CMS Privacy Rule Guidance Summary Overview
December 2002
The Privacy Rule Standards Addressed in December 2002 Guidance Released

General Overview
The Privacy Rule establishes, for the first time, a foundation of Federal protections for the privacy of protected health information. The Rule does not replace Federal, State, or other law that grants individuals even greater privacy protections, and covered entities are free to retain or adopt more protective policies or practices.

Incidental Disclosure
The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure.

See 45 CFR 164.502(a)(l)(iii). An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy.

Uses and Disclosures for Treatment, Payment, and Health Care Operations (45 CFR 164.506)
Rule generally prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities. Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

A covered entity may, without the individual's authorization:
Use or disclose protected health information for its own treatment, payment, and health care operations activities.

For example:
A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.
A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
A health plan may use protected health information to provide customer service to its enrollees.

A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule).

For example:
A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred.

A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information.

For example:
A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.
A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment services.

A covered entity may disclose protected health information to another covered entity for certain health care operation activities of the entity that receives the information if:

Each entity either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship; and
The disclosure is for a quality-related health care operations activity (i.e., the activities listed in paragraphs (1) and (2) of the definition of "health care operations" at 45 CFR 164.501) or for the purpose of health care fraud and abuse detection or compliance.

For example:
A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.

A covered entity that participates in an organized health care arrangement (OHCA) may disclose protected health information about an individual to another covered entity that participates in the OHCA for any joint health care operations of the OHCA.

For example:
The physicians with staff privileges at a hospital may participate in the hospital's training of medical students.

Minimum Necessary (45 CFR 164.502(b), 164.514(d))
The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Personal Representatives (45 CFR 164.502(g))

Business Associates (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e))
The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or

creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

Examples of Business Associates.
• A third party administrator that assists a health plan with claims processing.
• A CPA firm whose accounting services to a health care provider involve access to protected health information.
• An attorney whose legal services to a health plan involve access to protected health information.
• A consultant that performs utilization reviews for a hospital.
• A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
• An independent medical transcriptionist that provides transcription services to a physician.
• A pharmacy benefits manager that manages a health plan's pharmacist network

Marketing (45 CFR 164.501, 164.508(a))
The Privacy Rule addresses the use and disclosure of protected health information for marketing purposes by:
• Defining what is "marketing" under the Rule;
• Excepting from that definition certain treatment or health care operations activities;
• Requiring individual authorization for all uses or disclosures of protected health information for marketing purposes with limited exceptions.

Privacy Rule defines "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Generally, if the communication is "marketing," then the communication can occur only if the covered entity first obtains an individual's "authorization."

Public Health (45 CFR 164.512(b))
Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.

Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

Research (45 CFR 164.501, 164.508, 164.512(i), 164.514(e), 164.528, 164.532)
Researchers may obtain, create, use, and/ or disclose individually identifiable health information under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule.

Workers' Compensation Laws (45 CFR 164.512(/))
Rule does not apply to entities that are either workers' compensation insurers, workers' compensation administrative agencies, or employers, except to the extent they may otherwise be covered entities. However, these entities need access to the health information of individuals who are injured on the job or who have a work-related illness to process or adjudicate claims, or to coordinate care under workers' compensation systems.

Notice (45 CFR 164.520)
Privacy Rule gives individuals a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information.

Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's 0bligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices.

Provide the notice to the individual no later than the date of first service delivery (after the April 14, 2003 compliance date of the Privacy Rule) and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.

When first service delivery to an individual is provided over the Internet, through e-mail, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the individual's first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.

Make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the provider's office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.

Content of the Notice. Covered entities are required to provide a notice in plain language that describes:
• How the covered entity may use and disclose protected health information about an individual.
• The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.
• The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.
• Whom individuals can contact for further information about the covered entity's privacy policies.

Government Access (45 CFR Part 160, Subpart C, 164.512(f))
Government-operated health plans and health care providers 1nust meet substantially the sa1ne require1nents as private ones for protecting the privacy of individual identifiable health information. The only new authority for government involves enforcement of the protections in the Privacy Rule itself. To ensure that covered entities protect patients' privacy as required, the Rule requires that health plans, hospitals, and other covered entities cooperate with efforts by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to investigate complaints or otherwise ensure compliance.