Part 6
Introduction to HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted for several reasons, such as to:

- Improve portability and continuity of health insurance coverage;
- Combat waste, fraud, and abuse in health insurance and delivery of health care;
- Promote the use of medical savings accounts;
- Improve access to long-term care services and coverage; and
- Simplify the administration of health insurance.

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing and enforcing various unrelated provisions within HIPAA, therefore HIPAA may have different meanings depending on the circumstances. The two HIPAA provisions that are addressed within this document because they pertain specifically to CMS are HIPAA Insurance Reform (Title I) and HIPAA Administrative Simplification (Title II).

WHAT ROLE DOES CMS HAVE WITH HIPAA?

CMS is responsible for implementing and enforcing the following unrelated provisions of HIPAA:

- **HIPAA Insurance Reform** - Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- **HIPAA Administrative Simplification** - Title II of HIPAA requires the Secretary of the Department of Health and Human Services (DHHS) to establish national standards for electronic healthcare transactions and national identifiers for providers, suppliers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in health care. Although HIPAA was enacted in 1996, each provision of the

Administration Simplification is set into motion through the issuing of proposed and final regulations. Thus, each part of the Administrative Simplification has different effective dates and different compliance deadlines. CMS is responsible for implementing and enforcing all Administrative Simplification provisions except privacy.

WHAT ARE THE ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS?

The Administrative Simplification Requirements of HIPAA impact healthcare providers and suppliers who do business electronically, as well as many of their healthcare business partners. Many changes involve complex computer system modifications. The Administrative Simplification

Information Regarding HIPAA Requirements and Coverage

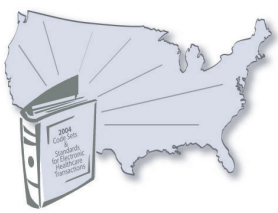
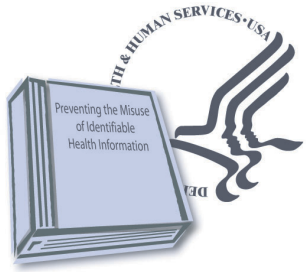
For help with determining whether you are a covered entity, access the decision tool at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp on the Web, or access coverage information at http://www.hhs.gov/ocr/hipaa/ on the Web.

For additional information regarding HIPAA requirements and coverage as a covered entity, contact the HIPAA Hotline at 1-866-282-0659.

Requirements of HIPAA consist of four parts (see Table 6-1.)

The Administrative Simplification standards adopted by the Secretary of DHHS under HIPAA apply to any entity that is:

Table 6-1. HIPAA Administrative Simplification Requirements.

Electronic Transactions and Code Sets	Security	Unique Identifiers	Privacy
			
HIPAA requires the adoption and use of national standards for certain healthcare electronic transactions and code sets.	HIPAA addresses how electronic health information that is stored, transmitted, and accessed should be secured.	HIPAA requires providers, suppliers, health plans, and employers to adopt and use unique identifiers.	Under HIPAA, covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. The privacy requirements are overseen by the Office of Civil Rights (OCR), an agency within the Department of Health and Human Services (DHHS).

- A healthcare provider or supplier that conducts certain transactions in electronic form or who use a billing service to conduct transactions on his or her behalf.
- All healthcare clearinghouses.
- All health plans.

An entity that is one or more of these types is referred to as a "covered entity" and must comply with the Administrative Simplification requirements of the HIPAA regulations.

ELECTRONIC TRANSACTIONS AND MEDICAL CODE SETS

Under HIPAA, electronic transactions are allowed provided that the transactions meet the requirements established. The requirements include adoption of national standards for electronic transactions, and use of standardized medical code sets used to encode data.

Table 6-2 lists the current electronic standard requirements.

ELECTRONIC TRANSACTIONS

Transactions are activities involving the transfer of healthcare information for specific purposes. Under HIPAA Administration Simplification, if a healthcare provider or supplier engages in one of the identified transactions, he or she must comply with the standard for that transaction. HIPAA requires every provider or supplier who does business electronically to use the same healthcare transaction standards, code sets, and identifiers. HIPAA has identified the following 10 National Standards for Electronic Data Interchange (EDI) for the transmission of healthcare data:

- Premium payments;
- Enrollment in and disenrollment from a health plan;
- Eligibility inquiry and response;
- Referrals and authorizations;
- Claims/encounter data;
- Claim status inquiry and response;
- Payment and Remittance Advice (RA);
- Coordination of Benefits (COB);

Table 6-2. Electronic Standard Requirements.

Electronic Transactions Standards for:	
Claims or Encounters and Coordination of Benefits (COB)	ASC X12N 837 - Professional Healthcare Claims ASC X12N 837 - Institutional Healthcare Claims ASC X12N 837 - Dental Healthcare Claims NCPDP - Telecommunication Version 5.1 and Batch Standard 1.1 - Retail Pharmacy Claims
Healthcare Payment and Remittance Advice (RA)	ASC X12N 835 - Healthcare Payment/Advice
Health Claims Status	ASC X12N 276/277 - Healthcare Claim Status, Request and Response
Eligibility for a Health Plan	ASC X12N 270/271 - Healthcare Eligibility Benefit Inquiry/Response NCPDP - Telecommunication Version 5.1 and Batch Standard 1.1 - Retail Pharmacy Claims
Referral Certification and Authorization	ASC X12N 278 - Healthcare services review - request for review and response NCPDP - Telecommunication Version 5.1 and Batch Standard 1.1 - Retail Pharmacy Claims
Enrollment and Disenrollment in a Health Plan	ASC X12N 834 - Benefit Enrollment and Maintenance
Health Plan Premium Payments	ASC X12N 820 - Payment Order/RA

Transaction Standards, Final Rule Guidelines, Code Set, and Identifier Information
Additional information regarding regulations governing transaction standards, Final Rule implementation guidelines, code sets, and identifier information can be found at http://www.cms.hhs.gov/hipaa/hipaa2/regulations on the Web.

HIPPA Implementation Guides
These guides may be downloaded for free at http://www.wpc-edi.com/hipaa/HIPAA_40.asp on the Web.

- First report of injury (pending); and
- Claim attachments (pending).

Standards have been developed for eight of the 10 transactions. Transaction standards have not been developed for claims attachments or for the first report of injury.

Not every covered entity will conduct all of the transactions. For instance, healthcare providers or suppliers would not engage in enrollment into, and disenrollment from, a health plan.

The Standards Development Organizations (SDOs) have developed implementation guides to assist covered entities and their business associates. The implementation guides provide the adopted implementation specifications and comprehensive technical details for HIPAA implementation and include detailed technical specifications that explain how to conduct a standard transaction. These details and specifications include:

- Format specification - how information should be arranged;
- Content specification - what information should be included; and
- Certain code sets - how information will be included using representational codes.

For example, the guides provide important information for an Information Technology (IT) group or vendor that handles electronic data exchange.

Providers and suppliers should also contact their payers and inquire whether they have companion guides available to accompany the implementation guides. If available, companion guides can provide additional information that is helpful in interpreting the implementation guides.

STANDARD MEDICAL CODE SETS

In addition to transaction standards, HIPAA regulations also require the use of standard code sets. Medical code sets include any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis, or medical procedure codes. The codes are an integral part of electronic transactions and are used to describe various healthcare services, procedures, tests, supplies, drugs, patient diagnoses; as well as many administrative activities.

E/M Code Information
The most recent E/M codes are contained within Chapter 6 of the *Medicare Resident and New Physician Training Manual*, which is available at http://www.cms.hhs.gov/medlearn. The prescribed use of the E/M codes is contained with Documentation Guidelines (DGs), which will be available at http://www.cms.hhs.gov/medlearn/emdoc.asp on the Web.

HIPAA refers to code sets as either medical codes (clinical codes) or non-medical codes (non-clinical codes). A subset of the Current Procedure Terminology (CPT)-4 codes includes a set of cognitive Evaluation and Management Service (E/M) codes. These codes are used by all types of physicians to document services performed during patient care. These codes explain how the physician gathered and analyzed information about the patient's illness, determined a condition, and devised the best treatment or course of treatment.

Table 6-2 outlines the code sets that have been adopted under HIPAA.

The transactions and code set regulation adopted these first sets of HIPAA standards. It also created a process to allow anyone to request a change in the standards. Six organizations known as Designated Standards Maintenance Organizations (DSMOs) were designated by the Secretary of DHHS and have agreed to work together to collect requests for changes to HIPAA standards, evaluate the requests, and suggest changes to the standards for the Secretary's consideration.

The six DSMOs include:

- Accredited Standards Committee X12N;
- Health Level Seven, Inc.;
- National Council for Prescription Drug Programs;
- National Uniform Billing Committee;
- National Uniform Claim Committee; and
- American Dental Association (ADA).

DSMO Modification Process
The Secretary may modify a standard, or its implementation guide, no more frequently than once every 12 months. The latest information on the DSMO Modification process can be found at http://www.hipaa-dsmo.org on the Web.

Table 6-2. HIPPA-Adopted Medical Code Sets.

HIPPA-Adopted Medical Code Sets for:	
Diagnosis	International Classification of Diseases, 9th revision, Clinical Modification, Vol. 1 & 2 (ICD -9-CM) codes [these volumes are maintained by the Center for Disease Control (CDC)]
Services provided by physicians and other professionals	CPT-4 codes [maintained and copyrighted by the American Medical Association (AMA)]
Products, supplies, and services not included in the CPT-4	HCPCS (Healthcare Common Procedure Coding System) codes [maintained by CMS, Blue Cross Blue Shield (BCBS) associations, and the Health Insurance Association of America]
Dental Terminology	Code used for dental procedures and nomenclature [maintained and copyrighted by the American Dental Association (ADA)]
National Drug Codes (NDCs)	Codes used by retail pharmacies and maintained by the Food and Drug Administration (FDA) within the Department of Health and Human Services (DHHS)]
Remark Codes	Codes used to inform the provider or supplier why a request for payment was fully or partially denied (codes approved by the Accredited Standards Committee X12 and maintained by CMS)
Reason Codes	Codes used to furnish information to supplement a Reason Code or to provide information related to the action. These codes explain why a service was not paid at the amount billed (codes approved by the Accredited Standards Committee X12 and maintained by the ASC X12N Code Maintenance Committee).

Approved Reason and Remark Codes
The master lists of approved Reason and Remark Codes are updated during March, July, and November. The latest master list of Remark Codes is available at http://www.wpc-edi.com/codes/Codes.asp on the Web.

Preparing for Electronic Claims Submission
To help prepare for electronic submission, providers and suppliers who are covered entities can access educational information, Provider Readiness Checklists, and news of upcoming seminars and HIPAA roundtable discussions at http://www.cms.hhs.gov/hipaa/hipaa2/ on the Web.

HIPAA ELECTRONIC CLAIMS SUBMISSION REQUIREMENTS FOR PROVIDERS AND SUPPLIERS

HIPAA does not require all providers or suppliers who are covered entities to submit claims electronically. HIPAA does require that if a provider or supplier is a covered entity and he or she conducts certain transactions electronically, they must comply with HIPAA standards.

DHHS recognizes that transactions often require the participation of two covered entities, and non-compliance by one covered entity may put the second covered entity in a difficult position. On July 24, 2003, DHHS issued guidance that stated that covered entities that make a good faith effort to comply with HIPAA transactions and code set standards may implement contingencies to maintain operations and cash flow.

On September 23, 2003, Medicare announced that it will implement a contingency plan to accept non-compliant Medicare electronic transactions after the October 16, 2003, compliance deadline. The contingency plan will ensure continued processing of claims from providers who were not able to meet the deadline and would otherwise have had their Medicare claims rejected. The contingency plan permits Medicare to continue to accept and process claims in the electronic formats now in use, giving providers additional time to complete the testing process. Medicare will regularly reassess the readiness of its trading partners to determine how long the contingency plan will remain in effect.

The Administrative Simplification Compliance Act (ASCA) includes a provision that states, **effective October 16, 2003**, Medicare may not pay claims submitted on paper, with certain exceptions. One of the major exceptions is for claims submitted by "a small provider of services or supplier". The term "small provider of services or supplier" is defined to mean:

- A provider of services with less than 25 full-time equivalent employees; and
- A physician, practitioner, facility, or supplier (other than provider of services) with less than 10 full-time equivalent employees.

The term "provider of services" is defined for Medicare by § 1861(u) of the Social Security Act

Claims Submission Information

Electronic Claims
Information regarding compliance with the latest electronic billing requirements is available at http://www.cms.hhs.gov/hipaa/hipaa2/guidance-final.pdf on the Web.

Paper Claims
Information on the latest CMS regulations regarding the limited acceptance of paper claims in lieu of electronic billing is available at http://www.cms.hhs.gov/hipaa/hipaa2/general/deadlines.asp on the Web.

Contingency Planning
Additional information regarding contingency planning guidelines is available at http://www.cms.hhs.gov/hipaa/hipaa2/general/default.asp#contingency_guide on the Web.

to include seven specific types of institutional or special purpose providers. This term generally describes hospitals, nursing facilities, and other institutional providers that are paid through Medicare fiscal intermediaries (FIs). The terms found in the phrase "physician, practitioner, facility or supplier" are used to describe entities that furnish Medicare services described in § 1861(s) of the Act, and are generally paid through Medicare carriers.

SECURITY STANDARDS

On February 20, 2003, DHHS published the Final Rule for Security Standards for electronic protected health information. The Security Final Rule specifies a series of administrative, technical, and physical security safeguards for covered entities to use to assure the confidentiality, integrity, and availability of protected health information in electronic format. The Security Final Rule adopts standards for the security of electronic protected health information to be implemented by health plans, healthcare clearinghouses, and certain healthcare providers and suppliers. The use of the security standards will improve the Medicare and Medicaid programs, other Federal health programs and private health programs, and the effectiveness and efficiency of the healthcare industry in general by establishing a level of protection for certain healthcare information.

COVERED ENTITY SECURITY REQUIREMENTS

Covered entities are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity, confidentiality, and availability of healthcare information and to protect against any reasonably anticipated threats or hazards to the security and integrity of the information.

Covered entities must:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonable anticipated threats or hazards to the security or integrity of such information.
- Define safeguards and procedures that protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
- Ensure compliance with this final rule by its workforce.

The security compliance dates are April 21, 2005, and April 21, 2006, for small health plans.

The security standards are:

- Scalable: All covered entities must be able to implement these standards. Covered entities are required to assess potential risks and vulnerabilities and to implement reasonable and appropriate security protections. Protections implemented to comply with the standards must be kept current and must be documented.
- Technology neutral: The standards must withstand changes caused by evolving technology without becoming obsolete.

The security standards protect electronic data at rest and in transit. Specific examples of security standards include:

- Administrative Safeguards
  - Security management process
  - Assigned security responsibility
  - Workforce security
  - Information access management
  - Security awareness and training
  - Security incident procedures
  - Contingency plan
  - Evaluation
  - Business associate contracts and other arrangements
- Physical Safeguards
  - Facility access controls
  - Workstation use
  - Workstation security
  - Device and media controls
- Technical Safeguards
  - Access control
  - Audit controls

- Integrity
- Person and entity authentication
- Transmission security

- Policies and Procedures and Documentation Requirements
  - Policies and procedures
  - Documentation

Some of the aforementioned specifications are required and some can be addressed on a case-by-case basis.

Final Rule for Security Standards Information
Additional information on the Security Final Rule can be found at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp on the Web.

UTILIZING UNIQUE IDENTIFIERS

HIPAA requires the adoption and use, in standard transactions, of the following unique health identifiers:

- The employer identifier;
- The provider identifier; and
- The health plan identifier.

EMPLOYER IDENTIFIER

The final regulations that adopt the employer identifier were published in May 2002. The Rule adopts the Employer Identification Number (EIN), an existing identifier already issued by the Internal Revenue Service (IRS), as the unique identifier for employers for use in standard healthcare transactions. The use of this identifier will improve the Medicare and Medicaid programs, and the effectiveness and efficiency of the healthcare industry in general, by simplifying and enabling the efficient electronic transmission of certain health information.

The compliance date for the employer identifier standard is July 30, 2004, for all covered entities. The compliance date is August 1, 2005, for small health plans.

PROVIDER IDENTIFIER AND HEALTH PLAN IDENTIFIER

The Secretary is expected to adopt the standard unique health identifier for providers in early 2004, and to propose the standard unique identifier for health plans sometime in 2004 as well.

Unique Indentification Information
The latest information on unique identifiers can be found at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/identifiers/ on the Web.

PRIVACY STANDARDS

The *Standards for Privacy of Individually Identifiable Health Information* (Privacy Final Rule) establishes, for the first time, a set of national standards for the protection of medical records and other health information. DHHS issued the Privacy Final Rule to implement HIPAA. The Privacy Final Rule standards address the use and disclosure of individuals' health information (called "protected health information") by organizations subject to the Privacy Final Rule (called "covered entities"), as well as standards for individuals' privacy rights to understand and control how their health information is used. The DHHS OCR is responsible for implementing and enforcing the HIPAA Privacy Final Rule.

HIPAA Privacy Final Rule
Further guidance on the HIPAA Privacy Final Rule can be found at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/default.asp#finalrule on the Web.

A major purpose of the Privacy Final Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered

entity may not use or disclose protected health information, except either:

- As the Privacy Final Rule permits or requires; or
- As the subject of the information (or the individual's personal representative) authorizes in writing.

A major goal of the Privacy Final Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and well being. The Privacy Final Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the healthcare marketplace is diverse, the Privacy Final Rule is designed to be flexible, comprehensive, and to cover the variety of uses and disclosures that need to be addressed.

Privacy Final Rule Implementation
Information on CMS implementation of the HIPAA Privacy Final Rule for the Original Medicare Program (fee-for-service Medicare) may be found at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/default.asp on the Web.

WHAT INFORMATION IS PROTECTED?

The Privacy Final Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Final Rule calls this information "protected health information (PHI)".

Individually identifiable health information is information, including demographic data, that relates to:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Individually identifiable health information includes many common identifiers [e.g., name, address, birth date, Social Security Number (SSN)].

De-Identified Health Information

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information:

(1) Using a formal determination by a qualified statistician; or
(2) By removing specified identifiers of the individual and of the individual's relatives, household members, and employers. This is required and considered adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

NOTICE AND OTHER INDIVIDUAL RIGHTS

Each covered entity, with certain exceptions, must provide a Privacy Practices Notice. The Privacy Final Rule requires that the notice contain certain elements. For example, the notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must also state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must also describe an individual's rights, including the right to complain to DHHS and to the covered entity if he or she believes his or her privacy rights have been violated. The notice must additionally include a point of contact for

further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices.

PRIVACY REQUIREMENTS FOR HEALTHCARE PROVIDERS AND SUPPLIERS

Every healthcare provider and supplier, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which DHHS has established standards under the HIPAA Transactions Final Rule. Using electronic technology such as e-mail does not mean a healthcare provider or supplier is a covered entity; the transmission must be in connection with a standard transaction.

The Privacy Final Rule covers a healthcare provider or supplier whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Healthcare providers include all providers of services (e.g., institutional providers such as hospitals) and providers of medical or health services (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

The Privacy Rule excludes, from protected health information, employment records that a covered entity maintains in its capacity as an employer, and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

DISCLOSURE OF PROTECTED HEALTH INFORMATION

A covered entity must disclose protected health information in only two situations:

(1) To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and

(2) To DHHS when it is undertaking a compliance investigation or review or enforcement action.

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information without an individual's authorization for the following purposes or situations:

- To the individual (unless required for access or accounting of disclosures);
- Treatment, payment, and healthcare operations;
- Opportunity to agree or object;
- Incident to an otherwise permitted use and disclosure;
- Public interest and benefit activities; and
- Limited data set for the purposes of research, public health, or healthcare operations.

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Authorization Uses and Disclosures

Except as otherwise permitted or required, a covered entity may not disclose protected health information without a valid authorization. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or laboratory test, or disclosures to a pharmaceutical firm for its own marketing purposes.

All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Final Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.

Disclosure of Psychotherapy Notes

A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

- The covered entity who originated the notes may use them for treatment; or
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual; for DHHS to investigate or determine the covered entity's compliance with the Privacy Final Rule; to avert a serious and imminent threat to public health or safety; to a health oversight agency for lawful oversight of the originator of the psychotherapy notes; or for the lawful activities of a coroner or medical examiner or as required by law.

Disclosure of Health Information for Marketing Purposes

Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. The Privacy Rule carves out the following health-related disclosure activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;
- Communications about participating providers or suppliers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;
- Communications for treatment of the individual; and
- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, healthcare providers or suppliers, or care settings to the individual.

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services.

A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. However, no authorization is needed to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact.

Limiting Use and Disclosure to the Minimum Necessary

A central aspect of the Privacy Final Rule is the principle of minimum necessary use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical

record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances:

- Disclosure to, or a request by, a healthcare provider or suppliers for treatment;
- Disclosure to an individual who is the subject of the information, or the individual's personal representative;
- Use or disclosure made pursuant to an authorization;
- Disclosure to DHHS for complaint investigation, compliance review, or enforcement;
- Use or disclosure that is required by law; or
- Use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Restricting Access and Use

For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of its workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

Limiting Disclosure Information

Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures*, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

Reasonable Reliance Standard

If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from:

- A public official;
- A professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or
- A researcher who provides the documentation or representation required by the Privacy Final Rule for research.

Privacy Practices Notice and Other Individual Rights

Each covered entity, with certain exceptions, must provide a Privacy Practices Notice. The Privacy Final Rule requires that the notice contain certain elements to include:

- A description of the ways in which the covered entity may use and disclose protected health information;
- A description of the covered entity's duties to protect privacy, to provide the notice of privacy practices, and to abide by the terms of the current notice;
- A description of the individual's rights, including the right to submit complaints to DHHS and to the covered entity if he or she believes his or her privacy rights have been violated;
- A point of contact for further information and for making complaints to the covered entity (covered entities must act in accordance with their notices); and

- Specific distribution requirements for direct treatment providers, all other healthcare providers and suppliers, and health plans.

Privacy Practice Notice Distribution

As of April 14, 2003, any covered healthcare provider having a *direct treatment relationship* with individuals must provide a Privacy Practices Notice to patients as follows:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);
- By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and
- In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers, indirect treatment providers* (such as laboratories), or *health plans* must supply notice to anyone on request. A covered entity must also make its notice electronically available on any website it maintains for customer service or benefits information.

Acknowledgement of Notice Receipt

A covered healthcare provider with a *direct treatment relationship* with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the Privacy Practices Notice. The Privacy Final Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Individual Access to Health Information

Except in certain circumstances, individuals have the right to review and obtain a copy of his or her protected health information in a covered entity's designated record set. The designated record set is that group of records maintained by or for a covered entity. This record set is used, in whole or part, to make decisions about individuals. It may also serve as a provider's or supplier's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

The Privacy Final Rule makes exceptions from the right of access for the following protected health information:

- Psychotherapy notes;
- Information compiled for legal proceedings;
- Laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access; or
- Information held by certain research laboratories.

For information included within the right of access, covered entities may deny access to an individual in certain specified situations, such as when a healthcare professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed healthcare professional for a second opinion. Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Accounting of Health Information Disclosure

Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before the Privacy Final Rule compliance date.

The Privacy Final Rule does not require accounting for disclosures:

- For treatment, payment, or healthcare operations;
- To the individual or the individual's personal representative;
- For notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories;
- Pursuant to an authorization;
- Of a limited data set;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or
- Incident to otherwise permitted or required uses or disclosures.

Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on its written representation that an accounting would likely impede its activities.

Restriction Request

Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or healthcare operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Amendment of Protected Health Information

The Privacy Final Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, the covered entity must make reasonable efforts to provide the amendment to persons identified as needing the amendment, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Privacy Final Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

Confidential Communications Requirements

Health plans and covered healthcare providers and suppliers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs. For example, an individual may request that the provider or supplier communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider or supplier send communications in a closed envelope rather than a postcard.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

ADMINISTRATIVE REQUIREMENTS FOR IMPLEMENTING HIPAA STANDARDS

In implementing HIPAA standards, a covered entity must fulfill many requirements in its organization and policies. These requirements

are set in place to ensure that HIPAA standards are maintained while the information remains protected.

Privacy Policies and Procedures

A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Final Rule.

Privacy Policy Compliance Information
For additional information on complying with privacy policies and procedures, contact the OCR Privacy Hotline at 1-866-627-7748.

Privacy Personnel

A covered entity must designate a privacy officer responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

Workforce Training and Management

Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity). A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Final Rule.

Mitigation

A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce, or its business associates, in violation of its privacy policies and procedures or the Privacy Final Rule.

Data Safeguards

A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Final Rule, and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes.

Complaints

A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Final Rule. The covered entity must explain those procedures in its privacy practices notice.

Among other things, the covered entity must identify to whom individuals can submit complaints and advise that complaints also can be submitted to the Secretary of DHHS.

Retaliation and Waiver

A covered entity may not retaliate against a person for exercising rights provided by the Privacy Final Rule, for assisting in an investigation by DHHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Final Rule. A covered entity may not require an individual to waive any right under the Privacy Final Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

Documentation and Record Retention

A covered entity must maintain, until six years after the later of the date of its creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Final Rule requires to be documented.

OTHER PROVISIONS

The Privacy Final Rule also addresses covered entities who fall under contain circumstances that require then to have a legal representative who can act on their behalf.

Personal Representatives

The Privacy Final Rule requires a covered entity to treat a “personal representative” the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Privacy Final Rule. A personal representative is a person legally authorized to make healthcare decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Final Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

Special Case: Minors

In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Final Rule defers to state and other law to determine the rights of parents to access and control the protected health information of their minor children. If state and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed healthcare professional in the exercise of professional judgment.

HOW DOES HIPAA ENFORCE STANDARDS?

CMS has been designated by the Secretary of DHHS to enforce all of the HIPAA administrative simplifications provisions, with the exception of the privacy standards. This includes transaction and code set standards, and the security standards and identifier standards when they go into effect. The DHHS OCR is responsible for enforcement of the privacy provisions.

CMS will focus on obtaining voluntary compliance and use a complaint-driven approach for enforcement of HIPAA's electronic transactions and code sets provisions. When CMS receives a complaint about a covered entity, it will notify the entity in writing that a complaint has been filed. Following notification from CMS, the entity will have the opportunity to:

(1) Demonstrate compliance;
(2) Document its good faith efforts to comply with the standards; and/or
(3) Submit a corrective action plan.

Demonstrating Compliance - Covered entities will be given an opportunity to demonstrate to CMS that they submitted compliant transactions.

Good Faith Policy - CMS's approach will utilize the flexibility granted in section 1176(b) of the Social Security Act to consider good faith efforts to comply when assessing individual complaints. Under section 1176(b), DHHS may not impose a civil money penalty where the failure to comply is based on reasonable cause, is not due to willful neglect, and the failure to comply is cured with a 30-day period. DHHS has the authority under the statute to extend the period within which a covered entity may cure the noncompliance

"based on the nature and extent of the failure to comply."

CMS recognizes that transactions often require the participation of two covered entities and that noncompliance by one covered entity may put the second covered entity in a difficult position. Therefore, during the period immediately following the compliance date, CMS intends to

look at both covered entities' good faith efforts to come into compliance with the standards in determining, on a case-by-case basis, whether reasonable cause for the noncompliance exists and, if so, the extent to which the time for curing the noncompliance should be extended.

CMS will not impose penalties on covered entities that deploy contingencies (in order to ensure the smooth flow of payments) if they have made reasonable and diligent efforts to become compliant and, in the case of health plans, to facilitate the compliance of their trading partners. Specifically, as long as a health plan can demonstrate to CMS its active outreach/testing efforts, it can continue processing payments to providers and suppliers. In determining whether a good faith effort has been made, CMS will place a strong emphasis on sustained actions and demonstrable progress.

Indications of good faith might include, for example, such factors as:

- Increased external testing with trading partners.
- Lack of availability of, or refusal by, the trading partner(s) prior to October 16, 2003, to test the transaction(s) with the covered entity whose compliance is at issue.
- In the case of a health plan, concerted efforts in advance of the October 16, 2003, and continued efforts afterwards to conduct outreach and make testing opportunities available to its provider/supplier community.

While there are many examples of complaints that CMS may receive, the following example illustrates how CMS expects the process to work.

Example: A complaint is filed against an otherwise compliant health plan that accepts and processes both compliant and non-compliant transactions while working to help its providers and suppliers achieve compliance.

In this situation, CMS would:

(1) Notify the plan of the complaint;
(2) Based on the plan's response to the notification, evaluate the plan's efforts to help its noncompliant providers and suppliers come into compliance; and
(3) If it is determined that the plan had demonstrated good faith and reasonable cause for its non-compliance, not impose a penalty for the period of time CMS determines is appropriate, based on the nature and extent of the failure to comply.

For example, CMS would examine whether the health plan undertook a course of outreach actions to its trading partners on awareness and testing, with particular focus on the actions that occurred prior to October 16, 2003. Similarly, healthcare providers and suppliers should be able to demonstrate that they took actions to become compliant prior to October 16, 2003. If CMS determines that reasonable and diligent efforts have been made, the cure period for noncompliance would be extended at the discretion of the Government. Furthermore, CMS will continue to monitor the covered entity to ensure that its sustained efforts bring progress towards compliance. If continued progress is not made, CMS will step up its enforcement efforts towards that covered entity.

Organizations that have exercised good faith efforts to correct problems and implement the changes required to comply with HIPAA should be prepared to document them in the event of a complaint being filed. This flexibility will permit health plans to mitigate unintended adverse effects on covered entities' cash flow and business operations during the transition to the

HIPAA Standards Enforcement Information
Additional information on CMS' enforcement of HIPAA standards is available at http://www.cms.hhs.gov/hipaa/hipaa2/general/default.asp on the Web.

standards, as well as on the availability and quality of patient care.

Corrective Action Plan (CAP) - After October 16, 2003, in addition to possible fines and penalties imposed, CMS will expect non-compliant covered entities to submit plans to achieve compliance in a manner and time acceptable to the Secretary.