, and relatives, employers or household members of the individual
- Geographic identifiers of the individual, et. al. including:
    - Subdivisions smaller than a state
    - Street addresses

  - City
  - County
  - Precinct
- Zip code—at any level less than the initial three digits (e.g. NNNxx-xxxx). However, if the initial digits cover a geographical area of 20,000 or less people, then it has to be reported as 000.
- "All elements of dates (except year) or dates directly related to an individual, including:
  - Birth date,
  - Admission date
  - Discharge date
  - Date of death, and
  - All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older."
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serials numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IO) address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code"

Once these data items are removed, the covered entity must also attest that it has "no actual knowledge" that the information could be used alone or in combination to identify a subject of the information.

In lieu of stripping off all these identifiers, the rule requires the covered entity to ensure or determine that health information is not identifiable, by requiring (§164.514(b)) that an expert, with appropriate knowledge and experience, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, make a determination that the [actual language at 65FR82818)] "risk is very small that the information [in question] could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information."

The covered entity will need to document the analysis and the results in case it must justify this determination. [see the preamble at 65FR82543 for additional information]

The covered entity can assign a code "or other means" ((§164.514 (c)) to de-identified information to allow for re-identification provided that:

- (Derivation) "the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated to as to identify the individual."
- (Security) "the covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification." [65FR82819]

{If an entity can de-identify its information subject to one or more of the alternatives above, then it is no longer PHI and not subject to the requirements of this rule. While these alternatives may not be easy, they need to be compared to the steps the entity must take to use PHI, especially if it is a situation that requires an authorization.}

Standard: Disclosures to Business Associates

The Rule (§164.502 (e)) indicates that "a covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information." (See Business Associate and Business Associate Contracts)

Specification: Documentation

The covered entity "must document the satisfactory assurances required…through a written contract or other written agreement or arrangement with the business associate that meets the requirements of" the Rules section on business associate contracts.

The Rule goes on to note that "a covered entity that violates the satisfactory assurances it provided as a business associate or another covered entity will be in noncompliance with" not only with the standards, implementation specifications, and requirements of the Rule, but also with the requirements related to business associate contracts [see below].

Rules Related to Individuals or Parties

{The Rule, at this point, discusses uses and disclosures of certain individual's PHI to certain parties that are identified in other sections of the Rule and this commentary. Unless specific content were discussed, at this point we will only identify the individual situation and hold discussion until a more appropriate place.}

The rule notes the following individuals or parties in its discussion [at §164.502]:

- **Specification: Adults and emancipated minors—**"If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under..[this Rule]..with respect to PHI relevant to such personal representation."

- **Specification: Unemancipated minors—**"If under applicable law a parent, guardian, or other person acting in *loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must

treat such person as a personal representative under this..[Rule], with respect to PHI relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to PHI pertaining to health care services if:
- The minor consents to such health care service; no other consent to such health care services is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
- The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in *loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or
- A parent, guardian, or other person acting in *loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service."

· **Specification: Deceased individuals—**"If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this..[Rule], with respect to PHI relevant to such personal representation."

· **Specification: Abuse, neglect, endangerment situations --** "Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:
- the covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and
- The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative."

Standard: Uses and Disclosures Consistent with Notice

A covered entity that is required…to have a Notice may not use or disclose PHI in a manner inconsistent with such Notice. A covered entity that is required…to include a specific statement in its Notice, if it intends to engage in an activity listed in [the Notice requirements] may not disclose PHI for such activities, unless the required statement is included in the Notice.

Standard: Disclosures by Whistleblowers and Workforce Member Crime Victims

Disclosures by Whistleblowers
The Rule indicates (§164.502 (j)) that "a covered entity is not considered to have violated the requirements of..[the Rule] if a member of its workforce or a business associate discloses PHI, provided that:
· The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical

standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

· The disclosure is to:
  - A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
  - An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct under scrutiny."

Disclosures by Workforce Members Who Are Victims of a Crime

"A covered entity is not considered to have violated the requirements of..[this Rule]..if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the criminal act and the PHI disclosed is limited to the Rules standard for release of information to law enforcement.

{This discussion is very much like some of the language in the Medicare compliance programs. Covered entities should note in policies, procedures, and training, the conditions noted above, the internal reporting mechanisms for handling problems, and the sanctions that will be applied if a member of the workforce does not comply with the Rule's requirement (above). At this point, this is the only way the entity will have any control related to a workforce member's activities. These same points and discussions should take place, when appropriate, with business associates as well.}

Uses and Disclosures: Organizational Requirements

Hybrid Entities

Standard/Specification: Healthcare Component

The discussion in this part of the Rule (§164.504) notes that except for where it is specifically noted, when dealing with a hybrid entity [see Definitions], the requirements of the Rule only apply to the healthcare component(s) of the entity. The discussion also notes that "a reference in such provision(s) to PHI refers to PHI that is created or received by or on behalf of the healthcare component of the covered entity.

Specification: Application of other Provisions

The Rule goes into some detail to note that terms like "covered entity," "health plan," "covered health care provider," and "clearinghouse" when used with requirements, specifications, and the like, apply to the covered component of the hybrid entity should it be performing the functions of such as defined in the Rule.

Specification: Safeguard Requirements

"The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of..[this Rule]." In addition, such a covered entity must ensure that:

- Its healthcare component does not disclose PHI to another component where the Rule would prohibit such a disclosure(s) if the healthcare component and the other component were separate and distinct legal entities.
- A component performing covered functions, defined in this Rule, that would make it a business associate if it were a separate and distinct legal entity, does not disclose PHI to other non-healthcare components.
- If a person performs duties for both the healthcare component, as a member of its workforce, and for a non-healthcare component, such a person must not use or disclose PHI created or received in the course of or incident to the member's work for the healthcare component in a way prohibited by the Rule.

{Given today's healthcare industry, the requirements on hybrid entities will require ongoing attention as the organization reorganizes and as personnel come and go from the "covered" part of the entity. The primary attention of the Rule is to PHI, and while the Rule recognizes that some components of PHI might reside outside the "covered" part of the entity, such an organization must be very careful with regard to any PHI essentially created or received in the "covered" area to ensure that PHI does not cross the line to the non-"covered" part of the entity. This issue will be addressed by the standards below.}

Standard: Affiliated Covered Entities

Section 164.504(d)) indicates that "Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of..[this Rule]."

Specifications: Requirements for Designation of an Affiliated Covered Entity

Legally separate covered entities may designate themselves (including any healthcare component of such covered entity) as a single affiliated covered entity for purposes of this Rule, if all of the covered entities designated are under common ownership or control. The designation of an affiliated covered entity must be documented and the documentation maintained as required [see Documentation below and under Administrative Requirements].

Specifications: Safeguard Requirements

An affiliated covered entity must ensure that its use and disclosure of PHI complies with the applicable requirements of the Rule, and if it combines the functions of a health plan, healthcare provider, or healthcare clearinghouse, it must also comply with the Rule's "Requirements for A Covered Entity with Multiple Covered Functions."

{Covered entities should examine all components of this Rule before deciding whether they should utilize the concept permitted here for affiliation. As you will see in reading the sections on Consents, Authorizations, and Notices, while affiliation might make sense for fulfilling some of the requirement, it might make it very difficult for complying with others. Each requirement should be reviewed to determine if affiliation will or will not work in your situation.}

Standard: Business Associate Contracts

The Rule states (§164.504(e)) that the contract or other arrangement between the covered entity and an entity defined as a business associate by this Rule must also meet the requirements of this Rule. (Also see Business Associate and Disclosures to Business Associate)

A covered entity is not in compliance if it "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 contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation as applicable, and if such steps were unsuccessful:

- Terminated the contract or arrangement, if feasible; or
- If termination is not feasible, reported the problem to the Secretary."

Specification: Business Associate Contract

A contract between the covered entity and a business associate must:

- Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of...[Rule} if done by the covered entity, except that the contract may permit the business to:
  - Use and disclose PHI for the proper management and administration of the business associate.
  - Provide data aggregation services relating to the healthcare operations of the covered entity.
- Provide that the business associate will:
  - Not use or further disclose the information other than as permitted or required by the contract or as required by law;
  - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
  - Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
  - Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
  - Make available PHI in accordance with the Rule's requirements for "Access of Individuals to PHI;"
  - Make available PHI for amendment and incorporate any amendments to PHI in accordance with the Rule's requirements for "Amendment of PHI;"
  - Make available the information required to provide an accounting of disclosures in accordance with the Rule's requirements for "Accounting of Disclosures of PHI;"
  - Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf or, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this [Rule]; and
  - Termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business

associate still maintains in any form and retain no copies of such information, or, if such return or destruction is not feasible, to extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

· Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Specifications: Other Arrangements

· If a covered entity and its business associate are both governmental entities:

- The covered entity may comply with the requirements for a business associate contract by entering into a memorandum of understanding with the business associate that contains the same terms that accomplish the objectives in the contract language required above.
- The covered entity may comply with the business associate contract requirements, if other law (including regulations adopted by the covered entity or its business associates) contains requirements applicable to the business associate that accomplish the objectives in the contract language required above.

· If a business is required by law to perform a function or activity on behalf of a covered entity, or to provide a service described in the [Rule's] definition of *business associate* to a covered entity, such covered entity may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this section on business associate contracts, provided that the covered entity attempts in good faith to obtain satisfactory assurances that appropriate safeguards have been instituted [similar to those required by this Rule], and if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

· The covered entity may omit from its other arrangements the termination authorization required by this [Rule], if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

Specifications: Other Requirements for Contracts and Other Arrangements

· The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary for the proper management and administration of the business associate, or to carry out the legal responsibilities of the business associate.

· The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes noted in the previous paragraph if the disclosure is required by law; or

- The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and
- The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Standard: Requirements for Group Health Plans

- A group health plan, in order to disclose PHI to the plan sponsor or to provide for or permit the disclosure of PHI to the plans sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this [Rule].
- The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of:
  - Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or
  - Modifying, amending, or terminating the group health plan.

Specifications: Requirements for Plan Documents

The plan documents of the group health plan must be amended to incorporate provisions to:

- Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this [Rule].
- Provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:
  - Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
  - Ensure that any agents, including a subcontractor, to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
  - Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan or the plan sponsor;
  - Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for which it becomes aware;
  - Make available PHI in accordance with the Rule's "Rights to Request Privacy Protection for PHI;"
  - Make available PHI for amendment and incorporate any amendments to PHI in accordance with the Rule's "Amendment of PHI;"
  - Make available the information required to provide an accounting of disclosures in accordance with the Rule's "Accounting of PHI;"
  - Make its internal practices, books, and records relating to the use and disclosure of PHI received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this Rule;
  - If feasible, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible; and
  - Ensure that the adequate separation required between the group health plan and the plan sponsor as required in this Rule exists (see immediately below).

- Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:
  - Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the PHI to be disclosed, provided that any employee or person who receives PHI relating to payment under, healthcare operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;
  - Restrict the access to and use by such employees and other persons, described in the previous paragraph, to the plan administration functions that the plan sponsor performs for the group health plan; and
  - Provide an effective mechanism for resolving any issues of noncompliance by such persons with the plan document provisions required by [the Rule].

Specifications: Uses and Disclosures

A group health plan may:

- Disclose PHI to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the requirements for plan documents noted above;
- Not permit a health insurance issuer or HMO with respect to the group health plan to disclose PHI to the plan sponsor except as permitted by the Rule;
- Not disclose and may not permit a health insurance issuer or HMO to disclose PHI to a plan sponsor as otherwise permitted by this paragraph, unless a statement required by the Rule's "Notice of Privacy for PHI" is included in the appropriate notice; and
- Not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions in connection with any other benefit or employee benefit plan of the plan sponsor.

Standard: Requirements for a Covered Entity with Multiple Covered Functions

- A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered healthcare provider, and a healthcare clearinghouse, must comply with the standards, requirements, and implementation specifications of this [Rule], as applicable to the health plan, healthcare provider, or healthcare clearinghouse covered functions that are performed.
- A covered entity that performs multiple covered functions may use or disclose the PHI of individuals who receive the covered entity'' health plan or healthcare provider services, but not both, only for purposes related to the appropriate function being performed.

Consent for Use or Disclosures to Carry Out Treatment, Payment, or Health Care Operations

Standard: Consent Requirement

The Rule states (§164.506) that "a covered health care provider must obtain the individual's consent, in accordance with this [Rule], prior to using or disclosing PHI to carry out treatment, payment, or health care operations," with two exceptions:

- A covered healthcare provider may, without consent, use or disclose PHI to carry out treatment, payment, or healthcare operations, if:
  - It has an indirect treatment relationship (§164.501) with the individual; or

- It created or received the PHI in the course of providing healthcare to an individual who is an inmate.

· A covered healthcare provider may, without consent, use or disclose PHI created or received under the following conditions to carry out treatment payment or healthcare operations:
  - In emergency treatment situations, if the covered healthcare provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;
  - If the covered healthcare provider is required by law to treat the individual, and the covered healthcare provider attempts to obtain such consent, but is unable to obtain such consent; or
  - If a covered healthcare provider attempts to obtain such consent from the individual, but is unable to obtain such consent due to substantial barriers to communication with the individual, and the covered healthcare provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.
· A covered health provider that fails to obtain such consent…must document its attempt to obtain consent and the reason why consent was not obtained.
· If a covered entity is not required to obtain consent…it may obtain an individual's consent for the covered entity's own use or disclosure of PHI to carry out treatment, payment, or healthcare operations, provided that such consent meets the requirements of this [Rule].
· Except as provided in the requirements for joint consent, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose PHI.

Specifications: General requirements

· A covered healthcare provider may condition treatment on the provision of a consent by the individual.
· A health plan may condition enrollment in the health plan on the provision of a consent by the individual, under this section, sought in conjunction with such enrollment.
· A consent under this section may not be combined in a single document with the notice required by the Rule's Notice of Privacy for Protected Health Information.
· A consent for use or disclosure may be combined with other types of written permission from the individual (for example, an informed consent for treatment or a consent to assignment of benefits) if the consent is visually and organizationally separate from such other written legal permission, and is separately signed by the individual and dated.
· A consent for use or disclosure may be combined with a research authorization.
· An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.
· A covered entity must document and retain any signed consent under the Rule's Documentation requirements.

Specifications: Content Requirements

A consent must be in plain language and:

· Inform the individual that PHI may be used and disclosed to carry out treatment, payment, or healthcare operations;
· Refer the individual to the notice required by the Rule's Notice of Privacy Practices for Protected Health Information for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;

- If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with the Rule's Notice of Privacy Practices for Protected Health Information, state that the terms of its notice may change and describe how the individual may obtain a revised notice;
- State that:
  - The individual has the right to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment, or healthcare operations;
  - The covered entity is not required to agree to requested restrictions; and
  - If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity.
- State 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 thereon; and
- Be signed by the individual and dated.

Specification: Defective Consents

There is no consent under this section [of the Rule], if the document submitted has any of the following defects:

- The consent lacks an element as required above and as applicable; or
- The consent has been revoked.

Standard: Resolving Conflicting Consents and Authorizations

- If a covered entity has obtained a consent [as specified here] and receives any other authorization or written legal permission from the individual for a disclosure of PHI to carry out treatment, payment, or healthcare operations, the covered entity may disclose such PHI only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.
- A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual by:
  - Obtaining a new consent from the individual…for the disclosure to carry out treatment, payment, or healthcare operations; or
  - Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose PHI in accordance with the individual's preference.

Standard: Joint Consents

Covered entities that participate in an organized healthcare arrangement and that have a joint notice under the Rule's Notice of Privacy Practices for Protected Health Information section, may comply with this section by a joint consent.

Specifications: Requirements for Joint Consents

A joint consent must:

- Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and
- Meet the requirements of this section, except that the statements required may be altered to reflect the fact that the consent covers more than one covered entity.

If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.

Uses and Disclosures for Which an Authorization Is Required

Standard: Authorizations for Uses and Disclosures

Authorizations Required: General Rule

The Rule states (§164.508) that except as otherwise permitted or required by [the Rule], a covered entity may not use or disclose PHI without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure must be consistent with such authorization.

Authorizations required: Psychotherapy Notes

Notwithstanding any other provision of this section, other than the transition provisions provided for in the Rule's section Transition Provisions, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

- To carry out the following treatment, payment, or healthcare operations, consistent with consent requirements in Consent for Uses or Disclosures to Carry Out Treatment, Payment, or Health Care Operations:
  - Use by originator of the psychotherapy notes for treatment;
  - Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
  - Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual, and a use or disclosure that is required or permitted with respect to the oversight of the originator of the psychotherapy notes.

Specifications: Core Elements and Requirements

Core Elements

A valid authorization must contain at least the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
- A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

- A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
- Signature of the individual and date; and
- If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

Plain Language Requirement

"The authorization must be written in plain language."

Specifications: Authorizations Requested by a Covered Entity for Its Own Uses and Disclosures

If an authorization is requested by a covered entity for its own use or disclosure of PHI that it maintains, the covered entity must comply with the following requirements:

- The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements for "core elements and requirements" [above], contain the following elements:
  - For any authorization to which the "prohibition on conditioning" [see below] of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;
  - A description of each purpose of the requested use or disclosure;
  - A statement that the individual may inspect or copy the PHI to be used or disclosed as provided in the Rule's Access of Individuals to Protected Health Information and refuse to sign the authorization; and
  - If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.
- A covered entity must provide the individual with a copy of the signed authorization.

Authorizations Requested by a Covered Entity for Disclosures by Others

If an authorization is requested by a covered entity for another covered entity to disclose PHI to the covered entity requesting the authorization to carry out treatment, payment, or healthcare operations, the covered entity requesting the authorization must comply with the following requirements:

- The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of "core elements and requirements" [above], contain the following elements:
  - A description of each purpose of the requested disclosure;
  - Except for an authorization on which payment may be conditioned [see conditioning below], a statement that the covered entity will not condition treatment, payment, enrollment in the health plan or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and
  - A statement that the individual may refuse to sign the authorization.
- A covered entity must provide the individual with a copy of the signed authorization.

Specification: Authorizations for Uses and Disclosures of PHI Created for Research that Includes Treatment of the Individual

Except as otherwise permitted for research, a covered entity that creates PHI for the purpose, in whole or part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must be for uses and disclosures not otherwise permitted or required…meet the requirements of "core element and requirements" "valid authorizations" and contain:

- A description of the extent to which such PHI will be used or disclosed to carry out treatment, payment, or healthcare operations;
- A description of any PHI that will not be use or disclosed for purposes permitted in accordance with Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Objects and Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required, provided the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or [this Rule].
- If the covered entity has obtained or intends to obtain the individual's consent under Consent for Uses or Disclosures to Carry Out Treatment, Payment, or Health Care Operations, or has provided or intends to provide the individual with a notice under Notice of Privacy Practices for Protected Health Information, the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to this section are binding.

Optional Procedure

An authorization may be in the same document as:

- A consent to participate in the research;
- A consent to use or disclose PHI to carry out treatment, payment, or healthcare operations, or
- A notice of privacy practices.

Specifications: General Requirements

Valid Authorizations

A valid authorization is a document that contains the required elements listed above. A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements that are required.

Defective Authorization

An authorization is not valid, if the document submitted has any of the following defects:

- The expiration date has passed or the expiration event is known by the covered entity to have occurred;
- The authorization has not been filled out completely, with respect to an element described in this section above;
- The authorization is known by the covered entity to have been revoked;
- The authorization lacks an element required by this section above;
- The authorization violates the "compound authorization" requirements [below], if applicable; and
- Any material information in the authorization is known by the covered entity to be false.

Compound Authorizations

An authorization for use or disclosure of PHI information may not be combined with any other document to create a compound authorization, except as follows:

- An authorization for the use or disclosure of PHI created for research that includes treatment of the individual may be combined as permitted by [this Rule];
- An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
- An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits…on the provision of one of the authorizations.

Prohibition on Conditioning of Authorizations

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

- A covered healthcare provider may condition the provision of research-related treatment on provision of an authorization under this discussion [above];
- A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:
  - The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
  - The authorization is not for a use or disclosure of psychotherapy notes.
- A health plan may condition payment of a claim for specified benefits on provision of an authorization…if :
  - The disclosure is necessary to determine payment of such claim and the authorization is not for a use or disclosure of psychotherapy notes.
- A covered entity may condition the provision of healthcare that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

Revocation of Authorizations

An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that the covered entity has taken action in reliance thereon or if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

Documentation

A covered entity must document and retain any signed authorization under these requirements as required by the Rule's section on Documentation.

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

The Rule states (§164.510) that "a covered entity may use or disclose PHI without the written consent or authorization of the individual as described in the sections..[on Consents and Authorizations], respectively, provided the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

Standard: Use and Disclosure for Facility Directories

Permitted Uses and Disclosure

Except when an objection is expressed in accordance with the sections immediately below, a covered healthcare provider may:

- Use the following PHI to maintain a directory of individuals in its facility:
  - The individual's name;
  - The individual's location in the covered healthcare provider's facility;
  - The individual's condition described in general terms that does not communicate specific medical information about the individual; and
  - The individual's religious affiliation; and
- Disclose for directory purposes such information:
  - To members of the clergy, or
  - Except for religious affiliation, to other persons who ask for the individual by name.

Opportunity to Object

A covered healthcare provider must inform an individual of the PHI that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by the paragraph [just above].

Emergency Circumstances

- If the opportunity to object to uses or disclosures required by this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered healthcare provider may use or disclose some or all of the PHI permitted by "permitted uses and disclosure" [just above] for the facility's directory, if such disclosure is:
  - Consistent with a prior expressed preference of the individual, if any, that is known to the covered healthcare provider; and
  - In the individual's best interest as determined by the covered healthcare provider, in the exercise of professional judgment.
- The covered healthcare provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required when it becomes practicable.

Standard: Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

Permitted Uses and Disclosures

- A covered entity may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's healthcare.
- A covered entity may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with this section as applicable.

Uses and Disclosures with the Individual Present

If the individual is present for, or otherwise available prior to, a use or disclosure permitted by "permitted uses and disclosures" [just above], and has the capacity to make healthcare decisions, the covered entity may use or disclose the PHI if it:

- Obtains the individual's agreement;
- Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

Limited Use and Disclosures When the Individual Is Not Present

If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's healthcare. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

Use and Disclosures for Disaster Relief Purposes

A covered entity may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted above. The requirements related to the presence of the individual apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required

The Rule states (§164.512) that "a covered entity may use or disclose PHI without the written consent or authorization of the individual as described in Consent for Uses or Disclosures to Carry Out Treatment, Payment, or Health Care Operations and Uses and Disclosures for Which an Authorization is Required, respectively, or the opportunity for the individual to agree or object as described in Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object in the situations covered this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section the covered entity's information and the individual's agreement may be given orally.

Standard: Uses and Disclosure Required by Law

A covered entity may use or disclose PHI to the extent that such uses or disclosure is required by law and the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. However, a covered entity must meet the requirements descried in the section [below] for uses or disclosures required by law.

Standard: Uses and Disclosure for Public Health Activities

Permitted Disclosures

A covered entity may disclose PHI for the public health activities and purposes described in this paragraph to:

- A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;
- A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
- A person subject to the jurisdiction of the Food and Drug Administration (FDA):
  - To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the FDA;
  - To track products if the disclosure is made to a person required or directed by the FDA to track the product;
  - To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or
  - To conduct post-marketing surveillance to comply with requirements or at the direction of the FDA.

- A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or
- An employer, about an individual who is a member of the workforce of the employer, if:
  - The covered entity is a covered healthcare provider who is a member of the workforce of such an employer or who provides a healthcare [service] to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury;
  - The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
  - The employer needs such findings in order to comply with its obligations under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose to record such illness or injury or to carry out responsibilities for workplace medical surveillance;
  - The covered healthcare provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer;
    - By giving a copy of the notice to the individual when healthcare is provided; or
    - If the healthcare is provided on the work site of the employer, by posting the notice in a prominent place at the location where the healthcare is provided.

Permitted Uses

If the covered entity also is a public health authority, the covered entity is permitted to use PHI in all cases in which it is permitted to disclose such information for public health activities under "permitted disclosures."

Standard: Disclosures About Victims of Abuse, Neglect, or Domestic Violence

Permitted Disclosures

Except for reports of child abuse or neglect permitted by the section of permitted uses under public health, a covered entity may disclose PHI about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

- To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
- If the individual agrees to the disclosure; or
- To the extent the disclosure is expressly authorized by statute or regulation, and:
  - The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
  - If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Informing the Individual

A covered entity that makes a disclosure permitted by the permitted uses [just above] of this section must promptly inform the individual that such a report has been or will be made, except if:

- The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgement.

Standard: Uses and Disclosures for Health Oversight Activities

Permitted Disclosures

A covered entity may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

- The healthcare system;
- Government benefits programs for which health information is relevant to beneficiary eligibility;
- Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- Entities subject to civil rights laws for which health information is necessary for determining compliance.

Exception to Health Oversight Activities

For the purpose of the disclosures permitted by "permitted disclosures" [see above] of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise from and is not directly related to:

- The receipt of healthcare;
- A claim for public benefits related to health; or
- Qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

Joint Activities or Investigations

Notwithstanding the paragraph on "exception to health oversight activities," if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of the standard for "uses and disclosures for health oversight activities."

Permitted Uses
If a covered entity is also a health oversight agency, the covered entity may use PHI for health oversight activities as permitted by the standard for "uses and disclosures for health oversight activities."

Standard: Disclosures for Judicial and Administrative Proceedings

Permitted Disclosures
A covered entity may disclose PHI in the course of any judicial or administrative proceeding:

- In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order; or
- In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if the covered entity receives satisfactory assurance from the party seeking the PHI that reasonable efforts have been made by such party to:
  - Ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request by receiving from such party a written statement and accompanying documentation demonstrating that:
    - The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
    - The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
    - The time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objectives were filed or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution; or
  - Secure a qualified protective order by receiving from such party a written statement and accompanying documentation demonstrating that:
    - The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
    - The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
- A qualified protective order means—with respect to PHI requested in this section—by an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
  - Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
  - Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.
- A covered entity may disclose PHI in response to lawful process described above without receiving satisfactory assurance if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this section or to seek a qualified protective as noted above.

Standard: Disclosure for Law Enforcement Purposes

A covered entity may disclose PHI for a law enforcement purpose to a law enforcement official if the following conditions are met, as applicable:

Permitted Disclosures: Pursuant to Process and as Otherwise Required by Law
A covered entity may disclose PHI:

- As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws that require special reporting to special agencies.
- In compliance with and as limited by the relevant requirements of:
  - A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
  - A grand jury subpoena; or
  - An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
    - The information sought is relevant and material to a legitimate law enforcement inquiry;
    - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
    - De-identified information could not reasonably be used.

Permitted Disclosures: Limited Information for Identification and Location Purposes
Except for disclosures required by law as permitted pursuant to process and as otherwise required by law [above], a covered entity may disclose PHI 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, provided that only the following information is disclosed:

- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including health, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

This section also discusses the issue of releasing information related to "DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue" for identification and location purposes. Covered entities cannot release any of this information, with the exception of the eight categories, noted just above, which can in some cases be determined through analysis such as DNA testing and the like.

Permitted Disclosures: Victims of a Crime

A covered entity may disclose PHI 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 a crime, other than disclosures that are subject to laws that require special reporting to special agencies, if the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

- The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
- The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
- The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgement.

Permitted Disclosure: Decedents

A covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

Permitted Disclosure: Crime on Premises

A covered entity may disclose to a law enforcement official PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

Permitted Disclosure: Reporting Crime in Emergencies

- A covered healthcare provider providing emergency healthcare in response to a medical emergency, other than such emergency on the premises of the covered health-care provider, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
  - The commission and nature of a crime;
  - The location of such crime or of the victim(s) of such crime; and
  - The identity, description, and location of the perpetrator of such crime;
- If a covered healthcare provider believes that the medical emergency is the result of abuse, neglect or domestic violence of the individual in need of emergency healthcare, this section, "report crime in emergencies" does not apply; rather, the standards under "Disclosures About Victims of Abuse, Neglect or Domestic Violence," apply

Standard: Uses and Disclosures About Decedents

Coroners and Medical Examiners

A covered entity may disclose PHI to a corner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use PHI for the purposes described here.

Funeral Directors
A covered entity may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation Purposes
A covered entity may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Standard: Uses and Disclosures for Research Purposes

Permitted Uses and Disclosures
A covered entity may use or disclose PHI for research, regardless of the source of funding of the research provided that:

Board Approval of a Waiver of Authorization
The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by Uses and Disclosures for Which an Authorization Is Required for use or disclosure of PHI has been approved by either:

- An Institutional Review Board (IRB), established in accordance with federal law [see 65FR82816]; or
- A privacy board that:
  - Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy right and related interests;
  - Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
  - Does not have any member participating in a review of any project in which the member has a conflict of interests.

Reviews Preparatory to Research
The covered entity obtains from the researcher representations that:

- Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
- No PHI is to be removed from the covered entity by the researcher in the course of the review; and
- The PHI for which use or access is sought is necessary for the research purposes.

Research on Decedent's Information
The covered entity obtains from the researcher:

- Representation that the use or disclosure sought is solely for research on the PHI of decedents;
- Documentation, as the request of the covered entity, of the death of such individuals; and

- Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

Documentation of Waiver Approval
For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver under the "board approval of a waiver" section above, the documentation must include all of the following:

Identification and Date of Action
A statement identifying the IRB or privacy board and the date on which the alteration or waver of the authorization was approved;

Waiver Criteria
A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
- The use or disclosure of PHI involves no more than minimal risk to the individuals;
- The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
- The research could not practicably be conducted without the alteration or waiver;
- The research could not practicably be conducted without access to and use of the PHI;
- The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
- There is an adequate plan to protect the identifiers from improper use and disclosure;
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and
- There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this [Rule].

Protected Health Information Needed
A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board had determined;

Review and Approval Procedures
A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
- An IRB must follow the requirements of the Common Rule (45CFR46), including the normal review procedures or the expedited review procedures required under federal law;
- A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion for nonaffiliation (stated above);
- A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subjects of the PHI for which

use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

Required Signature

The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRP or the privacy board, as applicable.

{This section on release of PHI for research purposes without authorization generated considerable discussion and comment when introduced in the NPRM. Readers are directed to 65FR82535-82539 in the section-by-section of the preamble, and 65FR82689-82699 in the comments section if interested. The secretary does note some concern for situations where a noncovered entity might receive PHI as proposed, but violates the internal commitments and releases the information.

According to the Rule, even if such a waiver is approved, the institution must still note research disclosures (general not specific) in its Notice. Such a note in the Notice might motivate some individuals and patients to restrict the release of their information, or cause them to seek healthcare from an entity not involved in research.

The IRB review process has been operating for some time under the Common Rule. Covered entities' (healthcare providers) involvement with IRBs have varied. It will be up to the covered provider to ensure the changes in IRB or privacy board processes meet the requirements of this Rule and that the on-going activity of the IRB/privacy board maintain its compliance to this Rule and the other rules that are applicable.

A review of this rule might cause some covered entities to consider a privacy board, as described in this section of the Rule. Adoption of such a board does call for the involvement of unrelated parties and certain attendance requirements. This should be seriously considered.

There are several national organizations calling for further review of the federal rules on the use of PHI in medical research. If your organization is involved with research, it would be best to regularly monitor the developments concerning this issue.}

Standard: Uses and Disclosures to Avert a Serious Threat to Health or Safety

Permitted Disclosures

A covered entity may—consistent with applicable law and standards of ethical conduct—use or disclose PHI, if the covered entity, in good faith, believes the use or disclosure:

- Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and disclosure is made to a person or persons whom can reasonably prevent or lessen the threat, including the target of the threat; or
- Is necessary for law enforcement authorities to identify or apprehend an individual:
  - Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim;

    {Note that in such a case the covered entity can only release the "statement" and not any other information except for that indicated in "Disclosures for Law Enforcement Purposes" noted above.}

    or

- Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody as those terms are defined in [this Rule].

Use or Disclosure Not Permitted
A use or disclosure pursuant to this section may not be made if the information described (see above) is learned by the covered entity:

- In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure noted above, or counseling or therapy; or
- Through a request by the individual to initiate or be referred for the treatment, counseling, or therapy just described.

Presumption of Good Faith Belief
A covered entity that uses or discloses PHI pursuant to "permitted disclosure" is presumed to have acted in good faith with regard to a belief that the individual may have caused serious physical harm to the victim or that the individual has escaped from a correctional institution or from lawful custody, if the belief is based upon the covered entity's actual knowledge or in reliance on credible representation by a person with apparent knowledge or authority.

Standard: Uses and Disclosure for Specialized Government Functions

Military and Veterans
"A covered entity may use and disclose the PHI 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, based on a future *Federal Register* notice to be published which will define who the appropriate military command authorities are and for what purposes PHI may be used or disclosed."

Separation or Discharge
"A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the PHI of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs"

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

Foreign Military Personnel
A covered entity may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which use and disclosures are permitted for Armed Forces personnel under the notice to be published for "Military and Veterans" above.

{While the items for separation or discharge and veterans pertain to armed forces and veterans entities, the sections on military service and foreign military personnel will apply to all covered entities once the

notice referred to is published. Covered entities will have to watch for such a notice and may have to include reference to such a notice in their Privacy Notice.}

National Security and Intelligence Activities

A covered entity may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (for example, Executive Order 12333).

Protective Services for the President and Others

A covered entity may disclose PHI to authorized federal officials for the provision of protective services to the president or other persons authorized by 19 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Medical Suitability Determinations

The Rule covers some unique situations for covered entities that are only a component of the US Department of State. *{As such, this section should not be viewed as required by any other entities.}*

{The three situations above are not situations most covered entities will encounter. Such situations should fall into an entity's plan to direct such inquires to a source that can determine the validity of such a request.}

Correctional Institutions and Other Law Enforcement Custodial Situations

Permitted Disclosures

"A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI about such inmate or individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:

- The provision of health care to such individuals;
- The health and safety of such individual or other inmates;
- The health and safety of the officers or employees of or others at the correctional institution;
- The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- Law enforcement on the premises of the correctional institution; and
- The administration and maintenance of the safety, security, and good order of the correctional institution."

Permitted Uses

"A **covered entity that is a correctional institution** may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed."

No Application After Release

"For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody."

{This set of requirements will require close attention. The permitted disclosures vary on what can be disclosed, to whom, and when. There is actually limited information that can be disclosed to the immediate custodian of the inmate or individual, who is the official most likely to be present as treatment is provided. Training of the entity's workforce on these differences will be necessary. Note that the permission is negated once there is a release.}

Covered Entities That Are Government Programs Providing Public Benefits

- "A health plan that is a government program providing public benefits may disclose PHI relating to **eligibility for or enrollment in** the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information is a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation."
- "A covered entity that is a government agency administering a government program providing public benefits may disclose PHI related to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs."

{Both of these sections relate to programs within a "government." The first limits the PHI to eligibility and enrollment purposes, but the second is much more broad. Protections here would have to be provided in the federal or local regulations governing these agencies.}

Standard: Disclosure for Workers' Compensation

"A covered entity may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illnesses without regard to fault."

{Workers' compensation programs are not covered under HIPAA. There is no requirement for such programs to use the Transaction Standards and Codes. This section would seem to provide additional authority for PHI disclosure even though it would also fall under payment activities. Affected covered entities might want to note this in their Privacy Notice.}

Presidential Executive Order: To Protect the Privacy of Protected Health Information in Oversight Investigations

On December 26, 2000 the President Clinton issued Executive Order 13181 in the *Federal Register* (65FR81321-81323 at http://www.access.gpo.gov/su_docs/fedreg/a001226c.html).

Essentially the order indicates that the policy of the US Government will be "that law enforcement [federal] may not use PHI concerning an individual that is discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations of a non-health oversight matter, except when the balance of relevant factors weights clearly in favor of its use. That is, PHI may not be so used unless the public interest and the need for disclosure clearly outweigh the potential for injury to the patient, to the physician-patient relationship, and to the treatment services."

Other Requirements Relating to Uses and Disclosures of Protected Health Information

This section of the Rule (§164.514) begins by covering the standard and specifications for de-identification of PHI. In this analysis, this item is covered in Uses and Disclosures of De-Identified Protected Health Information.

This section also covers implementation specifications for minimum necessary uses and disclosures of PHI. Again to make this analysis easier to understand, these items are covered in Uses and Disclosure of Protected Health Information: General Rules.

{Marketing to patients of healthcare entities and beneficiaries of health plans also received considerable comments in response to the NPRM. The final privacy rule has not resolved some parties' concern for the use of PHI in marketing (as defined in the Rule). There is considerable detailed discussion on marketing in the preamble (65FR82543-82545) and in the comments section (65FR82716-82718).}

Standard: Uses and Disclosures of PHI for Marketing

As noted in the definitions section the issue of marketing received considerable attention in the creation of this rule. Much of this attention came about because of public concerns that health information was being shared with manufacturers and distributors. Covered entities, however, were concerned that, given the NPRM definition of marketing, routing operations functions could be hampered and could affect the patient negatively. Therefore, DHHS is attempting balance when it comes to its marketing standard.

Specifications: Requirements Relating to Marketing

The Rule states (§164.514(e)) that "a covered entity may not use or disclose PHI for marketing without an authorization…" However, "a covered entity is not required to obtain an authorization when it uses or discloses PHI to make a marketing communication to an individual that:

- Occurs in a face-to-face encounter with the individual;
- Concerns products or services of nominal value; or
- Concerns the health-related products and services of the covered entity or a third party and the communication."

Specifications: Requirements for Certain Marketing Communication

For a "marketing communication" to be permitted under the Rule, it must:

- Identify "the covered entity as the party making the communication;"
- State "prominently," when appropriate, the fact that "the covered entity has received or will receive direct or indirect remuneration for making the communication;" and
- "Contain instructions describing how the individual may opt out of receiving future such communications," "except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals."

It should be noted here that the Rule explicitly notes that "the covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications…are not sent such communications" in the future.

If, instead of the communication just described, "the covered entity uses or discloses PHI to target the communication to individuals based on their health status or condition," then:

- "The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual being targeted; and
- The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual."

Note also that a covered entity may disclose PHI for the purpose of these marketing communications to "a business associate that assists the covered entity with such communications."

Standard: Uses and Disclosures for Fundraising

Fundraising was another issue raised by many hospitals who were concerned that the NPRM for privacy would eliminate this practice. The Rule (§164.514(f)) states that a "covered entity may use, or disclose to a business associate or to an institutionally related foundation," "demographic information relating to an individual and [the] dates of health care provided to an individual," [both of these items are considered PHI] "for the purpose of raising funds for its own benefit," without an authorization.

Specifications: Fundraising Requirements

In order to take advantage of this fundraising option, the covered entity must:

- "Not use or disclose PHI for fundraising purposes" other than under the circumstances just stated unless an authorization is appropriately used;
- State in the covered entity's privacy notice that it will be using PHI for fundraising purposes as permitted;
- "Include in any fundraising materials it sends to an individual…a description of how the individual may opt out of receiving any further fundraising communications;" and
- "Make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications."

Standard: Uses and Disclosures for Underwriting and Related Purposes

The Rule (§164.514(g)) allows a health plan to receive PHI for the "purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits." However, if such health insurance or health benefits are not placed with the health plan…[the] plan may not use or disclose such PHI for any other purpose except as may be required by law."

Standard: Verification Requirement

The Rule (§164.514(h)) requires that prior to disclosing PHI a covered entity must verify the identity of a person requesting the information and the authority of any such person to have access to the PHI. The only exception to this are the items noted under Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object (where a minimal amount of data is available for directory and notification purposes). In this case, if the identity or any such authority of such a person is not known to the covered entity that is being asked to disclose PHI, then it must "obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI".

The preamble to the rule (65FR82546) suggests that "the covered entity must establish and use written policies and procedures (which may be standard protocols) that are reasonably designed to verify the identify and authority of the requestor where the covered entity does not know the person requesting the PHI.

Specifications: Verification

Conditions on Disclosures

"If a disclosure [of PHI] is conditioned by this…[Rule] on particular documentation, statements, or representations from the person requesting the PHI, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face meet the applicable requirements."

Included in the "documentation, statements, or representations" allowed are:

- An administrative (from §164.512) request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
  - "The information sought is relevant and material to a legitimate law enforcement inquiry;
  - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
  - De-identified information could not reasonably be used."
- The covered entity receives an IRB waver that meets the conditions specified in the section above, provided that all waivers and requests are appropriately dated and signed.

{In other words, if an entity receives what it can reasonably consider the appropriate documentation necessary for the entity to disclose PHI to the requestor, then it may do so. Patently, the best practice would be to ensure that such an exchange is documented.}

Identity of Public Officials

"A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or person acting on behalf of the public official:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- If the request is in writing, the request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum

of understanding, or purchase order, that establishes that the person is acting on behalf of the public official."

Authority of Public Officials
"A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
- If a request is made pursuant to legal process, warrant, subpoena order, or other legal process is issued by a grand jury or judicial or administrative tribunal is presumed to constitute legal authority."

{The regulations in this section point to "circumstances," "professional judgement," "may." This leaves a significant amount of room for the covered entity to define when, where, who, and how it will meet this requirement. When a decision is made to release information, it is obvious that documentation will be necessary in the form of the original or copy of the document that caused the entity to release the PHI, or the badge number, or other identification that was accepted as being legitimate for the purposes of the release.

The requests for such releases come in through a variety of different points in an entity, especially a hospital or a health system. Decisions, policies, and procedures follow by training, and an internal communication system will need to be established to ensure that these requirements are appropriately followed and documented.}

Notice of Privacy Practices for Protected Health Information

Standard: Notice of Privacy Practices—Right to Notice
The Rule states (§164.520) that "an individual has a right to adequate **notice** of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to PHI." There are two exceptions to this part of the Rule, one (§164.520(a)(2)) dealing with who in various group health plan relationships must provide the notice (65FR82820), and the second indicating that "an inmate does not have a right to notice" and further stating that the requirements for notice "do not apply to a correctional institution that is a covered entity."

Specifications: Content of the Notice—Required Elements
A covered entity "must provide a notice [Notice] that is written in plain language and that contains the [following] elements:

- ***Header—***"The Notice must contain the following statement as a header or otherwise prominently displayed: 'THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.'"
- ***Uses and Disclosures—*** "The notice must contain:

- "A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted…to make for…treatment, payment, and health care operations" under the Rule.
- "A description of each of the other purposes for which the covered entity is permitted or required by" the Rule "to use or disclose PHI without the individual's written consent or authorization."
- A description of each of the previous two bullets where a more stringent law might apply, rather than that required of this Rule.
- For each purpose included in the first two bullets, "the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by" the Rule "and other applicable law."
- "A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by" the Rule.

· ***Separate Statements for Certain Uses or Disclosures*** — "If the covered entity intends to engage in any of the following activities, [then] the description required" in the first two bullets above (in *Uses and Disclosures*) "must include a separate statement as applicable that:"
- "The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;
- The covered entity may contact the individual to raise funds for the covered entity; or
- A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose PHI to the sponsor of the plan."

· ***Individual Rights***—"The notice must contain a statement of the individual's right with respect to PHI and a brief description of how the individual may exercise these rights, as follows:
- The right to request restrictions on certain uses and disclosures of PHI" (Rights To Request Privacy Protection for Protected Health Information) "including a statement that the covered entity is not required to agree to a requested restriction;"
- "The right to receive confidential communications of PHI as provided by" the Rule's section on the right to request privacy protection for PHI "as applicable;"
- "The right to inspect and copy PHI (Access of Individuals to Protected Health Information);
- "The right to amend protected health information" (Amendment of Protected Health Information);
- "The right to receive an accounting of disclosures (Accounting of Disclosures of Protected Health Information);
- "The right of the individual, including an individual who has agreed to receive the notice electronically…to obtain a paper copy of the Notice from the covered entity upon request."

· ***Covered Entity's Duties***—"The Notice must contain:

- "A statement that the covered entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI;
- A statement that the covered entity is required to abide by the terms of the notice currently in effect;" and…
- A statement that "it [the covered entity] reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains" and a description on how it "will provide individuals with a revised notice."

{The Notice must reflect the practices of the covered entity. So, if the entity's practices change the Notice must be changed accordingly. The way that the regulation is written, to be permitted to make changes in these privacy practices, the original and subsequent Notices need to indicate that the entity reserves the right to make such changes in its privacy practices, and what it will and must do when such changes occur.

The more detailed with which a Notice is written, the more often that it may need to be changed. Therefore it would behoove the covered entity to, within the Rule's requirements, write its Notice in clear, simple, language that will permit the most flexibility without having to rewrite and distribute a new Notice.}

· ***Complaints***—"The notice 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 brief description of how the individual may file a complaint with the covered entity, and
- A statement that the individual will not be retaliated against for filing a complaint.

· ***Contact***—"The notice must contain the name, or title, and telephone number of a person or office to contact for further information."

{Note that these sections on complaints and contact provide for some flexibility. Facilities that already have a complaint mechanism, like a patient relations department, might consider routing privacy complaints to the same office or department. Likewise, the contact point for "further information" could be that same office, the privacy officer, health information management, and so forth.}

· ***Effective Date***—"The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published."

Specifications: Content of the Notice—Optional Elements

In addition to the information required above for the Notice, if a covered entity elects to limit the uses or disclosures that it is permitted to make, it *may* describe its more limited uses or disclosures in its Notice, "provided that the covered entity may not include in its Notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by" the Rule's standard on the use and disclosures to overt a serious threat to health or safety. Again, any changes in the optional elements require the same changes in the Notice as that required for the required elements.

Revisions to the Notice

The covered entity must "promptly revise and distribute its Notice whenever there is a material change to:

- The uses or disclosures,
- The individual's rights,
- The covered entity's legal duties, or
- Other privacy practices stated in the Notice."

"Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the Notice in which such material change is reflected."

Specifications: Provision of Notice

A covered entity must make the notice available on request to any person and to individuals as follows:

- ***Health Plans***—must provide notice:
  - "No later than the compliance date for health plans ["small plans," as defined, have an extra year], to individual then covered by the plan;
  - Thereafter, at the time of enrollment, to individuals who are new enrollees; and
  - Within 60 days of a material revision to the Notice, to individuals then covered by the plan."

  The health plan must also "no less frequently than once every three years…notify individuals then covered by the plan of the availability of the Notice and how to obtain the Notice. The health plan can satisfy this Notice requirement "if a [privacy] Notice is provided to the named insured of a policy under which coverage is provide to the named insured and on or more dependents." If a plan has more than one Notice, it can satisfy these requirements by "providing the Notice that is relevant to the individual or other person requesting the Notice."

- ***Covered Healthcare Providers That Have a Direct Treatment Relationship with an Individual***—must:
  - "Provide the Notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date" [which for these rules would be the same as the large health plan.]
  - If maintain a physical service delivery site [facility or office],
    - "Have a Notice available at the service delivery site for individuals to request to take with them; and
    - Post [in a facility] the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the Notice; and
    - Whenever the Notice is revised, make the Notice available upon request on or after the effective date of the revision…"

- ***Specific Requirements for Electronic Notices:***
  - A covered entity that maintains a web site that "provides information about the covered entity's customer services or benefits must prominently post its Notice on the Web site and make the Notice available electronically through the Web site."
  - "A covered entity may provide the notice to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity

knows that the e-mail has failed, a paper copy of the Notice must be provided to the individual."

- A covered entity can meet the requirements for Notices as described above by sending an e-mail Notice, as long as the notice conforms with all the requirements noted.
- If an individual's "first service delivery" is delivered electronically (for example, electronic prescription) then "the covered healthcare provider must provide electronic Notice automatically and contemporaneously in response to this first request for service.
- "The individual who is the recipient of electronic Notice retains the right to obtain a paper copy of the Notice from a covered entity upon request."

Note that "a covered entity must document compliance with the[se] Notice requirement[s] by retaining copies of [all] the Notices" it issues and as required by the documentation requirements of the Rule.

{The requirements for electronic notices is written in very confusing language, and a better description of DHHS's intent can be found in the preamble at 65FR82551.}

Specifications: Joint Notices by Separate Covered Entities

The Rule provides (§164.520(d)) for a joint Notice by separately covered entities. Covered entities that participate in organized healthcare arrangements may comply with the notice requirement by a "joint notice, provided that:

- The covered entities participating in the organized health care arrangement agree to abide by the terms of the Notice with respect to PHI created or received by the covered entity as part of its participation in the organized health care arrangement;"
- The joint Notice meets the requirements related to the required and optional elements for a notice and the posting and availability of the Notice as covered above, except to the extent that the joint notice has to be altered "to reflect the fact that the notice covers more than one covered entity;" and that the joint Notice:
  - Describes with reasonable specificity the covered entities, or class of entities, to which the joint Notice applies;
  - Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint Notice applies; and
  - If applicable, states that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement."

  The covered entities included in the joint Notice must provide the Notice to individuals in accordance with the same rules as noted above. However, "provision of the joint Notice to an individual by any one of the covered entities included in the joint Notice will satisfy the provision requirements of" the Rule "with respect to all others covered by the joint Notice.

{Note that the same documentation requirements for Notices apply to joint and single covered entities. It is unclear in the Rule if each member of the organized healthcare arrangement must maintain these copies, however, until clarified, it is appropriate to assume that they should.

While a joint Notice offers some advantages, it also means that any change by any of the parties must undergo the same reflected changes in the Notice, and so forth. Any agreement among the entities that

want a joint Notice will have to be written and followed to ensure that the Notice is always in compliance with what is the current actual practice(s) of each and every entity it represents.}

Rights to Request Privacy Protection for Protected Health Information

Standard: Right of an Individual to Request Restriction of Uses and Disclosures of PHI

The Rule provides a standard (§164.522) that states that "a covered entity must permit an individual to request that the covered entity restrict uses and disclosures of PHI about the individual to carry out treatment, payment, or health care operations" and disclosures related to involvement in an individual's care. Note, however, that "a covered entity is not required to agree to [such] a restriction" and in some situations, listed elsewhere in the Rule, is prohibited from agreeing to some restrictions.

An obvious requirement is that "a covered entity that agrees to a restriction must document the restriction" in accordance with the Rules documentation requirements.

"A covered entity that agrees to a restriction may not use or disclose PHI." However, if the individual who requested the restriction is in need of emergency treatment, and the restricted PHI is needed to provide such treatment, the covered entity may use the restricted PHI or disclose the PHI to a healthcare provider, to provide such treatment to the individual. In such a situation, the covered entity "must request that such health care provider not further use or disclose the information."

Specifications: Terminating a Restriction

The entity may terminate its agreement to a restriction, if:

- "The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The covered entity informs the individual that it is terminating its agreement to restriction."

In these cases, "the termination is only effective with respect to PHI created or received after it has so informed the individual.

Standard: Confidential Communication Requirements

"A **covered health care provider** must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the covered health care provider by alternative means or at alternative locations." "A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis."

Likewise, "A **health plan** must permit individuals to request and must accommodate reasonable requests by individual to receive communications of PHI from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger that individual."

Specifications: Conditions on Providing Confidential Communications
A covered entity (in this case either the healthcare provider or the health plan may require the individual to make a request for a confidential communication as described above in writing. "A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual."

Either the covered healthcare provider or the health plan may condition the provision of a reasonable accommodation to the request on:

- When appropriate, information as to how payment, if any will be handled; and
- Specification of an alternative address or other method of contact.

Access of Individuals to Protected Health Information

Standard: Access to PHI—Right of Access
The Rule states (§164.524) that "an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding; and
- PHI maintained by a covered entity that is subject to Clinical Laboratory Improvements Act (CLIA) amendments of 1988" to the extent that CLIA would prohibit an individuals access to the information in question.

Unreviewable Grounds for Denial
"A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances:"

- The PHI is the subject of one of the items just mentioned above.
- "The covered entity that is a **correctional institution** or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, **if** obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate."
- "An individual's access to PHI created or obtained by a covered health care provider in the course of **research that includes treatment may be temporarily suspended** for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research."
- "An individual's access to PHI that is contained in records that are **subject to the Privacy Act,** 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law."
- "An individual's access may be denied if the PHI was obtained from someone other than a health care provider under a **promise of confidentiality** and the access requested would be **reasonably** likely to reveal the source of the information."

Reviewable Grounds for Denial
"A covered entity may deny an individual access, provided that the individual is given a right to have such denial reviewed." "If access is denied on the ground[s] permitted [below] 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. The covered entity must provide or deny access in accordance with the determination of this reviewing official."

A **denial might occur** under this part of the Rule when:

- "A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person (unless such other person is a healthcare provider) and a licensed healthcare professional has determined in the exercise of professional judgement that the access requested is reasonably likely to cause substantial harm to such other person; or
- 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 such personal representative is reasonably likely to cause substantial harm to the individual or another person."

Specifications: Request for Access and Timely Action
The covered entity **must permit an individual to request access** to inspect or to obtain a copy of the PHI about the individual that is maintained in a designated record set. The covered entity **may require** individuals to make **requests for access in writing, provided** that it informs individuals of such a requirement."

There are **timelines** set under the Rule when a request is made. The covered entity must act on it no later than 30 days after receipt of the request . "If the request for access is for PHI that is not maintained or accessible to the covered entity on-site, the covered entity must take an action by no later than 60 days from the receipt of such a request." The Rule reiterates that there is no permission for an extension beyond the 60 days (30 days initial plus 30 days extension) and requires that the covered entity must provide the "individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and the covered entity may have only one such extension of time for action on a request for access."

Specifications: Provision of Access
If the **covered entity grants the request**, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested by:

- ***Providing the Access Requested***— "The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated records sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the PHI once in response to a request for access."

- ***Form of Access Requested*** –The covered entity:
  - "Must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual."
  - "May provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if: (A) The individual agrees in advance to such a summary or explanation; and (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation."
- ***Time and Manner of Access***—"the covered entity must provide the access…including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access."
- ***Fees***—If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the covered entity may impose a reasonable cost-based fee, provided that the fee includes only the cost of:
  - Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual;
  - Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
  - Preparing an explanation or summary of the PHI, if agreed to by the individual."

Specifications: Denial of Access

If the **covered entity denies the request,** in whole or in part, it must provide the individual with a timely written denial. "The denial must be in plain language and contain:

- The basis for the denial;
- If applicable, a statement of the individual's review rights…, including a description of how the individual may exercise such review rights; and
- A description of how the individual may complain to the covered entity pursuant to the Rules complaint procedures or to the Secretary…the description must include the name, or title, and telephone number of the contact person or office."

"If the covered entity does not maintain the PHI that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access."

"If the individual **has requested a review of a denial…** the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such a designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards" noted above. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other actions…as required to carry out the designated reviewing official's determination."

"A **covered entity must document** the following and retain the documentation, as required:
- The designated record sets that are subject to access by individuals; and
- The titles of the persons or offices responsible for receiving and processing requests for access by individuals."

Amendment of Protected Health Information

Standard: Right to Amend

The Rule says (§164.526) that "an individual has the **right to have a covered entity amend** PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set."

Denial of Amendment

The Rule also says a **covered entity may deny an individual's request for amendment**, if it determines that the PHI or record that is the subject of the request:
- Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
- Is not part of the designated record set;
- Would not be available for inspection as noted in the regulation on access; or
- Is accurate and complete.

Specifications: Requests for Amendment and Timely Action -- Individuals Request for Amendment

"A covered entity must permit an individual to request that the covered entity amend the PHI maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements."

A covered entity **must act on the individual's request** for an amendment no later than 60 days after receipt of such as request, as follows:
- If the covered entity grants the requested amendment, in whole or in part, and
- If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial.

Timely Action by the Covered Entity

If a covered entity is **unable to act on the amendment within the 60-day time limit**, the covered entity may extend the time for such action by no more than 30 days, provided that :
- The covered entity, within the [initial] 60 day time limit, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
- The covered entity may have only one such extension of time for action on a request for an amendment.

Specifications: Making the Amendment

If the covered entity grants the requested amendment, in whole or in part it must:

- ***Make the Amendment***—"Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment."
- ***Inform the Individual***—"Timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared"
- ***Informing Others***—"Make reasonable efforts to inform and provide the amendment within a reasonable time to:
  - Persons identified by the individual as having received PHI about the individual and needing the amendment; and
  - Persons, including business associates, that the covered entity knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

Specifications: Denying the amendment

If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements:

- ***Denial***—**"**The covered entity must provide the individual with a timely, 60 days or less, written denial. The denial must use plain language and contain:
  - The basis for the denial in accordance with those provided in the Rule
  - The individuals right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
  - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
  - A description of how the individual may complain to the covered entity pursuant to the [Rules] complaint procedures. The description must include the name or title, and telephone number of the contact person or office."
- ***Statement of Disagreement***—"The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement."
- ***Rebuttal Statement***—"The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement."
- ***Recordkeeping***—The covered entity must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set."
- ***Future Disclosures:***
  - "If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with the recordkeeping requirements, or at

the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates."

- When a subsequent disclosure is made using a standard transaction [one of the HIPAA electronic transactions] that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by and as applicable to the recipient of the standard transaction.

Specifications: Actions on Notices of Amendment.
"A covered entity that is informed by another covered entity of an amendment to an individual's PHI,…must amend the PHI in designated record sets as provided" by this Rule.

Specifications: Documentation
"A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation" as the Rule requires.

Accounting of Disclosures of Protected Health Information

Standard: Right to an Accounting of Disclosures of PHI
The Rule states (§164.528) that "an individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six [6] years prior to the date on which the accounting is requested, except for disclosures:

- "To carry out treatment, payment and health care operations;"
- "To individuals of PHI about them:"
- "For the facility's directory or to persons involved in the individual's care or other notification purposes;
- "For national security or intelligence purposes '
- "To correctional institutions or law enforcement officials, as provided
- "That occurred prior to the compliance date for the covered entity."

Note, that "an individual may request an accounting of disclosures for a period of time less than six years from the date of the request."

The Rule requires that the covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official as provided elsewhere in the Rule, for the time specified by such agency or official, if such 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 and specifying the time for which such a suspension is required. If the request to temporarily suspend is made orally by the agency or official, "the covered entity must:

- Document the statement, including the identity of the agency or official making the statement;
- Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
- Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement…is submitted during that time."

Specifications: Content of the Accounting

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

- Except for the items covered under the discussion on temporary suspension (just above) "the accounting must include disclosures of PHI that occurred during the six years…[or a shorter period if requested] prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.
- The accounting for each disclosure must include:
  - The date of the disclosure
  - The name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such [a] statement…a copy of the individual's written authorizations…or a copy of a written request for a disclosure.
- If, during the period covered by the accounting, the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose…or pursuant to a single authorization…, the accounting may with respect to such multiple disclosures provide:
  - The information required (and listed above) for the first disclosure during the accounting period;
  - The frequency, periodicity, or number of the disclosures made during the accounting period; and
  - The date of the last such disclosure during the accounting period.

Specifications: Provision of the Accounting

"The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request. The covered entity must provide the individual with the accounting requested, or if the covered entity is unable to provide the accounting within the time required by...the covered entity may extend the time to provide the accounting by no more than 30 days." The 30-day extension is permissible, provided that within the first 60-day time period the covered entity must "provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting." The covered entity is only permitted one such extension of time for action on a request for an accounting."

"The covered entity must provide the first accounting to an individual in any 12-month period without charge. The entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee."

Specifications: Documentation

A covered entity must document the following and retain the documentation as required;

- "The information required to be included in an accounting…that is subject to an accounting under" this Rule.
- "The written accounting that is provided to the individual;" and

- "The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals."

Administrative Requirements

Standard: Personnel Designations—*Privacy Officer*
The Rule states (§164.530(1)(i)) that: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity." The Rule also states (§164.530(ii)) that "A covered entity must designate a contact person or office who is responsible for receiving complaints under this…[Rule] and who is able to provide further information about matters covered by the *Notice of Privacy Practices.*"

{Note that AHIMA has published a position description for the Privacy Officer. This description is available on the AHIMA Web site: www.ahima.org }

Specifications: Personnel Designations
The personnel and offices selected in these two designations—privacy official and contact person—must be documented per the Rules documentation requirements and requirements in the *Notice.*

{Note again, that the contact person and privacy official (officer) do not necessarily have to be the same individual.}

Standard: Training
"A covered entity (§164.530(b)(1)) must train all members of its workforce on the policies and procedures with respect to PHI required by this…[Rule]…as necessary and appropriate for the members of the workforce to carry out their function within the covered entity."

Specifications: Training
To meet this requirement, training must:
- Be provided to "each member of the covered entity's workforce by no later than the compliance date for the covered entity;'
- "Thereafter" provide such training "to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
- Provide additional training "To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this..[Rule]..within a reasonable period of time after the material change becomes effective."

A covered entity must document that the training as described has been provided.

{The training described here is significant in meeting the compliance requirements of the Rule. Since just about all members of the workforce have the potential to come across some amount and/or form of PHI, training will have to be directed to all workforce members. This does not mean that all members should or need to be trained to the same degree or amount. The Rule does not designate who should do the training, although there are some assumptions in impact analysis (65FR82758). The size of the workforce and turnover of that workforce will also affect just how the training is given and what it covers.

Documentation of training should be done both on a entity-wide and individual basis. A signed statement of training by the individual workforce member will be helpful to show that training has occurred. This can also be used for enforcement purposes.}

Standards: Safeguards
"A covered entity (§164.530(C)(1)) must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI."

Specification: Safeguards
As such, the entity "must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards implementation specifications or other requirements of this" [Rule].

{There is limited language here regarding safeguards. However, HIPAA also has a set of security regulations that will be issued and will work hand in hand with this Privacy rule.}

Standard: Complaints to the Covered Entity
A covered entity §164.530(d)(1)) "must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this..[Rule]..or its compliance with such policies and procedures of the requirements of this..[Rule]." A "covered entity must also document all complaints received and their disposition."

Standard: Sanctions
A covered entity (§164.530(e)(1)) "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" the Rule. This requirement or standard "does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of" the Rule's requirements for disclosures by whistleblowers and workforce member crime victims, or workforce members that are filing a complaint with the Secretary, testifying, assisting or participating in an investigation, compliance review or similar proceeding, or opposing any unlawful act or practice. "A covered entity must document the sanctions that are applied, if any."

Standard: Mitigation
"A covered entity (§164.530(f)) must mitigate, to the extent practicable, any harmful effect that is known to the covered entity as a use or disclosure of PHI in violation of its policies and procedures or the requirements of this [Rule] by the covered entity or its business associate."

Standard: Refraining from Intimidating or Retaliatory Acts
"A covered entity (§164.530(g)) may not intimidate threaten, coerce, discriminate against, or take other retaliatory action against:

- ***Individuals***—"Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this [Rule] including the filing of a complaint"…;
- ***Individuals and others***—"Any individual or other person for:
  - Filing a complaint with the Secretary;

- Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing under Part C of Title XI; or
- Opposing any act or practice made unlawful by this [Rule] provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of this [Rule]."

Standard: Waiver of Rights

"A covered entity (§164.530(h)) may not require individuals to waive their rights under" the Rule's section on "complaints to the Secretary" or other parts of the Rule "as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Standard: Policies and Procedures

"A covered entity (§164.530(i)(1)) must implement policies and procedures with respect to PHI that is designed to comply with the standards, implementation specifications, or other requirements of this [Rule]. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the covered entity, to ensure such compliance." The Secretary then states that, "This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this [Rule]."

Standard: Changes to Policies or Procedures

"A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this [Rule]. When a covered entity changes a privacy practice that is stated in the Notice…and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the Notice revision," if it has "included in the Notice a statement reserving its right to make such a change in its privacy practices…A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance" with all requirements of the Rule.

Specification: Change in Law

"Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice…, the covered entity must promptly make the appropriate revisions to the Notice…. Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law."

To implement these changes to privacy policies and procedures, a covered entity must:

- "Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its Notice, complies with the standards, requirements, and implementation specifications of the [Rule];"
- "Document the policy or procedure as revised" and as required under the documentation section of this Rule; and

· Revise the Notice as required…to state the changed practice and make the revised Notice available as required.

Note: "The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised Notice."

If the covered entity has not reserved its right…to change a privacy practice that is stated in the Notice, the covered entity is bound by the privacy practices as stated in the Notice with respect to PHI created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the Notice, and the related policies and procedures, without having reserved the right to do so, provided that the change meets the implementation requirements in the paragraph just above and that "such change is effective only with respect to PHI created or received after the effective date of the notice."

Specification: Changes to Other Policies or Procedures

"A covered entity (§164.530(i)(5)) may change at any time, a policy or procedure that does not materially affect the content of the Notice…provided that:

· The policy or procedure, as revised, complies with the standards, requirements, and implementation specification of this subpart; and
· Prior to the effective date of the change, the policy or procedure, as revised, is documented."

Standard: Documentation

"A covered entity (§164.530(j)(1)) must:

· Maintain the policies and procedures provided for [above] in written or electronic form;
· If a communication is required by this [Rule] to be in writing, maintain such writing, or an electronic copy, as documentation; and
· If an action, activity , or designation is required by this [Rule] to be documented, maintain a written or electronic record of such action, activity, or designation."

Specification: Retention Period

"A covered entity (§164.530(j)(2)) must retain the documentation required…for six years from the date of its creation or the date when it last was in effect, whichever is later."

Standard: Group Health Plans

A group health plan is not subject to the standards or implementation noted above in "personnel designations," "training," "safeguards," "complaints to the covered entity," "sanctions," "mitigation," and "policies and procedures" to the extent that:

· The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
· The group health plan does not create or receive PHI, except for
  - summary health information,
  - information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

For those documents that the group health plan is required to maintain, and the like, it must meet all of the documentation requirements noted above.

{Readers of the Administrative section above will see many similarities to the Medicare compliance program. While compliance officers should probably not serve as the privacy officer, he or she should be

part of any privacy task force, and could serve in an active capacity to handle nonpatient complaints and help coordinate audits, training, sanctions and so forth.}

Modifications

The Rule's provision for modifications (§160.104) follow the same approach as the other HIPAA regulations. "The Secretary may adopt a modification at any time during the first year after the standard [rule] or implementation specification is initially adopted [the rule becomes effective—for example April 14, 2001], if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification." This will permit the Secretary to correct this Rule, which is initially effective on April 14, 2001, up to April 14, 2002.

After the first year (again April 14, 2001), the Secretary may adopt a modification to the Rule and its standards no more frequently than once every 12 months, and the Secretary will establish the compliance date for any modification made under this Rule. Such a compliance date can occur "no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification. The Rule also permits the Secretary to "consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification." The Rule can also "extend the compliance date for small health plans, as the Secretary determines is appropriate."

{Essentially, under HIPAA the National Committee on Vital and Health Statistics would be one of the initiators of modifications to this Rule. The Secretary would have to use the NPRM and the final rule process to seek public comment and issue the final regulation.}

Transition Provisions

Standard: Effect of Prior Consents and Authorizations
Specification: Requirements for Retaining Effectiveness of Prior Consents and Authorizations

This section of the Rule, §164.532, deals with situations that might arise when a consent, authorization, or other "express legal permission" is obtained from an individual before this Rule becomes effective on the appropriate compliance date. This section permits exceptions to the Rules requirements for consents and authorizations. It does not withstand any other requirements of the Rule. This section is written in very legalistic terms, but, essentially, sections §164.532(a) and (b) say that if such a permission(s) was in place, before the Rule's compliance date, the covered entity may continue to use or disclose PHI as follows:

- If the permission was for the purpose of treatment, payment or healthcare operations, the covered entity may, with respect to PHI that it created or received before the applicable compliance date, use or disclose such information for the purposes of carrying out treatment, payment or healthcare operations, provided that:
  - The covered entity does not use or disclose such information that is expressly excluded from the permission document; and
  - The covered entity complies with all limitations placed by the permission document in effect.

- If the permission was for a purpose other than to carry out treatment, payment, or healthcare operations, the covered entity may, with respect to PHI that it created or received before the applicable compliance date, make such use or disclosure, provided that:
  - The covered entity does not use or disclose such information that is expressly excluded from the permission document; and
  - The covered entity complies with all limitations place by the permission document in effect.
- If the permission identifies a specific research project that includes treatment of individuals, then:
  - If the permission specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to PHI that it created or received either before or after the applicable compliance date of the Rule and to which the consent of authorization applies, make such use or disclosure for purposes of that project.
  - If the permission is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to PHI that it created or received as part of the project before or after the applicable compliance date of the Rule, make a use or disclosure for purposes of that project.

  Either of these last two conditions is permitted provided that the covered entity complies with all limitations placed by the permission.
- If, after the applicable compliance date of the Rule, a covered entity agrees to restrictions requested by an individual, a subsequent use or disclosure PHI that is subject to the restriction based on one of the permissions just described in this section (§164.532), then the covered entity must comply with such a restriction.

Compliance and Enforcement

Applicability and Principles for Achieving Compliance

The Rule (§160.300 and .304) indicates that compliance is required of all covered entities and any others mentioned in the Rule itself.

The Rule specifically mentions that "the Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable…standards, requirements, and implementation specifications. The Rule further states that "the Secretary may provide technical assistance to covered entities to help them comply voluntarily with" these same applicable standards, etc.

{Past experience indicates that the Secretary and DHHS will try to provide as much assistance as possible. To date most of this has been via the DHHS Web sites and DHHS staff who have participated in numerous conferences, workshops, and so on. While these efforts have been a tremendous help, HIPAA seems to indicate Congresses desire to have DHHS take an even more active role. To date, however, Congress has not funded such a role.}

Complaints to the Secretary

Right to File a Complaint

The Rule states (§160.306) that "a person who believes a covered entity is not complying with the applicable requirements of..[the Rule]…may file a complaint with the Secretary."

Requirements for Filing Complaints

Complaints made to the Secretary must meet the following requirements:

- "A complaint must be filed in writing, either on paper or electronically."
- "A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable…standards, requirements, and implementation specifications of" [this Rule].
- "A complaint must be filed within 180 days of when the complainant know or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown."
- "The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the *Federal Register*."

Investigation

The Secretary is empowered to and "may investigate" the complaints just reviewed. "Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance."

Compliance Reviews

The Secretary "may" also "conduct compliance reviews to determine whether covered entities are complying with the applicable requirements" of this Rule.

Responsibilities of Covered Entities

Provide Records and Compliance Reports

Section 160.310 of the Rule requires that "A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable…standards, requirements, and implementation specifications" of the Rule.

Cooperate with Complaint Investigations and Compliance Reviews

The Rule essentially says a covered entity must cooperate with the Secretary in any cases where any such investigation(s) or compliance review(s) occur.

Permit Access to Information

The Rule covers three areas regarding access to information during an investigation or compliance review:

- Similar to Medicare regulations the Rule states that "A covered entity must permit access by the Secretary during normal business hours to its facilities, book, records, accounts, and other

sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable …standards," etc., of the Rule. "If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice."

- "If any information required of a covered entity under..[the Rule].. is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information the covered entity must so certify and set forth what efforts it has made to obtain the information."
- "PHI obtained by the Secretary in connection with an investigation or compliance review…will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable…standards," etc., of the Rule, "or if otherwise required by law."

Secretarial Action Regarding Complaints and Compliance Reviews

Resolution Where Noncompliance Is Indicated

"If an investigation…or compliance review…indicates a failure to comply, the Secretary will so inform the covered entity and if the matter arose from a complaint the complainant, in writing and attempt to resolve the matter by informal means whenever possible." If the matter cannot be resolved by informal means, the Secretary "may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the noncompliance."

Resolution When No Violation Is Found

If, after investigation or review, the Secretary determines that no further action is warranted, the Secretary will inform the covered entity, and if the incident arose from a complaint, the complainant in writing.

{The preamble notes (65FR82487) that DHHS plans to issue an "Enforcement Rule" that applies to all the HIPAA regulations for administrative simplification. This enforcement rule will address the imposition of civil monetary penalties and the referral of criminal cases where there has been a violation of this Privacy Rule. Depending on the nature of the violation and how the enforcement rule is written, financial penalties could range anywhere from $100 to $250,000 per incident. Criminal penalties, especially related to inappropriate use or disclosure of PHI could range anywhere from 1 to ten years in prison in addition to the fine.}

Reaction to AHIMA's Previous Comments on the Standards for the Privacy of Individual Identifiable Health Information

Applicability

AHIMA recommended that the scope of the rule be extended to include all individually identifiable health information, including purely paper records, maintained by covered entities.

This comment was addressed positively. The scope of the protections extend to all individually identifiable health information in any form or medium that is held or transmitted by a covered entity. This includes paper records that have never been electronically stored or transmitted and oral communications.

(164.500, 164.501-definition of "protected health information")

Definitions

Health Care Operations—AHIMA recommended that the words "risk reduction activities" be added to the definition of "health care operations" under subpart 1 or 5.

The specific words "risk reduction activities" were not added to the final definition of "health care operations." Still, the definition of "health care operations" was revised in such a manner that actual risk reduction activities are included in the definition.

AHIMA's comments contended that not all risk reduction activities "can be classified as either 'quality assessment and improvement' (subpart 1) or "in anticipation of legal proceedings" (subpart 5), although risk managers are indeed involved in both of these activities.

In response to comments, DHHS revised and expanded the original definition of healthcare operations. Specifically, subpart 1 was revised ***from***: "Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines;" ***to***: "Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;"

Subpart 5 was renumbered to subpart 4 and revised ***from***: "Compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding." ***To***: "Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs."

(164.501)

Individual—Disclosures pursuant to power of attorney. AHIMA requested further clarification on "the person informally designated as the patient's health care decision-maker."

References to the "power of attorney" have been deleted from the final rule. Further clarification of "the person informally designated as the patient's health care decision-maker" was provided in situational form in section 164.510 (b)—Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

The final rule specifies that "covered entities may disclose to a person involved in the current health care of the individual…PHI directly related to the person's involvement in the current health care of an individual or payment related to the individual's health care." For example, the preamble to the rule states "the fact that a person brings a family member into the doctor's office when treatment information will be discussed constitutes verification of the involved person's identity…" Furthermore, the final rule suggested that "the fact that a friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that the friend is involved in the individual's care, and the rule allows the pharmacist to give the filled prescription to the friend."

(164.502 (g), 164.510 (b))

AHIMA recommended amending the definition of "psychotherapy notes" to ensure their appropriate inclusion in the medical record. AHIMA recommended that the definition recognize a distinction between psychotherapy notes and the case notations maintained by the therapist.

Addressed affirmatively through a clarification of the definition. The definition distinctly mentions that "psychotherapy notes" are "separated from the rest of the individual's medical record."

The definition of "psychotherapy notes" also excludes medication and prescription monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

(164.501)

Introduction to General Rules

AHIMA recommended treating all health information equally, regardless of type.

Addressed affirmatively. This is addressed through the definitions of "individually identifiable health information" and "protected health information." Furthermore, the general rules regarding use and disclosure contain no special provisions for the various types of health information. Regardless of type, the information is addressed as either individually identifiable health information or PHI.

(164.501, 164.502)

Minimum Necessary Use and Disclosure

AHIMA urged DHHS to establish a "good faith" standard for covered entities who disclose the information with a statement that prohibits the use of the information for other than the stated purpose and requires the destruction of the information after the stated need has been fulfilled. AHIMA further recommended that covered entities be deemed in compliance with the "minimum

necessary use and disclosure" standard with regard to internal uses and disclosures if their computer-based patient record (CPR) systems use the appropriate safeguard mechanisms and meet the forthcoming security requirements.

AHIMA's recommendations were not specifically agreed to, but changes in the structure of the minimum necessary requirements in the final rule have a positive effect. The final rule states that, "the proposed requirement for individual review of all uses of PHI is replaced with a requirement for covered entities to implement policies and procedures that restrict access and uses based on the specific roles of members of the covered entity's workforce. Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures to limit the PHI in routine disclosures to the minimum necessary to achieve the purpose of that type of disclosure…Covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary of the use or disclosure intended." Healthcare provider disclosures and/or requests related to treatment are not subject to the minimum necessary standard.

Right of an Individual to Request Restrictions on Uses and Disclosures
AHIMA recommended deleting the proposed standard "Right of an individual to request restriction on uses and disclosures."

DHHS disagreed with AHIMA's recommendation. The final rule expands the individual's right to request restrictions beyond the healthcare provider to the remainder of the covered entities—health plans and healthcare clearinghouses that create or receive PHI other than as a business associate of another covered entity. Moreover, the rule clarifies that an individual may request that a covered entity agree not to disclose PHI to persons assisting with the individual's care, even if the disclosure is in accordance with the care standard (164.510 (b)). If the covered entity agrees to the request, they must abide by the agreement.

The final rule's discussion of this subject does provide exceptions for emergency circumstances and various other situations.

Covered entities are required to document the restriction via a note in the medical record or some similar notation. The documentation must be retained for six years from the date it was created or the date it was last in effect, whichever is later.

Covered entities are not required to agree to the request.

(164.510)

Creation of De-Identified Information
AHIMA supported this concept, but requested further clarification on removing information from the body of the medical record that may indirectly identify the individual.

DHHS did not provide any further clarification on this issue. AHIMA harbors concerns about the possibility that any of the 18 potential identifiers required to be removed from individually identifiable health information to create de-identified health information establishes a difficult standard because any of these identifiers may be buried in lengthy text fields.

DHHS responded that they "see no alternative that protects privacy…" and "that such unstructured text fields have little or no value in a de-identified information set and would be removed in any case…with time, we expect that such identifiers will be kept out of places where they are hard to locate and expunge."

(164.514 (a)-(c))

AHIMA recommended that DHHS establish a "good faith" standard for covered entities who make reasonable efforts to de-identify information when required.

This recommendation was addressed positively in the standard for de-identifying individually identifiable health information. The final rule establishes two different methods to meet the de-identification standard:

1. If a person with appropriate knowledge and experience applying 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 the subject of the information. The covered entity is required to document the analysis and results that justify the determination.

2. A "safe harbor" approach where covered entities can meet the standard by removing the list of 18 identifiers 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. In the final rule, geographic location and age can be included in the de-identified information. All dates directly related to the subject of the information must be removed or limited to the year, and zip codes must be removed or aggregated to include at least 20,000 people. Moreover, ages of 90 and over must be aggregated to a category of 90+ to avoid identification of very old individuals.

The covered entity is prohibited from disclosing the mechanism for re-identification of the information.

(164.514 (a)-(c))

AHIMA additionally recommended that the receiver of the de-identified information be required to sign an agreement not to reidentify or link the information to the individual(s) to whom it pertains. AHIMA believed that the proposed rule should make it a violation to attempt to reidentify or relink the previously de-identified information to the individual(s) to whom it pertains.

This recommendation was not addressed. DHHS response contended that they do not have the authority to regulate persons other than covered entities. Therefore, they could not attempt to regulate entities (receivers of the de-identified information) outside the scope of the final rule.

(164.514 (a)-(c))

Business Partners

AHIMA recommended that transcription services be specifically included as business partners.

Transcription services were not specifically included in the definition of "business associate." "Business associates" are based on what the entity does, not what the entity is. Therefore, since the "business associate" is based on the concept of function, DHHS did not list the types of entities that could be a "business associate."

(164.504 (e))

Deceased Persons

AHIMA recommended that the privacy standards for deceased persons be the same as those for living persons.

Agreed with AHIMA's recommendation. Protections for a deceased individual's health information will remain in effect for as long as the covered entity maintains the information.

(164.502 (f))

Individual Authorization (Consent)

The final rule distinguished between a consent and an authorization. A consent "allows use and disclosure of PHI only for treatment, payment, and health care operations." An authorization "allows use and disclosure of PHI for purposes other than treatment, payment, and health care operations."

AHIMA recommended that authorizations be required to specify an expiration date not to exceed one year.

DHHS did not establish an expiration date not to exceed one year. In lieu of an expiration date, DHHS cited that an individual has the right to revoke an authorization at any time. DHHS stated in the comment section that "If an individual determines that an authorized use or disclosure is no longer in her best interest, she should be able to withdraw the authorization and prevent any further uses or disclosures."

(164.506, 164.508)

AHIMA also recommended that the use of "prospective" authorizations (authorizations signed prior to the treatment episode from which the information is requested) be prohibited.

DHHS did not specifically address this issue. The right to revoke and the right for an individual to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment, or healthcare operations are applicable to this concern.

(164.506 (b)(5), (c)(4), 106.508, 164.522)

In all cases, AHIMA recommended that it be a violation of the rule if the information is redisclosed beyond what was authorized by the patient or the patient's legal representative.

A covered entity may not use or disclose PHI without an authorization that is valid under this section (164.508). Covered entities may use or disclose PHI only as permitted or required by this rule (164.502).

Noncovered entities are not bound by this final rule. If information is authorized to be disclosed by a covered entity to a noncovered entity, the noncovered entity could redisclose the information unless they are bound by a contractual agreement.

(164.508, 164.502)

Law Enforcement

AHIMA recommended that, except in cases described in Section 164.510 (f)(2), Limited information for identifying purposes, a warrant, subpoena, or court order be required for the release of PHI.

DHHS addressed AHIMA's recommendation affirmatively, but stipulated several exceptions where PHI could be released by a covered entity to a law enforcement official in the absence of a warrant, subpoena, or court order. The final rule permits PHI to be released under the following circumstances:

1. **Pursuant to process and as otherwise required by law.** This includes the release of information pursuant to a court order or court-ordered warrant, subpoena, or summons issued by a judicial officer; a grand jury subpoena; or an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law. The administrative request must meet a three-part test that requires that: (1) the information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) De-identified information could not reasonably be used.

2. **Limited information for identification and location purposes.** PHI may be disclosed 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. A law enforcement official's request may be made orally or in writing, and DHHS intends for it to include requests by a person acting on behalf of law enforcement as a media

organization making a television or radio announcement seeking the public's assistance with identifying a suspect. The covered entity is only permitted to disclose (A) Name and address; (B) Date and place of birth; (C) Social security number; (D) ABO blood type and rh factor; (E) Type of injury; (F) Date and time of treatment; (G) Date and time of death, if applicable, and (H) A description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

3. **Victims of a crime.** A covered entity may disclose PHI 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 a crime if the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that: (A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

4. **Decedents.** A covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual 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 PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

6. **Reporting crime in emergencies.** A covered healthcare provider providing emergency healthcare in response to a medical emergency, other than such emergency on the premises of the covered healthcare provider, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to: (A) The commission and nature of a crime; (B) The location of such crime or of the victim(s) of such crime; and (C) The identity, description, and location of the perpetrator of such crime. Any medical emergencies that the provider believes are the result of abuse, neglect, or domestic violence, the disclosures are beholden to a different standard that exists at (164.510 (c)).

(164.510 (f))

Rights and Procedures for a Written Notice of Informaiton Practices

AHIMA supported the requirement that an entity maintaining healthcare information must prepare and make available to patients upon request a written statement outlining its information practices and posting the notice in a clear and conspicuous manner. AHIMA did not support the idea of obtaining a signed acknowledgement from the individual upon the receipt of a notice of information practices.

The final rule agreed with AHIMA's position of not obtaining a signed acknowledgement from the individual upon the receipt of a notice of information practices.

(164.520)

Access for Inspection or Copying

AHIMA supported the reasonable, cost-based fee standard for copying health information pursuant to this section. In addition, AHIMA recommended that a covered entity be permitted to charge a reasonable, cost-based fee for inspection of the record and establish the procedures for the review process.

DHHS agreed with AHIMA's position. The covered entity can charge a reasonable, cost-based fee if the individual requests a copy of PHI or agrees to a summary or explanation of such information. The reasonable, cost-based fee can only include the cost of:

- Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual;
- Postage, when the individual has requested the copy, or the summary or explanation be mailed; and
- Preparing an explanation or summary of the PHI, if agreed to by the individual.

Covered entities may not charge any fees for retrieving or handling the information or for processing the request. These costs are not acceptable under this rule.

(164.524 (c)(4))

Accounting of Disclosures

AHIMA did not support the proposed requirement that covered entities maintain an accounting of disclosures for as long as the entity maintains the PHI. AHIMA recommended that the accounting of disclosures be maintained for a period of six years.

DHHS agreed with AHIMA's recommendation. The final rule provides that 'individuals have a right to an accounting of the applicable disclosures that have been made in the six-year period prior to a request for an accounting."

(164.528 (a)(1))

Rights and Procedures for Amendment and Correction

AHIMA supported the proposed requirement that covered plans and providers be required to accommodate requests for amendment or correction for as long as the entity maintains the PHI.

No change was necessary. The rule is consistent with AHIMA's position.

(164.526)

Designation of a Privacy Official

AHIMA supported the proposal that covered entities designate a privacy official. AHIMA strongly recommends that the privacy official be a credentialed health information management professional.

DHHS retained the requirement that covered entities designate a privacy official. DHHS did not agree with AHIMA's recommendation that the privacy official be a credentialed health information management professional. DHHS cited that a specific set of qualifications "sacrifice flexibility and scalability in implementation."

(164.530 (a))

Training

AHIMA supports the concept of requiring recertification once every three years and retraining in the event of material changes in the policy.

DHHS slightly revised these provisions by eliminating the requirement for recertification once every three years. Retraining is still required for material changes in the privacy policies and procedures of the covered entity.

(164.530 (b))

Relationship to State Laws

AHIMA continues to support federal preemptive legislation as a necessary ultimate solution. While recognizing the limitations of the HIPAA statute with respect to state laws and regulations, AHIMA recommended that federal efforts must preempt state laws and regulations to create a single national standard for handling health information. AHIMA will continue to pursue health information confidentiality legislation that preempts state laws and regulations, treats all health information equally, and establishes a strong, single, national standard for the use and disclosure of health information.

As expected, the HIPAA final privacy rule does not provide a uniform national standard for the use and disclosure of health information. The final rule does preempt state laws to a certain degree and establishes what can be termed as a federal "floor." Section 160.203 of the final rule outlines the preemption criteria and exceptions, including an exception for provisions of state law relating to the privacy of health information and are more stringent than the standards, requirements, or implementation specifications contained in the HIPAA final privacy rule. States are permitted to enact additional laws relating to health information privacy. Furthermore, the final rule establishes a process where states can request an exception to the Federal standards.

The preemption result was expected as the policy choice was made by Congress in the HIPAA legislation (PL 104-191).

(160.203)

Background and History

As noted at the beginning of this document, the final HIPAA privacy rule was published in the *Federal Register* on December 28, 2000. The content of the final rule was determined on the basis of the content of and comments to the NPRM published in November of 1999, as well as "fact finding" meeting conducted by DHHS and members of the (Clinton) White House staff. AHIMA members and staff were involved in some of the fact-finding meetings.

More than 50,000 comments were made to the proposed Rule. The final Rule's comment section (65FR82565) groups these comments and the Secretary's comments. As noted above a reading of this section will provide greater depth on the rationale DHHS used in promulgating the final Rule.

The final Rule's preamble (65FR82463) gives a detailed history and philosophy behind the Rule and the federal government's approach. It should be noted that while these privacy regulations were included under the HIPAA administrative simplification umbrella, Congress and the administration embraced a much larger goal than the privacy protection of electronic data transactions. It is for that reason that the HIPAA law and the Privacy Rule fall short on some of the protections that AHIMA and other organizations sought to achieve.

Between the signing of HIPAA and the final Rule there was hope that the Congress would pass additional legislation to make up for the deficiencies in the privacy requirements of HIPAA and what the Secretary could and could not include in regulation. Unfortunately, no legislation was passed. Readers of the Rule will see several suggestions by the Secretary for more legislation, and it will be up to the Congress to fill in these gaps, or individuals will quickly find the limits to protection this Rule provides.

Many see this Rule as a first step. It is applying confidentiality to an environment that is in transition from paper to electronic media. The HIPAA security rule and the enforcement rule will also have considerable bearing on the implementation of this Privacy Rule. At present, these rules are expected to be released in 2001, but no dates have been set.

Resources

Initially the reader will find only a few Web site resources available. As with other HIPAA components, this will change as the industry matures in its understanding. Since the final Rule has already created comments, the Secretary has already indicated that several technical amendments will be made. Readers should be alert to AHIMA and DHHS's Web sites to stay abreast of the current status on the Privacy Rule.

AHIMA members have been and are key to the privacy process. AHIMA will be expanding these resources in the area of policy, models, best practices, privacy officer helps, and so forth.

At present the following Web sites offer:

Federal Register:
Final Rule
http://www.access.gpo.gov/su_docs/fedreg/a001228c.html

Privacy NPRM
http://www.access.gpo.gov/su_docs/fedreg/a991103c.html

DHHS Administrative Simplification Web Page:
http://aspe.os.dhhs.gov/adminsimp/

DHHS Office of Civil Rights
http://www.hhs.gov/ocr/

DHHS Privacy Committee
http://aspe.os.dhhs.gov/datacncl/privcmte.htm

AHIMA
http://www.ahima.org

---

[1] Readers will notice that some word such as "healthcare" may be written in more than one way in this analysis. Style guides often require the term "healthcare" be stated as such, however, the federal government uses the term as "health care." In this document we will be using the term "healthcare" both ways. It will be two words within quotes from the Rule, and one word in all other situations. There are a few other situations, such as state vs.State, that the reader might also notice.

[2] All references to parts of this rule or any other material included in the *Federal Register*, in this analysis, will use the typical reference 65FR, meaning volume 65 of the *Federal Register*, and then the page. Specific referenced to a CFR (Code of Federal Regulation) section will include the section number and the page in the FR.

[3] FR copies can take up to 12 weeks for delivery. Those who wish to obtain a copy can send their request to: New Orders, Superintendent of Documents, PO Box 371954, Pittsburgh, PA 15250-7954. You must specify the date, December 28, 2000, and enclose a check or money order made payable to the Superintendent of Documents. Credit cards are also accepted, and if you choose to use a credit card, consider phoning in your order to (202) 512-1800. (Fax is also available at (202) 512-2250.) The cost for each copy is $8.

[4] "Small Health Plans" have been previously defined in the Transactions and Code Sets Rule as plans having $5 million or less in annual receipts.

[5] NPRM – Notice of Proposed Rule Making – in this case the NPRM for the Rule was November 3, 1999.

[6] Transactions as defined here include: Healthcare claims or equivalent encounter information; healthcare payment and remittance advice; coordination of benefits; healthcare claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; and other transactions that the Secretary may prescribe under HIPAA by regulation.