Wiggin & Dana

Counsellors at Law

One Century Tower
P.O. Box 1832
New Haven, Connecticut
06508-1832
Telephone 203.498.4400
Telefax 203.782.2889

Offices in:
New Haven
Hartford
Stamford
Philadelphia
www.wiggin.com

# H I P A A

# PRIVACY, SECURITY, & ELECTRONIC TRANSACTIONS

## SUMMARY OF STATUTE AND REGULATIONS

**Revised July 1, 2003**

## TABLE OF CONTENTS

I. INTRODUCTION ..... 1

II. THE HIPAA STATUTE ..... 2

A. Standards to Enable Electronic Interchange (Transactions Rule) ..... 2

B. Standards for Unique Health Identifiers ..... 2

C. Standards for Code Sets (Code Sets Rule) ..... 3

D. Security Standards for Health Information ..... 3

E. Standards for Electronic Signatures ..... 3

F. Standards for Transfer of Information Among Health Plans ..... 3

G. Privacy Standards (Privacy Rule) ..... 4

H. Development by HHS of HIPAA Regulations ..... 4

III. SCOPE OF HIPAA REGULATION ..... 5

A. Which Organizations Are Covered by HIPAA? ..... 5

1. Health Plans ..... 5

2. Health Care Clearinghouses ..... 5

3. Health Care Providers ..... 5

4. Business Associates ..... 6

5. Structural Designations ..... 6

a. Organized Health Care Arrangements (OHCAs) ..... 6

b. Affiliated Covered Entities ..... 7

c. Hybrid Entities ..... 7

B. Which Types of Information Are Covered by HIPAA? ..... 8

1. Individually Identifiable Health Information ..... 8

2. De-Identified Information ..... 9

3. Limited Data Sets....9
C. HIPAA Timetable....10
D. Scalability....10
IV. HIPAA PRIVACY REGULATIONS (PRIVACY RULE)....11
A. Scope of the Privacy Rule....11
B. Uses and Disclosures....11
1. Uses and Disclosures That Do Not Require Authorization....12
a. Use or Disclosure for Treatment, Payment or Health Care Operations 12
b. Incidental Uses or Disclosures....13
c. Use or Disclosure for Certain Legal or Public Health Purposes....13
d. Opportunity to Agree or Object....15
e. Required Disclosures....16
2. "Authorization" Needed for Most Other Uses and Disclosures....17
a. When Is An Authorization Required?....17
b. Form of Authorization....17
c. Defective Authorizations....18
d. Combining Authorizations with Other Documents ("Compound Authorizations")....18
e. Prohibition Against Conditioning Treatment, Payment, Eligibility, or Enrollment on Authorization....19
f. Validity of Patient Permission Obtained Prior to the Compliance Date of Rule....20
g. Marketing....20
h. Fundraising....21
i. Research....22

j. Psychotherapy Notes....24

C. Minimum Necessary Uses, Disclosures and Requests....24

1. Exceptions....25

2. Implementation of Minimum Necessary Standard....25

a. Uses of Protected Health Information....25

b. Disclosures of Protected Health Information....26

c. Requests by the Covered Entity for Protected Health Information....27

D. Personal Representatives....27

E. Business Associates....27

F. Individual Rights....30

1. Right to a Notice of the Covered Entity's Privacy Practices....30

2. Right to Request Restrictions of Protected Health Information....30

3. Right to Obtain Access to Protected Health Information for Inspection and Copying....31

4. Right to Obtain an Accounting of Disclosures....31

5. Right to Request Amendment of Protected Health Information....32

G. Administrative Requirements....32

1. Privacy Official....33

2. Internal Complaint Process....33

3. Training....33

4. Safeguards....33

5. Internal Sanctions....33

6. Mitigation in Event of Prohibited Use or Disclosure....34

7. Non-retaliation....34

H. Compliance & Enforcement ....34

1. Delegation of Authority to the Office for Civil Rights ....34

2. Enforcement Approach ....34

3. Individual Complaints and OCR Compliance Reviews ....34

4. Covered Entity's Compliance Responsibilities ....35

5. Penalties ....36

V. HIPAA SECURITY REGULATIONS (SECURITY RULE) ....37

A. General Requirements ....37

B. Administrative Safeguards ....38

C. Physical Safeguards ....39

D. Technical Safeguards ....39

E. Security Standards: Matrix ....41

VI. HIPAA REGULATIONS ON ELECTRONIC TRANSACTIONS AND CODE SETS (TRANSACTIONS AND CODE SETS RULE) ....42

A. Background ....42

B. Publication of Regulations and Implementation Guides ....42

C. Transactions and Code Sets Requirements ....43

VII. OTHER HIPAA REGULATIONS ....45

A. Employer Identifier ....45

B. Electronic Signature ....45

C. Health Care Provider Identifier ....45

D. Individual Health Identifier ....46

E. Health Plan Identifier ....46

VIII. ENFORCEMENT AND PENALTIES FOR VIOLATIONS OF HIPAA ....47

IX. EFFECT ON STATE LAW ..... 48

A. General HIPAA Preemption ..... 48

B. State Exemption Process ..... 48

C. "More Stringent" State Privacy Requirements ..... 49

Wiggin & Dana

Counsellors at Law

One Century Tower
P.O. Box 1832
New Haven, Connecticut
06508-1832
Telephone 203.498.4400
Telefax 203.782.2889

Offices in:
New Haven
Hartford
Stamford
Philadelphia
www.wiggin.com

# I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") marks a new era of information management. HIPAA mandated the nation-wide standardization of concepts and practices for assuring the privacy and security of health information. Since the enactment of HIPAA, all segments of the health care industry have witnessed a heightened awareness of patient privacy rights and health information practices.

Compliance with HIPAA requires a substantial and well-organized effort by covered health care organizations and their business associates. Careful planning in implementing each set of regulations enables covered entities to minimize the burdens of HIPAA and incorporate strategies for effective use of information technology and the Internet in enhancing and improving patient care. In addition, ongoing evaluation of compliance efforts will be necessary to ensure consistent adherence to the HIPAA regulations.

In this summary, we present major highlights of the HIPAA law and regulations related to privacy, security and electronic transactions and code sets as well as the implementing regulations.

## II. THE HIPAA STATUTE

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191. In addition to requirements concerning the transferability of health insurance and provisions that further empower the federal government in fighting fraud and abuse, HIPAA framed an expansive approach for regulating standardization, security and privacy of health information. The "Administrative Simplification" provisions of HIPAA (§§ 261-264 of HIPAA, 42 U.S.C. §§ 1320d-2 *et seq.*) call for the adoption of national standards in several critical areas. Congress stated that its purpose for these requirements is to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information. Section 262 of HIPAA enacted a new part C of Title XI of the Social Security Act, §§ 1171 through 1179, codified at 42 U.S.C. § 1320d *et seq*., 42 U.S.C. § 1301 *et seq*.

The HIPAA statute focuses on the electronic exchange of health information in connection with certain transactions listed below. However, as implemented by the Department of Health and Human Services (HHS) and as applied in practice, the requirements of HIPAA are more far reaching and will, in the end, likely govern essentially all collection, maintenance, transmission and disclosure of individually identifiable health information.

**A. Standards to Enable Electronic Interchange (Transactions Rule)** (42 U.S.C. § 1320d-2(a))

HIPAA requires that HHS adopt standards for certain transactions and data elements for such transactions to enable electronic exchange of health information. The specific transactions identified by Congress are:

a. Health claims or equivalent encounter information
b. Health claims attachments
c. Enrollment and disenrollment in a health plan
d. Eligibility for a health plan
e. Health care payments and remittance advice
f. Health plan payment premiums
g. First report of injury
h. Health claim status
i. Referral certification and authorization

**B. Standards for Unique Health Identifiers** (42 U.S.C. § 1320d-2(b))

HIPAA requires that HHS adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system.

**C. Standards for Code Sets (Code Sets Rule)** (42 U.S.C. § 1320d-2(c))

HIPAA requires that HHS adopt standards to select code sets for appropriate data elements for the transactions listed above from among code sets that have been developed by private and public entities or to establish code sets for such data elements if no code sets have already been developed.

**D. Security Standards for Health Information (Security Rule)** (42 U.S.C. § 1320d-2(d))

HIPAA requires that HHS adopt security standards that take into account the technical capabilities of available record systems, the costs of security measures, the need for training persons who have access to health information, the value of audit trails in computerized record systems, and the needs and capabilities of small health care providers and rural health care providers.

HIPAA requires that covered entities who maintain or transmit health information have reasonable and appropriate administrative, technical, and physical safeguards to

a. ensure the integrity and confidentiality of information;

b. protect against any reasonably anticipated

(i) threats or hazards to the security or integrity of the information and

(ii) unauthorized uses or disclosures of the information; and

c. ensure compliance by officers and employees.

**E. Standards for Electronic Signatures** (42 U.S.C. § 1320d-2(e))

HIPAA requires that HHS adopt standards specifying procedures for the electronic transmission and authentication of signatures in connection with the transactions listed above. Once adopted, these standards will be deemed to satisfy federal and state statutory requirements for written signatures relating to these transactions.

**F. Standards for Transfer of Information Among Health Plans** (42 U.S.C. § 1320d-2(f))

HIPAA requires that HHS adopt standards for transferring standard data elements among health plans needed for coordination of benefits, sequential processing of claims, and other data elements for individuals who have more than one health plan.

**G. Privacy Standards (Privacy Rule)** (42 U.S.C. § 1320d-2)

HIPAA required that HHS develop detailed recommendations on the privacy of "individually identifiable health information" within twelve months after HIPAA's enactment (by August 21, 1997). HHS issued such recommendations on September 11, 1997 together with a report recommending that Congress enact legislation providing fundamental privacy rights for patients and defining privacy responsibilities concerning individually identifiable health information.

HIPAA further provided that if federal legislation governing privacy standards for health data transmitted in connection with electronic exchanges concerning the identified transactions was not enacted by August 21, 1999, the Secretary would be required to promulgate final regulations concerning privacy standards no later than February 2000. Since Congress did not act, HHS proceeded in developing the Privacy Rule.

**H. Development by HHS of HIPAA Regulations**

As outlined below, HHS has issued thus far a variety of proposed and final regulations implementing the several HIPAA mandates. Although these separate regulations are not completely coordinated, they will eventually be interpreted and applied in a coordinated, integrated manner. The regulations and proposed regulations are lengthy and detailed. This outline provides a summary of key provisions.

## III. SCOPE OF HIPAA REGULATION

### A. Which Organizations Are Covered by HIPAA?

HIPAA applies to health plans, health care clearinghouses and health care providers that electronically transmit health care information. These entities are referred to throughout the HIPAA regulations as "covered entities." Unless otherwise noted, the terms described here apply to all of the HIPAA regulations promulgated to date, including the standards for Privacy, Security and Transactions and Code Sets.

#### 1. Health Plans

The HIPAA regulations provide a very detailed and broad definition of "health plan." The definition includes all individual or group plans that provide or pay for health care, such as certain insured and self-insured employee welfare benefit plans, insurers, health maintenance organizations, Medicare and Medicaid. (45 C.F.R. § 160.103)

#### 2. Health Care Clearinghouses

The term "health care clearinghouse" means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements or vice versa. This is generally an organization that receives information from a provider and translates it into a format for use by a health plan. (45 C.F.R. § 160.103)

#### 3. Health Care Providers

Health care providers include any individuals or organizations that provide, bill or are paid for health care services or supplies. Health care providers will include, for example, physicians and other health care practitioners, hospitals, skilled nursing facilities, home health agencies, labs and pharmacies. To be covered, a provider must transmit health information in electronic form in connection with any transaction covered by HIPAA. (45 C.F.R. § 160.103)

"Health care" is defined broadly in the HIPAA regulations as care, services, or supplies related to the health of a patient. It includes, but is not limited to, any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body, or any sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription. (45 C.F.R. § 160.103)

**4. Business Associates**

Congress provided that only health plans, health care providers and health care clearinghouses are "covered entities" subject to HIPAA. HHS has expressed concern about this narrow range of covered entities, given the reality of information sharing among a wide range of entities, and has effectively expanded the reach of the statute by including requirements for "business associates" of covered entities (see, e.g., comments to proposed privacy regulations at 64 Fed. Reg. 59,923). In order to protect information that passes from a covered entity to another person or organization, the Privacy and Security Rules discussed below include requirements for contracts with entities to which information flows. The Privacy Rule refers to "business associates" as persons to whom the covered entity discloses protected health information so that the business associate can carry out or assist with the performance of a function or activity for the covered entity.

Business associates include a broad range of contractors and other persons who receive protected health information, including consultants, third-party administrators, health care clearinghouses, billing firms, auditors, lawyers, and others. As explained below, HIPAA regulations require covered entities to contract with business associates concerning the use and disclosure of individually identifiable health information.

The Security Rule requires covered entities to obtain satisfactory assurances that business associates will safeguard data that passes from the covered entity to the business associate (45 C.F.R. § 164.308(b)).

The Transactions and Code Sets Rule addresses "trading partner" agreements with organizations "who assist covered entities in conducting covered electronic transactions in order to maintain the consistency of standards and codes." (45 C.F.R. § 162.915)

**5. Structural Designations**

**a. Organized Health Care Arrangements** (45 C.F.R. § 160.103)

The term, "organized health care arrangement" (OHCA), describes certain structural arrangements in which participants share information about their patients to manage and benefit the common enterprise. An example of such an arrangement is a hospital or nursing home setting, where the facility and physicians with staff privileges together provide treatment to an individual.

The HIPAA regulations identify five types of OHCAs. The first two types of OHCAs involve arrangements between or among health care providers.

One arises where legally separate entities participate in a clinically integrated care setting where individuals ordinarily receive treatment from more than one health care provider, such as the hospital situation mentioned above. The second type of OHCA is formed where more than one covered entity participates in an organized system of health care in which the entities hold themselves out to the public as a joint arrangement and participate together in at least one of the following: utilization review, quality assessment and improvement, or payment activities (involving sharing of risk and information). An example of this would be an independent practice association of various physicians. Certain provider networks and alliances may also constitute OHCAs, depending on the circumstances.

There are also three types of OHCAs related to group health plans. These include relationships between or among: (1) a group health plan and health insurance issuer/HMO with respect to information relating to individuals who are participants or beneficiaries of the group health plan; (2) two or more group health plans maintained by the same plan sponsor; and (3) a combination of group health plans maintained by the same sponsor and the health insurance issuers/HMOs with respect to such plan.

**b. Affiliated Covered Entities** (45 C.F.R. § 164.105(b))

Under the Privacy and Security Rules, legally separate covered entities that are affiliated may designate themselves as a single "affiliated" covered entity for purposes of complying with HIPAA. To be affiliated entities, all of the entities must be under "common control" or "common ownership." "Common control" is defined as when an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity. "Common ownership" is defined as when an entity or entities possess an ownership or equity interest of five (5) percent or more in another entity. (45 C.F.R. § 164.103) This provision may help health care systems and other affiliated entities streamline resources expended in complying with HIPAA.

Affiliated entities that designate themselves as a single affiliated covered entity under HIPAA remain separately liable for HIPAA compliance according to HHS comments.

**c. Hybrid Entities** (45 C.F.R. §§ 164.103; 164.105(a))

An organization that performs both covered and non-covered functions may elect to be considered a "hybrid entity" under the HIPAA regulations. A covered entity may choose to be a hybrid entity if it is a single legal entity that performs both covered and non-covered functions, regardless of

whether the non-covered functions are that entity's primary functions. To be considered a hybrid entity, the organization must designate its health care components, which may include a non-covered health care provider component or a business associate-like division in addition to the covered entity component. If the entity does not designate its health care components, then the entire organization will be considered a covered entity and subject to the HIPAA regulations.

Only the covered component of a hybrid entity must comply with the applicable requirements of the Privacy and Security Rules. A hybrid entity must ensure that its health care component does not disclose protected health information to its non-health care component. For example, if a large corporation operates an employee health clinic that is covered under the Privacy and Security Rules, the corporation may choose to be "hybrid" and designate the clinic as its health care component. In such a case, the clinic would be subject to the Privacy and Security Rules but the rest of the corporation would not.

## B. Which Types of Information Are Covered By HIPAA?

### 1. Individually Identifiable Health Information

Generally, the HIPAA regulations apply to "protected health information" or "PHI." The regulations define "protected health information" as "individually identifiable health information" transmitted or maintained in any form or medium. (45 C.F.R. § 160.103) This includes information transmitted or maintained electronically, as well as oral and written information. The Privacy Rule covers all forms of PHI, while the Security Rule applies only to electronic PHI.

"Individually identifiable health information" means health information, including demographic information collected from an individual, that

a. is created or received by a health care provider, employer, or health care clearinghouse; and

b. 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.

To be considered "individually identifiable health information," the information must identify the individual or there must be a reasonable basis to believe that the information can be used to identify the individual. (45 C.F.R. § 160.103)

Employment records maintained by a covered entity in its capacity as an employer (e.g., a doctor's statement to document sick leave) are not protected under the HIPAA regulations.

**2. De-Identified Information** (45 C.F.R. §§ 164.514(a), (b), (c))

De-identified health information is not protected by the Privacy Rule and thus may be used or disclosed freely. A covered entity may de-identify information by removing, coding, or otherwise eliminating or concealing aspects of the information that make it individually identifiable.

The Privacy Rule lists specific identifiers that, if removed or concealed, will render information presumptively de-identified (i.e, a "safe harbor" list).[1] The Privacy Rule also permits an entity to treat information as de-identified if a person with appropriate statistical experience and expertise determines that the probability of identifying individuals with the remaining information is very small and has no actual knowledge that the information could be used to identify individuals. The entity must document the methods used to de-identify the information and the results that justify the determination that the information is de-identified.

A covered entity may assign a code or other means of record identification to allow de-identified information to be re-identified. However, the code may not be derived from or related to the information about the individual, or otherwise capable of being translated so as to identify the individual (such as a code based upon a person's social security number). The code may not be used or disclosed for any other purpose, nor may the mechanism for re-identification be disclosed.

**3. Limited Data Sets** (45 C.F.R. §§ 164.514(e), 164.502(a))

As an alternative to de-identification for purposes of research, public health, or health care operations, the Privacy Rule permits the use and disclosure of a

[1] For de-identification, the following identifiers of the individual or relatives, employers, or household members of the individual must be removed: (a) names; (b) geographic subdivisions smaller than a state, including zip codes (the first three digits of a zip code may ordinarily be retained); (c) all elements of dates relating directly to the individual, except the year (e.g., birth date, admission date)(ages over 89 must be aggregated in a single category for 90+); (d) telephone numbers; (e) fax numbers; (f) electronic mail addresses; (g) social security numbers; (h) medical record numbers; (i) health plan beneficiary numbers; (j) account numbers; (k) certificate/ license numbers; (l) vehicle identifiers and serial numbers, including license plate numbers; (m) device identifiers and serial numbers; (n) Web Universal Relocators Locators (URLs); (o) Internet Protocol address numbers (IP); (p) biometric identifiers, including finger and voice prints; (q) full face photographic images and comparable images; (r) any other unique identifying number, characteristic, or code, except for a re-identification code.

"limited data set" containing certain identifying information that does not directly identify the individual.[2]

Disclosure of a limited data set is conditioned on a covered entity and the recipient of the information entering into a data use agreement. In the agreement, the recipient must agree to limit the use of the information to the specific purposes for which it was given, to limit who can use or receive the data and to agree not to re-identify the data or contact any individual whose data is disclosed in the limited data set. If a covered entity knows of a pattern of activity or practice of the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to cure the breach or end the violation. If these steps were unsuccessful, the covered entity must discontinue disclosure of protected health information to the recipient and report the problem to HHS.

## C. HIPAA Timetable

HIPAA is structured such that full compliance with each set of HIPAA regulations is required within twenty-four months after the effective date of the final regulation (or within thirty-six months for small health plans). (HIPAA, 42 U.S.C. § 1320d-4(b)(1)) For example, the final privacy regulations became effective on April 14, 2001, which made the compliance deadline April 14, 2003. Congress enacted legislation extending by one year the compliance date for the regulations addressing standards for electronic transactions and code sets provided the covered entity filed a compliance plan with HHS prior to the original compliance date of October 16, 2002.

## D. Scalability

Both the security and the privacy standards are considered "scalable," meaning that they have been designed in recognition that entities of all types and sizes will be subject to their requirements. Although both the Security and Privacy Rules expressly require the development of many policies and procedures to comply with standards, generally HHS has avoided identifying specific technological approaches and instead establishes conceptual standards that must be met. Organizations attempting to determine "how much is enough" may be guided by evolving industry interpretation of the standards as well as a combination of care and attention to detail, good faith, and common sense.

[2] For a limited data set, the following identifiers of the individual or relatives, employers, or household members of the individual must be removed: (a) names; (b) postal address information, other than town or city, State, and zip code; (c) telephone numbers; (d) fax numbers; (e) electronic mail addresses; (f) Social security numbers; (g) medical record numbers; (h) health plan beneficiary numbers; (i) account numbers; (j) certificate/license numbers; (k) vehicle identifiers and serial numbers, including license plate numbers; (l) device identifiers and serial numbers; (m) Web Universal Resource Locators (URLs); (n) Internet Protocol (IP) address numbers; (o) biometric identifiers, including finger and voice prints; and (p) full face photographic images and any comparable images.

## IV. HIPAA PRIVACY REGULATIONS (PRIVACY RULE)

HHS proposed HIPAA privacy regulations on November 3, 1999. After reviewing approximately 52,000 comments, HHS issued a final Privacy Rule on December 28, 2000, just as President Clinton was leaving office. HHS delayed the effective date of the Privacy Rule for technical reasons until April 14, 2001 and thus, compliance with the Privacy Rule was required by April 14, 2003 (or, for small health plans, by April 14, 2004).

On July 6, 2001, the HHS Office for Civil Rights ("OCR"), which is charged with enforcement of the Privacy Rule, issued its initial Guidance on the Privacy Rule. In the Guidance, OCR clarified certain requirements in the Privacy Rule and suggested that HHS would issue proposed regulations modifying some of these requirements. On March 27, 2002, HHS issued a Notice of Proposed Rule-Making (NPRM) proposing numerous modifications to the Privacy Rule. HHS adopted many of the proposed modifications and issued a Final Rule on August 14, 2002. On December 3, 2002, OCR published a 122-page Guidance with commentary, explanations and "frequently asked questions" about many of the Privacy Rule standards. HHS subsequently published additional regulations concerning addresses to which privacy complaints may be sent and certain enforcement provisions. The major provisions of the Privacy Rule are summarized below.

### A. Scope of the Privacy Rule

The Privacy Rule applies to the three types of health care organizations mandated by the HIPAA statute: health care providers that store and transmit health information electronically, health plans and health care clearinghouses. The Privacy Rule also extends its regulatory reach to "business associates" of covered entities through required contractual obligations. (See discussion of business associates below)

The Privacy Rule covers all "protected health information" (defined in Section III(B)(1) of this Summary), whether it is electronic, on paper or orally transmitted. However, two types of protected health information are not covered by the Privacy Rule. Health information that has been "de-identified" (as discussed above) is not covered by the Privacy Rule and may be used or disclosed freely. As an alternative to de-identification, the Privacy Rule permits certain health information that does not directly identify the individual ("limited data sets") to be used or disclosed for purposes of research, public health or health care operations. See discussion at Section III(B) of this Summary.

### B. Uses and Disclosures

The Privacy Rule applies to both the "disclosure" and "use" of protected health information. A covered entity may use or disclose an individual's protected health information only as permitted by the Privacy Rule (and applicable state law). (45 C.F.R. § 164.502(a)) "Disclosure" means "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information." "Use" is defined as "the sharing, employment, application, utilization, examination, or

analysis of [individually identifiable health] information within an entity that maintains such information." (45 C.F.R. § 160.103)

The final HIPAA Privacy Rule established the general rule that protected health information may not be used or disclosed except as permitted by the Rule. The Rule outlines the various types of use and disclosure that do not require the individual's Authorization. Any use or disclosure that does not fall within these exceptions must be based on the individual's Authorization.

**1. Uses and Disclosures That Do Not Require Authorization**

**a. Use or Disclosure for Treatment, Payment or Health Care Operations** (45 C.F.R. §§ 164.506, 164.501)

**i. General Rule: Authorization Not Required**

Under the Privacy Rule, a covered health care provider may use or disclose an individual's identifiable health information for certain treatment, payment, or health care operations[3] purposes without obtaining the individual's consent. However, this statutory permission does not apply to uses or disclosures that specifically require an Authorization (see Section IV(B)(2) of this Summary).

A covered entity may use or disclose protected health information for purposes of treatment, including the treatment activities of any health care provider. A covered entity also may use or disclose protected health information for the payment activities of the covered entity, another covered entity, or a health care provider. In addition, a covered entity may use or disclose protected health information for its own health care operations and for certain health care operations activities, such as quality improvement, case management and credentialing, of other covered entities that have a relationship with the individual. Finally, a covered entity participating in an Organized Health Care Arrangement (OHCA) may disclose protected health information to another covered entity that

[3] The definitions of "treatment" and "payment" in the Privacy Rule are broad and fairly straightforward. (See 45 C.F.R. § 164.501) The term "health care operations" is broadly defined to include (but is not limited to) (1) conducting quality assessments and improvement activities; (2) reviewing the competence or qualifications of health care professionals and 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; (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development (e.g., cost-management analyses); and (6) business management and administrative activities (e.g., HIPAA compliance, customer service, resolution of internal grievances, the sale or transfer of covered entity and related due diligence and record transfers, the creation of de-identified health information or a limited data set, and fundraising for the benefit of the covered entity).

participates in the OHCA for any health care operations activities of the OHCA.

**ii. "Consent" Process Is Optional**

Covered entities may choose to obtain consent from individuals for use or disclosure of protected health information for treatment, payment, or health care operations. If a covered entity chooses to implement a consent process, the entity has broad discretion in designing that process.

**b. Incidental Uses and Disclosures** (45 C.F.R. § 164.502(a)(1)(iii))

Authorization is not required for uses or disclosure that are incidental to an otherwise permitted use or disclosure so long as the covered entity uses reasonable safeguards and follows the minimum necessary rule (see Sections IV(G)(4) and (IV)(C) of this Summary). For example, doctor's offices may use waiting room sign-in sheets, hospitals may keep patients' charts at bedside, doctors can talk to patients in semi-private rooms, and doctors can confer at nurses' stations without fear of violating the Privacy Rule if overheard by a passerby. However, if a covered entity does not use reasonable safeguards or follow the minimum necessary rule, any incidental disclosures may violate the Privacy Rule.

**c. Use or Disclosure for Certain Legal or Public Health Purposes** (45 C.F.R. § 164.512)

Subject to specific, detailed requirements included in the Rule, covered entities may use or disclose individually identifiable information without an Authorization for certain legal or public health-related purposes. These include uses and disclosures:

i. To the extent required by law;

ii. For public health activities:

- To a public health authority for the purpose of preventing or controlling disease or injury;
- To a public health authority or other government authority authorized to receive reports of child neglect or abuse;
- To a person subject to the jurisdiction of the Food & Drug Administration (FDA) for public health purposes related to the quality, safety or effectiveness of FDA-regulated products or activities. This would include reporting adverse events with

respect to food or dietary supplements and product defects (including defective labeling) to the FDA, tracking products, enabling product recalls, repairs, replacements or look back (including locating and notifying persons who have received defective products); and conducting post-marketing surveillance in compliance with FDA requirements;

- To 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 authorized by law;

- To an employer about an individual who is a member of the employer's workforce, under highly limited circumstances outlined in the Rule, generally related to on-site illness or injury or workplace medical surveillance;

iii. To a social services or protective services agency, or other government authority authorized by law to receive reports of abuse, neglect or domestic violence (except for reports of child abuse, which are handled as a public health activity).

iv. To a health oversight agency for oversight activities authorized by law;

v. For judicial or administrative proceedings where required by order of a court or administrative tribunal or in response to a subpoena or discovery request, so long as certain precautions are taken and any necessary written assurances obtained;

vi. For certain law enforcement purposes enumerated in the Rule, including: the reporting of certain injuries required by law; disclosure of health information to aid in identifying or locating a suspect, fugitive, material witness or missing person; disclosure of the health information of a suspected victim of a crime to allow determination of whether a violation of law has occurred; disclosure of the death of an individual suspected to have died as a result of a crime; disclosure of health information relevant to the commission of a crime on the entity's premises; and disclosures occurring in certain emergency situations;

vii. To a coroner or medical examiner for the purposes of identifying the deceased person or determining the cause of death;

viii. To a funeral director as necessary to carry out duties with respect to the decedent;

ix. To an organization engaged in the procurement, banking, or transplantation of organs, eyes, or tissues for the purpose of facilitating donation or transplantation;

x. For medical research, so long as (a) the covered entity obtains a waiver of the individual authorization required by an Institutional Review Board or privacy board; (b) the information is used only in preparation for research; or (c) the information relates solely to deceased patients;

xi. To avert a serious and imminent threat to the health or safety of a person where the disclosure is made to someone reasonably able to prevent or lessen the threat;

xii. To comply with laws relating to workers' compensation or other similar programs established by law to provide benefits for work-related injuries or illnesses without regard to fault; or

xiii. For certain specialized government functions outlined in the Rule, such as certain military and national security and intelligence activities.

**d. Opportunity to "Agree" or "Object"** (45 C.F.R. § 164.510)

There are certain circumstances where written Authorization is not required so long as the individual is informed and has an opportunity to object to the use or disclosure. In these instances, subject to detailed limits and conditions, the covered entity may proceed without an Authorization if the covered entity gives the individual the opportunity to restrict or prohibit some or all of the proposed uses or disclosures. These circumstances include:

**i. Facility Directories**

A covered provider may include a patient's name, location in the facility, general condition (not communicating specific medical information), and religious affiliation in its directory. A provider may disclose this directory information to members of the clergy and (except for religious affiliation) to any person asking about the patient by name.

The covered provider must give the individual the opportunity to restrict or prohibit the disclosures or uses mentioned above, unless it would be impracticable to do so as a result of incapacity or an emergency treatment situation. Under those circumstances, the provider may disclose such information if the disclosure is either consistent with a prior expressed

preference of the individual or is in the individual's best interest, as determined by the provider, using professional judgment. Once it becomes practicable to do so, however, the provider must give the individual the opportunity to restrict or prohibit uses or disclosures for facility directory purposes.

**ii. Disclosure to Family/Friends Involved in Care or Payment**

A covered entity may disclose protected health information to notify a family member, relative, close personal friend, or any other person identified by the patient or any person responsible for the patient's care of the patient's location, general condition, or death. However, the covered entity may disclose only protected health information that is directly relevant to that person's involvement in the patient's care or payment for care.

- Individual available and has capacity

If the patient is available and has capacity to make health care decisions, the covered entity may disclose the above information only if: (a) the patient agrees; (b) the patient is provided with an opportunity to object and does not express any objection; or (c) the covered entity reasonably infers from the circumstances that the patient does not object to the disclosure.

- Patient not present or incapacitated

If the patient is not present or cannot practically exercise the right to object due to incapacity or there is an emergency situation, the covered entity may determine whether disclosure is in the patient's interest. If disclosure is in the patient's interest, the covered entity may disclose protected health information that is directly related to the person's involvement in the patient's health care.

**iii. Disaster Relief**

Disclosures may be made to a public or private entity engaged in disaster relief efforts.

**e. Required Disclosures** (45 C.F.R. §§ 160.300, 160.502, 160.524, 160.528)

The Privacy Rule generally does not require covered entities to disclose any protected health information except: (1) where an individual requests to inspect or copy his or her protected health information or requests an accounting of disclosures of such protected health information maintained during the prior six

years, or (2) where HHS requires such disclosure to investigate or determine the entity's compliance with HIPAA requirements.

**2. "Authorization" Needed for Most Other Uses and Disclosures** (45 C.F.R. § 164.508)

**a. When Is an Authorization Required?**

If a use or disclosure of protected health information does not fit into one of the exceptions discussed above, the use or disclosure will generally require a written "Authorization." An individual may revoke the Authorization in writing at any time, except to the extent that the covered entity has taken action in reliance on that Authorization. Special rules for Authorizations apply to marketing activities, fundraising, research, and psychotherapy notes.

**b. Form of Authorization**

Covered entities may use one Authorization Form for all purposes. All Authorizations must be written in "plain language" and must contain at least the following "core" elements and notification statements:

i. A "specific and meaningful" description of the information to be used or disclosed;

ii. The name of the covered entity or class of entities or persons authorized to make the requested use or disclosure;

iii. The name, type or class of persons to whom the requested use or disclosure may be made;

iv. A description of each purpose of the use or disclosure (e.g., "at the request of the individual");

v. An expiration date or event (research studies may indicate, "end of the research study" or "have," if applicable);

vi. Language informing the individual of the right to revoke the Authorization in writing and either the exceptions to the right to revoke and a description of how to revoke or a reference to the covered entity's Notice if this information is included there;

vii. Language informing the individual that treatment, payment, enrollment, or eligibility benefits generally may not be conditioned on the Authorization or, if conditioning is permitted, a statement about the consequences of refusing to sign the Authorization;

viii. Language informing the individual that the information disclosed pursuant to the Authorization could be subject to redisclosure by the recipient and no longer be protected by the Privacy Rule; and

ix. The signature of the individual and date. (If signed by the individual's representative, a description of such representative's authority to act for the individual is also required.)

In addition, if the covered entity conducts certain marketing activities that involve direct or indirect remuneration to the covered entity from a third party, the Authorization must state that fact. See discussion at Section IV(B)(2)(g) of this Summary.

**c. Defective Authorizations**

A covered entity may not use or disclose protected health information referenced in an Authorization if the Authorization is defective in one of the following ways:

i. Fails to contain any one of the required core elements or notification statements specified above, as applicable;

ii. The expiration date or event has passed;

iii. The Authorization is not filled out completely with respect to any required element;

iv. The covered entity knows that the Authorization has been revoked;

v. Any material information in the Authorization is known by the covered entity to be false; or

vi. The Authorization is an impermissible compound or conditioning Authorization.

**d. Combining Authorizations With Other Documents ("Compound Authorizations")**

A covered entity may not act upon an Authorization that is combined with any other document, including any other type of written permission from the individual, except that:

i. An Authorization for use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study;

ii. Authorizations for the use or disclosure of psychotherapy notes for multiple purposes may be combined in a single document, but may not be combined with Authorizations for the use or disclosure of other protected health information; and

iii. Authorizations for the use or disclosure of protected health information may be combined, provided that the covered entity does not condition treatment, payment, enrollment or eligibility upon obtaining the Authorization (an Authorization for psychotherapy notes is treated specially, as noted below).

**e. Prohibition Against Conditioning Treatment, Payment, Eligibility or Enrollment on Authorization**

In general, a covered entity may not condition treatment, payment, eligibility or enrollment on obtaining an Authorization. This prohibition is intended to prevent entities from coercing individuals into signing an Authorization that is not necessary to carry out the primary services provided by the covered entity to the individual. There are three exceptions to the general prohibition:

i. Covered entities seeking to use or disclose protected health information created for the purpose of research that includes treatment of the individual (e.g., clinical research trials) may condition the research-related treatment upon the individual's Authorization;

ii. Health plans may condition eligibility for benefits and enrollment in the health plan on Authorization for the use or disclosure of protected health information for the purposes of eligibility or enrollment determinations relating to the individual, or for underwriting and risk-rating determinations, provided the Authorization is not for the use or disclosure of psychotherapy notes;

iii. Covered entities may condition the provision of health care that is solely to create protected health information for disclosure to a third party on the provision of an Authorization for the disclosure of the protected health information to the third party. For example, a health care provider that provides pre-employment physicals may require that applicants for employment must sign an authorization to release the examination results to the employer.

**f. Validity of Patient Permission Obtained Prior to Compliance Date of Rule** (45 C.F.R. § 164.532)

Under certain circumstances, a covered entity may continue to use or disclose protected health information pursuant to any authorization or other express legal permission obtained prior to the compliance date of the Privacy Rule, even if these permissions do not meet the requirements of the Rule.

**i. Prior Legal Permission for Purposes Other Than Research**

If an individual previously permitted the use or disclosure of protected health information for specific purposes, the covered entity may use or disclose information created prior to the compliance date for those specific purposes, provided that the entity complies with all limitations placed upon the permission. The entity must, however, obtain an Authorization in conformity with the regulations in order to disclose protected health information obtained after the compliance date.

**ii. Prior Legal Permission for Purposes of Research**

A covered entity may use or disclose for a specific research study (either involving treatment or not) protected health information that is created or received either before or after the compliance date if the covered entity has obtained, prior to the compliance date, one of the following: an authorization or other express legal permission from an individual to use or disclose protected health information for the research study; informed consent from the individual to participate in the research study; or an IRB waiver of the informed consent for the research study.

**g. Marketing** (45 C.F.R. §§ 164.501; 164.508(a)(3))

**i. General Rule: Authorization Required**

Covered entities generally must obtain an Authorization before using or disclosing protected health information for marketing activities. "Marketing" includes any communication about a product or service that encourages the recipient to use or purchase that product or service. In addition, "marketing" includes any disclosure of protected health information that is made in exchange for direct or indirect remuneration for use in communication by a third party. This includes, for example, selling lists of patients to third parties or disclosing protected health information to a third party for its marketing activities. If the marketing activity involves direct or indirect remuneration to the covered entity from a third party, the Authorization must state that fact.

**ii. Exceptions Where No Authorization Is Required**

- A covered entity is not required to obtain an Authorization for:
  - the face-to-face marketing of products; or
  - the distribution of promotional gifts of nominal value (such as pens or calendars for self-promotion)
- "Marketing" does not include communications intended (1) to describe the entities in a health care network or to describe the products or services provided by a covered entity; (2) for treatment of the individual; or (3) for case management or care coordination, or to direct or recommend treatment alternatives. For example, health care providers can communicate with patients about treatment options and health care plans can inform patients of additional health coverage and value-added services such as discounts for prescription drugs or eyeglasses. Notably, these three types of communications may be made without Authorization regardless of whether remuneration is directly or indirectly received (e.g., health care providers may send prescription refill reminders to patients whether or not a third party pays for or subsidizes the communication).

**h. Fundraising** (45 C.F.R. § 164.514(f))

**i. Within Certain Parameters, Authorization Is Not Required**

A covered entity, business associate, or "institutionally related foundation" may use protected health information for fundraising on behalf of the covered entity, provided the information is limited to demographic information and the dates on which health care was provided. This fundraising is considered part of "health care operations" as defined in 45 C.F.R. § 164.501, and is therefore not required to have an Authorization. An "institutionally related foundation" is a nonprofit charitable foundation whose charter statement of charitable purposes includes an explicit linkage to the covered entity. Such a foundation may raise funds for the covered entity as well as other covered entities or health care providers explicitly provided for in its charter statement.

The covered entity must provide a statement in its Privacy Notice (discussed below) that the covered entity may make fundraising communications to the individual.

In addition, fundraising materials must explain how individuals may opt out of any future fundraising communications.

**ii. Authorization Required**

An Authorization is required for any use or disclosure of protected health information for fundraising purposes that does not fall within the parameters discussed above or within the definition of health care operations.

**i. Research** (45 C.F.R. §§ 164.501; 164.512(i); 164.508(b)(3)(i); 164.506(b)(4)(i))

The Privacy Rule defines "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." Research should be distinguished from "health care operations," which includes use or disclosure of patient data and information for purposes such as quality assessment and improvement or business planning or management. Research may be performed using health information that has been "de-identified" in accordance with the Privacy Rule without any Authorization.

The Privacy Rule (45 C.F.R. § 164.512(i)) requires that an Authorization be obtained in order to use or disclose protected health information for purposes of research, subject to three exceptions discussed below. The Privacy Rule requires only one Authorization for all uses and disclosures of protected health information, and the Authorization may be combined with any other legal permission related to the research study, including informed consent.

**i. Approval of IRB or Privacy Board**.

The first exception applies when an Institutional Review Board (IRB) or a Privacy Board changes or waives the Authorization (in whole or in part). The Privacy Board must be composed of persons with varying background and appropriate competency and include at least one member not affiliated with the covered entity or research sponsor. The IRB or Privacy Board must determine that the following waiver criteria, which are compatible with the federal "Common Rule" governing federally-funded research, are satisfied:

- The use or disclosure of protected health information involves no more than minimal risk to the individuals based on, at least, the presence of the following elements:

- An adequate plan to protect identifiers from improper use and disclosure;

- An adequate plan to destroy the identifiers at the earliest opportunity unless there is a health or research justification for retaining the identifiers or such retention is required by law; and

- Adequate written assurances that the protected health information will not be reused or disclosed except as permitted under the Privacy Rule.

- The research could not practicably be conducted without the alteration or waiver;

- The research could not practicably be conducted without access to or use of the protected health information;

The Privacy Rule contains detailed requirements for the review, approval and documentation of the IRB or Privacy Board Review process.

**ii. Reviews Preparatory to Research**.

This exception to requiring an Authorization for research applies for reviews preparatory to research, where the covered entity obtains the researcher's representations that use or disclosure is solely as needed to prepare a research protocol or for similar purposes preparatory to research; that no protected health information will be removed from the covered entity and that the use or access requested is necessary for the research purposes.

**iii. Research on Protected Health Information of Decedents**.

This exception to requiring an Authorization for research applies if the researcher represents to the covered entity that use or disclosure is sought solely for research on protected health information of decedents; the researcher provides documentation, at the request of the covered entity, of the death of such individual; and the requested protected health information is necessary for research purposes.

A covered entity that allows protected health information to be used without Authorization for research purposes under one or all of these exceptions must include a statement to this effect in its Privacy Notice.

In accordance with 45 C.F.R. § 164.514(d)(3)(iii)(D), a covered entity may rely on a request for protected health information from a researcher as the minimum necessary to accomplish the research if the documentation or representations described above for research without an Authorization are provided.

As discussed above, a covered entity may use or disclose for a specific research study (either involving treatment or not) protected health information that is created or received either before or after the compliance date if the covered entity has obtained, prior to the compliance date, one of the following: an authorization or other express legal permission from an individual to use or disclose protected health information for the research study; informed consent from the individual to participate in the research study; or an IRB waiver of the informed consent for the research study. (45 C.F.R. § 164.532(c))

**j. Psychotherapy Notes** (45 C.F.R. § 164.508(a)(2))

**i. General Rule: Authorization Required**

Generally, a covered entity must obtain an Authorization for use or disclosure of psychotherapy notes. "Psychotherapy notes" are broadly defined as notes recorded in any medium by a health care provider who is a mental health professional that (1) document and analyze the contents of conversations with a patient during individual or group counseling and (2) are kept separate from the rest of the patient's medical record.

**ii. Exceptions Where Authorization is Not Required**

An Authorization is not required if the psychotherapy notes are used by the originator of the psychotherapy notes for treatment purposes; or used or disclosed by the covered entity for its own training programs, or to defend itself in a legal action brought by the patient. In addition, Authorization is not required for health oversight activities with respect to the oversight of the originator of the psychotherapy notes, for use or disclosure about decedents to coroners and medical examiners, and for use or disclosure necessary to prevent or lessen a serious threat to the health or safety of the public or an individual.

**C. Minimum Necessary Uses, Disclosures and Requests** (45 C.F.R. §§ 164.502(b), 164.514(d))

The Privacy Rule provides that a covered entity must make reasonable efforts to ensure that it uses, discloses or requests only "the minimum amount [of protected health information] necessary to accomplish the intended purpose of the use or disclosure."

**1. Exceptions**

The minimum necessary requirement applies to disclosures, uses or requests for any purpose, but it does not apply to:

a. Disclosures to or requests by a health care provider for treatment;

b. Individual requests to access the individual's own information;

c. Uses or disclosures for which the covered entity has received an Authorization;

d. Uses or disclosures for HIPAA enforcement or compliance; or

e. Uses or disclosures required by law (e.g., worker's compensation).

**2. Implementation of Minimum Necessary Standard**

A covered entity must develop policies and procedures addressing access to and use of protected information by its workforce based on the workforce member's specific job duties.

For routine disclosures or requests, the Privacy Rule requires a covered entity to adopt and implement policies and procedures to limit disclosures and requests to the amount reasonably necessary to achieve the purpose of the disclosure or request. Non-routine disclosures and requests require an individualized review based upon predetermined criteria.

Under the minimum necessary requirement, a covered entity may not honor a request for an entire medical record unless the request is specifically justified as reasonably necessary to accomplish the purpose of the request. Likewise, a covered entity must develop policies and procedures that address when the use or disclosure of an entire medical record is justified.

**a. Uses of Protected Health Information**

Covered entities must develop policies and procedures to limit the use of protected health information to the minimum necessary. This is, essentially, a three-step process. The covered entity should first identify the persons or classes of persons in the entity's workforce who need access to protected health information to perform their job duties. Next, the covered entity must determine the nature of the information required by each class of workers and any conditions or restrictions that are appropriate for their access. Finally, the covered entity must make reasonable efforts to limit access accordingly.

*Example*: A covered entity might determine that nurses should have access to all protected health information of patients on their units, while on duty.

**b. Disclosures of Protected Health Information**

**i. Routine or recurring disclosure**

For all types of disclosures occurring on a routine or recurring basis, covered entities must implement policies and procedures to limit the information disclosed to the amount that is reasonably necessary to achieve the purpose of the disclosure. To do this, an entity must identify the types of protected health information to be disclosed, identify the types of persons who may receive the protected health information, and define the conditions that must be met for disclosure.

*Example*: A covered health care provider routinely discloses protected health information to health plans/third-party payers for purposes of claims payment. The covered health care provider should identify what protected information ordinarily may be disclosed to support the claims and the conditions for disclosure. As noted below, the covered entity could also rely on the request of the health plan/payer (a covered entity) as the minimum necessary to pay the claims, but is not required to do so.

**ii. Non-routine disclosures**

For non-routine disclosures, covered entities must develop reasonable criteria for determining and limiting information disclosed to the minimum necessary and individually review non-routine requests for disclosure in accordance with the criteria adopted.

A covered entity may rely on a requested disclosure as the minimum necessary for the purpose of the disclosure when the information is requested by:

- A public official who represents that the requested information is the minimum necessary;
- Another covered entity (health plan, covered health care provider, health care clearinghouse);

- A professional who is a member of the covered entity's 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 requested information is the minimum necessary; or

- A person requesting the information for research purposes, who has complied with other requirements outlined in the regulations.

**c. Requests by the Covered Entity for Protected Health Information**

For routine or recurring types of requests, covered entities may establish standards or protocols that describe what information is reasonably necessary for the purpose of the request and require that only that amount of information be requested by the covered entity. Covered entities should establish standards for individualized review of their non-routine requests for protected health information to ensure the request is appropriately limited.

**D. Personal Representatives** (45 C.F.R. § 164.502(g))

Covered entities must treat an individual's personal representative as the individual for purposes of the Privacy Rule (e.g., for disclosures of protected health information and for notice and access rights), including personal representatives for:

- incapacitated adults;

- unemancipated minors (however, any applicable State or other law governs disclosure);

- deceased individuals; and

- abuse, neglect or endangerment situations (however, any applicable State or other law governs disclosure).

**E. Business Associates** (45 C.F.R. §§ 160.103, 164.502(e), 164.504(e))

While the Privacy Rule applies directly only to providers, health plans, and health care clearinghouses, the reach of the Rule is extended through the concept of "business associates." A business associate relationship arises any time a person or entity uses, discloses, creates, or obtains individually identifiable health information in order to perform functions or activities on behalf of a covered entity, or when a person or entity provides certain services to or for a covered entity that involves the use or disclosure of protected health information. The Privacy Rule lists the following examples of the types of services that may give rise to a business associate relationship: legal; actuarial;

accounting; consulting; management; administrative; accreditation; data aggregation; financial services; claims processing or administration; data analysis; processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. These services were identified because they are commonly provided to covered entities and routinely require the disclosure of individually identifiable health information.

Members of the covered entity's workforce are not considered business associates. (45 C.F.R. § 160.103)

A covered entity may not disclose protected health information to a business associate and may not allow a business associate to create or receive protected health information on its behalf unless the covered entity obtains "satisfactory assurances" that the business associate will appropriately guard this information. The Rule requires that the covered entity document these assurances in a written contract. This contract between a covered entity and its business associate must:

1. Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not permit a business associate to use or disclose the information in a manner that would violate the Rule if done by the covered entity.

2. Provide that the business associate will:

    a. Not use or disclose the information other than as permitted under the contract or required by law;

    b. Use appropriate safeguards to prevent unauthorized uses or disclosures;

    c. Report any unauthorized use or disclosure to the covered entity;

    d. Ensure that any agent or subcontractor to whom it provides the information agrees to the same conditions;

    e. Make an individual's protected health information available if the individual requests it, subject to the requirements and conditions of the Rule;

    f. Make available protected health information for amendment and incorporate any amendments to protected health information;

    g. Make available information to provide an accounting of disclosures;

    h. Make its internal practices, books, and records relating to the use and disclosure of protected health information available to the federal

Department of Health and Human Services (HHS) to determine compliance;

i. Return or destroy all relevant protected health information at termination of the contract, if feasible, or if not feasible, extend protections of the contract and limit further uses.

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

(45 C.F.R. § 164.504(e)(1),(2)) The Appendix to the Privacy Rule contains model business associate contract provisions to assist covered entities in developing a contract to implement the requirements. Covered entities are not obligated to use the model and may choose to include provisions in addition to those required, such as indemnification and insurance.

A covered entity may be held responsible under the Privacy Rule for the actions of its business associates if it knows of a pattern of activity of the business associate that violates the business associate contract and fails to take reasonable steps to rectify the problem. If the covered entity discovers a problem and the problem is not rectified, it must terminate its contract with the business associate, if feasible. If termination is not feasible, the covered entity must report the problem to HHS.

A covered entity will be "deemed to be in compliance" with the business associate provisions if an existing written contract is not amended or renewed between October 15, 2002 and April 14, 2003. This "deemed compliance" will last only until renewal or modification of the agreement or April 14, 2004 (whichever is sooner). Even in the interim, however, the covered entity must still ensure certain of the "individual rights" guaranteed by HIPAA with respect to the information maintained by the business associate. This means that the covered entity must provide access to protected health information, the right to request amendment of protected health information, and the right to an accounting of disclosures of protected health information. The covered entity is also obligated to mitigate the harmful effects of any improper disclosures. All of these requirements will apply to information maintained or used by a contractor or vendor on the covered entities' behalf, even if the contractor is not yet bound by a business associate agreement.

Note further that according to Guidance issued by the Office for Civil Rights (the government agency charged with enforcing the HIPAA Privacy Rule), contracts with "evergreen" provisions which automatically renew are still eligible for the extension, even if the automatic renewal occurs between October 15, 2002 and April 14, 2003.

Significantly, HHS never adopted the highly controversial proposed requirement that business associate agreements include language making protected individuals third-party beneficiaries of the agreement. That language potentially could have given those

individuals the ability to sue under the business associate contract, even though the HIPAA statute does not expressly create a private right of action for protected individuals.

## F. Individual Rights

The Privacy Rule creates five basic individual rights and defines in detail the nature and limits of these rights and the specifications for their implementation.

### 1. Right to a Notice of the Covered Entity's Privacy Practices and Acknowledgement of Notice (45 C.F.R. § 164.520)

All covered entities must provide written notice in plain language of their privacy practices for protected health information ("Privacy Notice"). The Privacy Rule outlines in detail the elements required to be included in the Privacy Notice. A lengthy notice is required in order to include all of the required elements. If desired, a summary of the notice can be attached to the front of the complete notice (i.e., the "layered notice").

The Privacy Notice must inform the individual how the protected health information may be used, tell the individual how to file complaints with the covered entity and with HHS, and identify a contact person who can provide additional information. The Privacy Notice must reflect the applicable "more stringent" provisions of state law. (See Section IX of this Summary). The Privacy Notice should describe how the covered entity will provide individuals with a revised notice if the Privacy Notice is changed. The Privacy Rule requires health plans to inform their enrollees every three years about the availability of the Privacy Notice and how to obtain a copy of it. If a covered entity changes its privacy policies or procedures as outlined in the entity's Privacy Notice, it may make the changes effective for protected health information that it created or received prior to the effective date of its revision of the Privacy Notice only if the entity has previously included in its Privacy Notice a statement reserving the right to change its privacy procedures or policies and to make the new notice effective for all protected health information that it maintains.

Note that participants in an Organized Health Care Arrangement (OHCA) may use a joint Privacy Notice. Similarly, affiliated covered entities (ACEs) may distribute a single shared Privacy Notice.

A covered health care provider that has a direct treatment relationship with a patient must make a "good faith effort" to obtain the patient's written acknowledgement that the patient has received the provider's Privacy Notice. The provider must attempt to obtain the written acknowledgement no later than the date of first service delivery or, in an emergency treatment situation, as soon as reasonably practicable. If a written acknowledgement is not obtained from the

patient, the provider must document the good faith efforts made and indicate the reason why the acknowledgement was not obtained.

Covered health plans must provide a Privacy Notice to individuals at enrollment, within 60 days of a material revision to the Notice, and at least once every three years.

**2. Right to Request Restrictions on Protected Health Information and Right to Request Confidential Communications by Alternative Means** (45 C.F.R. § 164.522)

Individuals have the right to request restrictions on the use and disclosure of their protected health information. Covered entities are not required to agree to these requests, but if they do, they will be bound by them. A covered entity must document any restriction to which it agrees and maintain the documentation for at least six years.

Individuals also have the right to request that they receive communications involving protected health information by alternative means or at alternative locations. For example, a patient may request that the covered entity not telephone him or her at home. Covered entities must accommodate reasonable requests for alternative communications and covered health care providers may not require that patients explain the reasons for their requests.

**3. Right to Obtain Access to Protected Health Information for Inspection and Copying** (45 C.F.R. § 164.524)

Individuals have a right to access, inspect, and copy protected health information about themselves, subject to certain exceptions. For example, individuals do not have an automatic right to obtain psychotherapy notes (as narrowly defined in the Rule), information compiled for use in a civil, criminal, or administrative proceeding or information restricted from disclosure by the Clinical Laboratory Improvements Amendments of 1988 (CLIA). Additionally, access may be denied (subject to review) if in the judgment of a licensed health care professional the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. Covered entities must provide the right to access for as long as the health information is maintained.

**4. The Right to Obtain an Accounting of Disclosures** (45 C.F.R. § 164.528)

Individuals have a right to an accounting of disclosures made by a covered entity for purposes other than treatment, payment, or health care operations made within six years prior to the request. The accounting must include a brief statement of the information disclosed and the purpose of the disclosure and the name and address of the recipient of the disclosure. Certain types of disclosures are

exempted from such accountings, including disclosures for treatment, payment, or health care operations; incidental disclosures; disclosures made pursuant to an Authorization; disclosures for the facility's directory; disclosures made for national security or intelligence purposes; disclosures to law enforcement officials; disclosures as part of a limited data set; or disclosures made prior to the effective date of the Privacy Rule.

For multiple research disclosures that involve at least 50 records, a covered entity may use a simplified accounting by providing a description of the research for which an individual's protected health information may have been disclosed, and the researcher's contact information.

**5. The Right to Request Amendment of Protected Health Information** (45 C.F.R. § 164.526)

The regulations require that each covered entity establish a process for permitting individuals to request amendment and correction of their protected health information. Individuals may be required to make a request for amendment in writing and to provide a reason to support the request if informed of these requirements in advance. A covered entity may deny such a request if the information is:

a. accurate and complete;

b. not created by the covered entity;

c. not part of the designated record set; or

d. a type excluded from disclosure (see Section IV(F)(4) of this Summary, regarding 45 C.F.R. § 164.524).

If the requested amendment is denied, the covered entity must inform the individual of his/her options with respect to future disclosures of the information to which the individual objects.

NOTE: The Privacy Rule outlines in detail the procedures to be followed in complying with each of these individual rights requirements. The individual rights provisions of the Rule do not apply to clearinghouses, except that clearinghouses must provide an accounting of any disclosures for purposes other than treatment, payment or health care operations to individuals upon request.

**G. Administrative Requirements** (45 C.F.R. § 164.530)

The Privacy Rule imposes a variety of general administrative requirements in addition to the requirements discussed above.

**1. Privacy Official**

Covered entities must designate a privacy official responsible for the development of policies and procedures for the use and disclosure of protected health information. Participants in an Organized Health Care Arrangement (OHCA), for services covered under the OHCA, and Affiliated Covered Entities (ACEs) may designate a single Privacy Official.

**2. Internal Complaint Process**

Covered entities are required to implement an internal complaint process, including designating a contact person or office to receive complaints concerning compliance with the Privacy Rule and provide further explanation of any matters in the entity's Privacy Notice. A covered entity must document all complaints received and their resolution.

**3. Training**

Covered entities must provide training to all members of its workforce on the entity's policies and procedures with respect to protected health information as necessary and appropriate to carry out their functions within the covered entity. All members of the workforce, including employees, volunteers, trainees and other persons likely to obtain access to protected health information, were required to receive such training by the Privacy Rule's compliance date (April 14, 2003 for most entities). Each new member of the workforce must be trained within a reasonable time after the person joins the workforce. In addition, when a material change is made to a covered entity's privacy policies or procedures, all workforce members whose functions are affected by the change must be retrained. Training must be documented by the covered entity.

**4. Safeguards**

Covered entities are required to implement administrative, technical and physical safeguards to protect the integrity and privacy of protected health information. This requirement overlaps with certain requirements of the Security Rule. (see Section V of this Summary).

**5. Internal Sanctions**

Covered entities must develop and enforce internal sanctions against members of the entity's workforce who fail to comply with the entity's policies and procedures or the Privacy Rule, and document any sanctions that are applied.

**6. Mitigation in Event of Prohibited Use or Disclosure**

Covered entities are required to develop procedures to mitigate any deleterious effects of a prohibited use or disclosure.

**7. Non-retaliation**

Covered entities must refrain from retaliating against or intimidating any individual for exercising the individual's rights under the Privacy Rule, including filing a complaint with HHS, testifying, assisting, or participating in a compliance review, proceeding or hearing, or opposing an act the individual believes to be unlawful.

## H. Compliance and Enforcement Under the Privacy Rule

**1. Delegation of Authority to the Office for Civil Rights**

The Secretary of HHS has officially delegated authority to administer, interpret and implement the privacy standards to the Office for Civil Rights ("OCR"). Pursuant to the delegation, OCR also has the authority to impose civil fines and to enforce the privacy standards. (See Statement of Delegation Authority, 65 Fed. Reg. 82,381)

**2. Enforcement Approach** (45 C.F.R. § 160.304)

The enforcement approach outlined by HHS in the Privacy Rule favors cooperation between HHS and covered entities. The Rule focuses on attaining voluntary enforcement. To this end, OCR is authorized to provide technical assistance to covered entities and has developed guidance and other technical assistance to help covered entities effectively implement the Privacy Rule. (see postings on OCR web site, http://www.hhs.gov/ocr/hipaa). Also, HHS has published an interim final rule (the "Enforcement Rule") on civil monetary penalties and enforcement procedures. See discussion below at Section VIII.

**3. Individual Complaints and OCR Compliance Reviews** (45 C.F.R. §§ 160.306, 160.308, 160.312)

An individual who believes that a covered entity is not acting in compliance with regulations, standards, requirements or implementation specifications may file a complaint with OCR. The complaint must be in writing (either on paper or electronically) and must specify the name of the covered entity and the alleged actions or omissions believed to be in violation. The complaint must be filed within 180 days of the date on which the complainant knew or should have known of the alleged action or omission (unless waived by the Secretary of HHS).

For covered entities located in Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island or Vermont, complaints may be mailed or faxed to:

Region I, Office for Civil Rights
U.S. Dept. of Health & Human Services
Government Center
J.F. Kennedy Federal Building – Room 1875
Boston, MA 02203
FAX (617) 565-3809

For covered entities located in New Jersey, New York, Puerto Rico, or the Virgin Islands, complaints may be mailed or faxed to:

Region II, Office for Civil Rights
U.S. Dept. of Health & Human Services
Jacob Javits Federal Building
26 Federal Plaza – Suite 3312
New York, NY 10278
FAX (212) 264-3039

For the addresses applicable to covered entities in other states, refer to 68 Fed. Reg. 13,711 (March 20, 2003). All complaints filed by email may be sent to: OCRComplaint@hhs.gov.

OCR may investigate any complaint and, if a violation is found, shall attempt to resolve the matter informally. If the matter cannot be resolved informally, the Secretary may issue written findings documenting the non-compliance, which will be given to the covered entity as well as the complainant.

OCR may also conduct compliance reviews independently of any complaint being filed.

**4. Covered Entity's Compliance Responsibilities** (45 C.F.R. § 160.310)

In order to facilitate compliance, a covered entity is required to:

a. Keep records and submit compliance reports when required by the HHS Secretary;

b. Cooperate with complaint investigations and compliance reviews; and

c. Permit the Secretary access to its facilities, books, records, accounts, and other sources of information relevant to ascertaining compliance with applicable requirements, standards, and implementation specifications.

If information sought by the Secretary is in the exclusive possession of another agency, institution, or person, and that person fails to release the information, the covered entity must certify that this is the case and explain the efforts it made to obtain the information.

**5. Potential Penalties**

See Section VIII of this Summary.

## V. HIPAA SECURITY REGULATIONS (SECURITY RULE)

HHS published the final HIPAA security regulations on February 20, 2003. (68 Fed. Reg. 8,334 *et seq.*; see proposed security regulations at 63 Fed. Reg. 43,242 *et seq.* (Aug. 12, 1998)) The regulations require covered entities to implement administrative, physical and technical safeguards to protect certain health information. The final regulations use many of the same terms and definitions as the HIPAA privacy standards to make it easier for covered entities to comply; one major difference between HIPAA privacy and security is that the security regulations apply only to electronic protected health information, while the privacy regulations require safeguards for all PHI, including PHI on paper or in electronic form. Under the security regulations, electronic PHI includes PHI stored on a computer disk, magnetic tape or computer hard drive, or PHI that is transmitted over the Internet; electronic PHI does not include PHI on paper sent by fax or oral PHI transmitted by phone.

The Security Rule applies to the same three types of health care organizations that are covered by the Privacy Rule: health care providers that transmit health information electronically, health plans and health care clearinghouses. The final Security Rule went into effect on April 21, 2003 and covered entities have until April 21, 2005 to comply (small health plans have until April 21, 2006). Like the privacy regulations, the Security Rule is designed to be flexible (as well as "technology-neutral") to fit an organization's unique characteristics and technical environment. According to HHS, "[h]ow individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make." (63 Fed. Reg. 43,250)

### A. General Requirements.

1. A covered entity is required to protect the confidentiality, integrity and availability of electronic PHI that it creates, stores, maintains or transmits.

2. The regulations categorize the required administrative, physical and technical safeguards into 18 security standards, many of which are accompanied by "implementation specifications." Each of the implementation specifications is either "required" or "addressable." If HHS has indicated that an implementation specification is addressable, the covered entity must implement it only if the covered entity determines that it is a "reasonable and appropriate safeguard." A matrix of the security standards and implementation specifications is included at the end of this Section (adapted from 68 Fed. Reg. 8,380 (Feb. 20, 2003)).

3. The regulations include standards for business associate contracts and other arrangements, and standards for plan documents of group health plans.

4. The security regulations require covered entities to adopt formal security policies and procedures in written or electronic form and to document any activity that is required by the regulations.

**B. Administrative Safeguards** (45 C.F.R. § 164.308)

Covered entities must have:

1. A security management process involving risk analysis and risk management of the security process to prevent, detect, contain and correct security violations. This includes the establishment of accountability, management controls, electronic controls, security, and penalties for the abuse and misuse of physical and electronic assets. The entity must develop disciplinary and sanctions policies for employees, contractors, and agents as well as security policy statements. Regular record review of information system activity, such as audit logs, access reports and security incident tracking reports, is also required.

2. Assignment of security responsibility to manage the execution and use of security measures and the conduct of personnel.

3. Workforce security procedures to ensure that members of the workforce have appropriately limited access to electronic PHI. Addressable procedures include supervision and oversight of personnel; establishing personnel clearance and security policies and procedures for personnel with access to sensitive information; and implementing procedures for terminating access to PHI when employment ends. Termination procedures could include changing locks, removing the user from access lists, removing user accounts, and requiring the user to turn in keys, tokens, or cards that allow access to electronic PHI.

4. Information access management, including formal documented policies and procedures for granting different levels of access to health care information and isolating health care clearinghouse functions. Addressable specifications include access authorizations, access establishment, and access modification.

5. Training of all members of the workforce, including management, on security awareness and security policies and procedures. Addressable specifications include periodic security reminders, user education on virus protection, training on the importance of monitoring log-in success or failure and password management.

6. Security incident procedures including formal, documented procedures for reporting and responding to security breaches.

7. A "contingency plan" that is routinely updated and establishes policies and procedures for responding to an emergency such as fire, vandalism, system failure or natural disaster. The plan must include procedures for data backup, disaster recovery and emergency mode operations. Addressable specifications include testing and revision procedures and applications and data criticality analysis.

8. Periodic technical and non-technical evaluations to determine compliance with the security regulations.

**C. Physical Safeguards** (45 C.F.R. § 164.310)

Covered entities must have:

1. Facility access controls including policies that limit physical access to the facility and its electronic information systems while ensuring that properly authorized access is allowed. Addressable specifications include disaster recovery and emergency mode policies and procedures; a plan to safeguard the premises from unauthorized physical access; procedures for verifying a person's authorization to access a facility or electronic PHI, including visitor control procedures; and maintenance of records of repairs and modifications to security-related mechanisms such as hardware, doors and locks.

2. Policy and guidelines on workstation use, including proper functioning at each workstation and the physical surroundings of a workstation.

3. Secure workstation locations to eliminate or minimize the possibility of unauthorized access.

4. Device and media controls including policies and procedures governing the receipt and removal of hardware and software into and out of a facility and within a facility. This will include procedures on data disposal and media re-use such as removing data from a computer's hard drive before making it available for re-use. Addressable specifications include accountability for any movement of hardware or electronic media and data backup and storage.

**D. Technical Safeguards** (45 C.F.R. § 164.312)

Covered entities must have:

1. Access controls for the electronic information system, including unique user identification and an emergency access procedure. Addressable specifications include automatic logoff after a predetermined time of inactivity, encryption and decryption.

2. Audit control mechanisms to record and examine information system activity.

3. Data integrity to ensure that data has not been improperly altered or destroyed.

4. Person or entity authentication to ensure that the person or entity asking for electronic PHI is the one claimed.

5. Technical security measures to guard against unauthorized access to data that is transmitted over a communications network. Addressable specifications include integrity controls to ensure that data is not improperly modified, and encryption where appropriate.

## SECURITY STANDARDS: MATRIX

| Standards | Sections | Implementation Specifications (R) = Required, (A) = Addressable |
|---|---|---|
| **Administrative Safeguards** | | |
| Security Management Process | 164.308(a)(1) | Risk Analysis (R) |
| | | Risk Management (R) |
| | | Sanction Policy (R) |
| | | Information System Activity Review (R) |
| Assigned Security Responsibility | 164.308(a)(2) | (R) |
| Workforce Security | 164.308(a)(3) | Authorization and/or Supervision (A) |
| | | Workforce Clearance Procedure |
| | | Termination Procedures (A) |
| Information Access Management | 164.308(a)(4) | Isolating Health Care Clearinghouse Function (R) |
| | | Access Authorization (A) |
| | | Access Establishment and Modification (A) |
| Security Awareness and Training | 164.308(a)(5) | Security Reminders (A) |
| | | Protection from Malicious Software (A) |
| | | Log-in Monitoring (A) |
| | | Password Management (A) |
| Security Incident Procedures | 164.308(a)(6) | Response and Reporting (R) |
| Contingency Plan | 164.308(a)(7) | Data Backup Plan (R) |
| | | Disaster Recovery Plan (R) |
| | | Emergency Mode Operation Plan (R) |
| | | Testing and Revision Procedure (A) |
| | | Applications and Data Criticality Analysis (A) |
| Evaluation | 164.308(a)(8) | (R) |
| Business Associate Contracts and Other Arrangement | 164.308(b)(1) | Written Contract or Other Arrangement (R) |
| **Physical Safeguards** | | |
| Facility Access Controls | 164.310(a)(1) | Contingency Operations (A) |
| | | Facility Security Plan (A) |
| | | Access Control and Validation Procedures (A) |
| | | Maintenance Records (A) |
| Workstation Use | 164.310(b) | (R) |
| Workstation Security | 164.310(c) | (R) |
| Device and Media Controls | 164.310(d)(1) | Disposal (R) |
| | | Media Re-use (R) |
| | | Accountability (A) |
| | | Data Backup and Storage (A) |
| **Technical Safeguards** | | |
| Access Control | 164.312(a)(1) | Unique User Identification (R) |
| | | Emergency Access Procedure (R) |
| | | Automatic Logoff (A) |
| | | Encryption and Decryption (A) |
| Audit Controls | 164.312(b) | (R) |
| Integrity | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Informati |
| Person or Entity Authentication | 164.312(d) | (R) |
| Transmission Security | 164.312(e)(1) | Integrity Controls (A) |
| | | Encryption (A) |

## IV. HIPAA REGULATIONS ON ELECTRONIC TRANSACTIONS AND CODE SETS (TRANSACTIONS AND CODE SETS RULE)

### A. Background

The HIPAA statute required that the HHS Secretary adopt standards for certain transactions and data elements for these transactions to standardize the electronic exchange of health information. HIPAA also required the HHS Secretary to establish standard code sets to be used with the standard transactions, selecting when possible from code sets previously developed by private and public industry groups. Congress required that, in developing the required transactions and code sets, HHS consult with national standard setting organizations, such as the American National Standards Institute ("ANSI") and its Accredited Standards Committee ("ASC") X12N Subcommittee, before adopting any required standards for the electronic exchange of health information.

### B. Publication of Regulations and Implementation Guides

On August 17, 2000, HHS published final regulations addressing standards for electronic transactions and code sets. (65 Fed. Reg. 50,312 *et seq*.) The regulations adopted standards for the following eight electronic transactions:[4]

1. Health care claims or equivalent encounter information
2. Eligibility for a health plan
3. Referral certification and authorization
4. Health care claim status
5. Enrollment and disenrollment in a health plan
6. Health care payment and remittance advice
7. Health plan premium payments
8. Coordination of benefits

The regulations also adopted a number of existing medical coding systems (including ICD-9-CM, CPT-4, HCPCS, CDT, and NDC) to be used in the standard transactions. The regulations became effective October 16, 2000 and originally required compliance by October 16, 2002 (except for small health plans, which were given an original compliance date of October 16, 2003).

On December 27, 2001, President Bush signed into law the Administrative Simplification and Compliance Act ("ASCA"). ASCA extended the compliance date to October 16, 2003 if the covered entity submitted a compliance plan to HHS by October 15, 2002, one day prior to the original compliance deadline. ASCA authorized HHS to exclude from Medicare any covered entity that did not file a compliance plan or was not in compliance

[4] "Transactions" are defined also to include three additional types of information exchanges: first report of injury, health claims attachments, and other transactions the Secretary may prescribe by regulation; however, HHS has not yet adopted standards for these transactions. (45 C.F.R. § 160.103)

with the requirements by October 16, 2002. Congress mandated in ASCA that HHS issue a model compliance plan for covered entities, and on March 29, 2002, HHS issued the model compliance plan requiring the covered entity to address the reason for extension request, the workplan for achieving compliance and plans to begin testing by April 14, 2003.

HIPAA requirements for standard transactions are included both in the regulations and in detailed technical "implementation guides" established for each transaction by the HHS contractor, the Washington Publishing Company, 5284 Randolph Road, Rockville, MD, 20852-2116; telephone 301-949-9740; fax 301-949-9472. The implementation guides are available through the Washington Publishing Company's website at http://www.wpc-edi.com. For each designated transaction, the standards specify the format, the data elements required or permitted to structure the format, and the data content permitted for each of the data elements, including designated code sets where applicable.

## C. Transactions and Code Sets Requirements

Under the Transactions and Code Sets Rule, if a "covered entity" conducts with another "covered entity" (or within the same covered entity, unless excepted) using "electronic media," a transaction for which the Secretary has adopted a standard by regulation, the covered entity must conduct the transaction as a standard transaction. (45 C.F.R. § 162.923(a)) The regulations define "electronic media" to include transmissions over the Internet, over the "extranet" (using internet technology to link a business with information only accessible to collaborating parties), 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 disk media. (45 C.F.R. § 162.103)

A covered entity may use a "business associate," including a health care clearinghouse, to conduct a covered transaction and thus achieve compliance through a contracted entity so long as the business associate complies with the regulations. (45 C.F.R. § 162.923(c)(1)) The regulations briefly address "trading partner agreements," defined as an agreement relating to the exchange of information in electronic transactions. (45 C.F.R. § 160.103) Trading partner agreements may not contain provisions that change or add data elements or conditions or change the meaning or intent of a standard's implementation specifications. (45 C.F.R. § 162.915)

Modifications to the final Transaction Standard and Code Sets rule, published on February 20, 2003, include:

- repealing the National Drug Code (NDC) as the standard medical data code set for reporting drugs and biologics in all non-retail pharmacy transactions;

- adopting changes to the implementation guides with some technical revisions;

- certain changes for retail pharmacy transactions such as continuing the use of the NDC code set for the reporting of drugs and biologics; and

- adopting modified standards for two transactions: health plan premium payments and coordination of benefits.

Use of the HIPAA-mandated transaction standards and code sets may require providers to collect and maintain data elements that have not previously been collected and will require education of individuals who work in areas relating to billing and claims review and payment. Significantly, implementing the standards will eliminate the previous wide-spread use of non-uniform "local codes" by individual insurers and other payers.

Providers should determine whether they conduct any of the transactions covered by these HIPAA regulations governing electronic transactions. It is advisable to consult with vendors to determine their ability to comply with the standards for electronic transactions and to determine further whether the provider is collecting and maintaining all necessary data elements to comply with the transactions standards.

## VII. OTHER HIPAA REGULATIONS

### A. Employer Identifier

CMS published a Final Rule on May 31, 2002 (67 Fed. Reg. 38,009) which will be codified at 45 C.F.R. Parts 160 and 162, adopting as the standard employer identifier the taxpayer employer identification number ("EIN") assigned by the Internal Revenue Service. (63 Fed. Reg. 32,784). The proposed rule had been issued June 16, 1998. (63 Fed. Reg. 32,784).

Under the Rule, providers, health plans, and health care clearinghouses are obligated to use an employer's EIN in electronic transactions that require an employer identifier. Each employer is required to disclose its EIN, when requested, to any covered entity that conducts electronic transactions that require the employer's identifier.

Health plans, health care clearinghouses, and health care providers must comply with this Rule by July 30, 2004, and small health plans must comply by Aug. 1, 2005.

### B. Electronic Signature

The proposed security regulations had provided for a "digital signature" to be the electronic signature standard (proposed 45 C.F.R. § 142.310). A "digital signature" is an electronic signature authenticated using cryptographic methods. However, HHS did not address electronic signatures in the final security regulations and thus, this proposed provision has not been adopted.

### C. Health Care Provider Identifier

On May 7, 1998, CMS issued a proposed rule that the standard health care provider identifier be a "national provider identifier" ("NPI") overseen and managed by CMS. (63 Fed. Reg. 25,320). The NPI would be an eight-position alphanumeric identifier, which would include as the eighth position a "check" digit to assist in identifying invalid NPIs. As of this writing, the final provider identifier rule is expected to be published in 2003.

#### 1. Use of NPIs in Connection with Electronic Transactions

Health plans and health care clearinghouses would be bound to use the NPI in all HIPAA electronic transactions wherever required. Each health care provider would be obligated to use the NPI wherever required on all HIPAA electronic transactions it directly transmits or accepts. The NPI application process has not been established; however, the proposed rule outlines options for obtaining a NPI, including possible automatic assignment of NPIs to health care providers already participating in Medicare, Medicaid or other federal programs.

### 2. Other Approved Uses

The proposed rule lists approved uses of the NPI, in addition to its use in electronic transactions. The NPI may be used in fraud and abuse files and "other program integrity files (for example, the HHS Office of the Inspector General sanction file)" as well as to identify health care providers for debt collection and "for any other lawful activity requiring individual identification of health care providers." (63 Fed. Reg. 25,334)

## D. Individual Health Identifier

HHS has not yet issued a proposed rule for individual unique health identifiers. In light of the serious privacy issues raised by use of a unique health identifier, we understand that prior to issuing a proposed rule the Secretary plans to first issue a notice of intent to discuss options for a unique identifier and to ask for public comment.

In addition, the National Committee on Vital Health Statistics ("NCVHS"), the body appointed under HIPAA to advise the Secretary on standards issues, recommended that HHS refrain from adopting a standard individual identifier until after privacy legislation is enacted. (See HHS White Paper on Unique Health Identifier for Individuals at p. 5)

## E. Health Plan Identifier

HHS has not yet issued a proposed rule for the health plan identifier.

## VIII. ENFORCEMENT AND PENALTIES FOR VIOLATIONS OF HIPAA

The HIPAA statute grants the Secretary of HHS authority to impose civil monetary penalties against covered entities that are non-compliant with HIPAA requirements and to establish criminal penalties for certain wrongful disclosures of protected health information. (42 U.S.C. §§ 1320d, 1320c)

Potential civil penalties for non-compliance with HIPAA include a fine of up to $100 for each violation with a $250,000 per calendar year maximum for "violations of an identical requirement or prohibition." A penalty may not be imposed if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated that provision. Additionally, penalties will not be imposed if the failure to comply was due to reasonable cause and not to willful neglect, and such failure is corrected during the thirty-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

Criminal penalties may be applied to a person who knowingly and in violation of HIPAA: (1) Uses or causes use of a unique health identifier; (2) Obtains individually identifiable health information relating to an individual; or (3) Discloses individually identifiable health information to another person. Such penalties may include: (1) Fines of up to $50,000 or imprisonment for up to a year, or both; (2) For an offense committed under false pretenses, fines up to $100,000, imprisonment for up to five years, or both; and (3) If an offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, fines up to $250,000, imprisonment up to ten years, or both.

On April 17, 2003, HHS published an interim final rule on civil monetary penalties: procedures for investigations, imposition of penalties, and hearings (68 Fed. Reg. 18,895-18,906). This interim rule is the first installment of what HHS is calling the "Enforcement Rule" and became effective May 19, 2003. The Enforcement Rule covers procedures for investigations and hearings such as subpoenas, settlement, discovery, exchange of witness lists, evidence, motions, penalties, hearings before an administrative law judge and judicial review. However, the preamble to the Enforcement Rule restates that HHS's general approach to HIPAA enforcement will be to seek voluntary compliance through technical assistance and to resolve privacy matters by informal means before issuing findings of non-compliance. (68 Fed. Reg. 18,897).

In addition, under the Administrative Simplification and Compliance Act, which extended the date by which a covered entity that submitted a compliance plan must be in compliance with the standards for electronic transactions and code sets, HHS was authorized to exclude from Medicare any covered entity that did not file a compliance plan or was not in compliance with the Transactions and Code Sets standards by October 16, 2002.

## IX. EFFECT ON STATE LAW

### A. General HIPAA Preemption

Generally, the HIPAA statute (42 U.S.C. § 1320d-7) provides that HIPAA law and regulations will supersede any contrary provisions of state law, including any provision that requires medical or health plan records to be maintained or transmitted in written rather than electronic form. In practice, most state laws governing health information issues will not be preempted as covered entities are able to comply with both the state law requirement and any HIPAA-related requirements.

State laws regulating the privacy of health information that are more stringent than the regulations are not preempted, as further explained below. Provisions of state law that provide for reporting of disease or injury, child abuse, birth, death, or for public health surveillance, investigation or intervention are also not preempted. Finally, provisions of state law that require a health plan to report, or to provide access to information for the purpose of management or financial audits, program monitoring and evaluation, or licensure and certification are not preempted. (45 C.F.R. § 160.203)

### B. State Exemption Process

HHS may except a particular state law from preemption where:

1. The law is necessary to prevent fraud or abuse, insure appropriate state regulation of insurance and health plans, allow state reporting on health care delivery or costs, or where HHS determines that a compelling issue of public health, safety, or welfare outweighs the intrusion upon privacy interests; or

2. Where the principal purpose of the state law is to regulate the manufacture, distribution, or dispensing of a controlled substance. (45 C.F.R. § 160.203(a))

   In order for a state law to be excepted under this provision, the state, or any person, must submit a written request to the Secretary (under 45 C.F.R. § 160.204) detailing:

   a. The state law for which the exception is requested;

   b. The standard, regulation, or implementation specification from which the exception is requested;

   c. The part of the standard, regulation or implementation specification that will not be implemented if the request for exception is granted;

   d. How the exception will impact health care providers, health plans and other entities; and

e. The reasons why the state law should not be preempted, including how the state law meets the criteria described above.

The address for submission of requests for preemption exception determinations is:

Director
Office for Civil Rights
Dept. of Health and Human Services
Mail Stop Room 506F
Hubert H. Humphrey Bldg.
200 Independence Ave., SW
Washington, DC 20201

(68 Fed. Reg. 11,554 (March 11, 2003)). The Secretary may request additional information in order to make the determination.

**C. "More Stringent" State Privacy Requirements** (42 U.S.C. § 1320d-7; 45 C.F.R. Part 160, Subpart B).

State laws[5] that are "more stringent" than the Privacy Rule (including standards, requirements and implementation specifications) are not preempted. Generally, a state requirement is "more stringent" when it provides for a more limited use or disclosure of information; permits individuals greater rights of access or amendment; requires more information to be provided individuals; provides for greater recordkeeping or retention requirements; or otherwise provides greater privacy protection. State provisions concerning authorizations for use or disclosure are "more stringent" if they provide requirements that narrow the scope or duration of the authorization, increase the privacy protections afforded or reduce the coercive effect surrounding authorizations or consent. (45 C.F.R. § 160.202)

State laws concerning the disclosure of HIV/AIDS information, substance abuse treatment records, psychiatric treatment records and genetic information, among others, should be carefully analyzed to determine whether the state requirement (usually, a restriction on disclosure) is "more stringent" than the Privacy Rule.



[5] For purpose of these preemption provisions, "state law" includes any constitution, statute, regulation, rule or other state action (including court decisions) having the effect of law. (45 C.F.R. § 160.202)