

SUMMARY OF THE HIPAA PRIVACY RULE

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

Introduction	3
Who is Covered by the Privacy Rule	4
What Information is Protected	5
General Principle for Uses and Disclosures	6
Permitted Uses and Disclosures	7
Authorized Uses and Disclosures	12
Limiting Uses and Disclosures to the Minimum Necessary	14
Notice and Other Individual Rights	16
Administrative Requirements	19
Other Provisions: Personal Representatives and Minors	21
Enforcement and Penalties for Noncompliance	22
Compliance Dates	22

SUMMARY OF THE HIPAA PRIVACY RULE

Introduction

The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used.

A major goal of the Privacy 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 health care and to protect the public’s health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule but is not intended to be a complete explanation of all areas of the HIPAA Rules which apply to any company or individual. The document cannot be relied upon for completeness or accuracy in the event of any dispute over compliance with the Rules.

Who is Covered by the Privacy Rule

The Privacy Rule applies to “covered entities”, which are health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form.

Health Plans.

Plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (“HMOs”), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government funded programs are not health plans:

- (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and
- (2) those programs whose principal activity is directly providing health care, such as a community health center, or the making of grants to fund the direct provision of health care.

Health Care Clearinghouses.

These are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse’s uses and disclosures of protected health information.⁸ Health care clearinghouses include billing services, re-pricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

Health Care Providers.

Every health care provider, 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 HHS has established standards under the HIPAA Transactions Rule. Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care 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.

What Information is Protected

Protected Health Information.

The Privacy 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 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).

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; either:

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

General Principle for Uses and Disclosures

Basic Principle.

A major purpose of the Privacy 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:

- (1) as the Privacy Rule permits or requires; or
- (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Required Disclosures

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

- (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
- (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

Permitted Uses and Disclosures

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:

- (1) To the Individual (unless required for access or accounting of disclosures);**
- (2) Treatment, Payment, and Health Care Operations;**
- (3)) Uses and Disclosures with Opportunity to Agree or Object;**
- (4) Incident to an otherwise permitted use and disclosure;**
- (5) Public Interest and Benefit Activities; and**
- (6) Limited Data Set for the purposes of research, public health or health care operations.**

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

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations are any of the following activities:

- (a) quality assessment and improvement activities, including case management and care coordination;
- (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation;
- (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs;

- (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk;
- (e) business planning, development, management, and administration;
- and
- (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below. Obtaining “consent” (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities. The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility.²⁵ The provider may then disclose the individual’s condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

For Notification and Other Purposes. A covered entity also may rely on an individual’s informal permission to disclose to the individual’s family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person’s involvement in the individual’s care or payment for care.²⁶ This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual’s informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual’s care of the individual’s location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as “incident to,” an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the “minimum necessary,” as required by the Privacy Rule.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual’s authorization or permission, for national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by statute, regulation, or court orders).

Public Health Activities. Covered entities may disclose protected health information to:

- (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
- (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and postmarketing surveillance;
- (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and
- (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or similar state law.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.³³

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions:

- (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
 - (2) to identify or locate a suspect, fugitive, material witness, or missing person;
 - (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime;
 - (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
 - (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises;
- and
- (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either:

- (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
- (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or

(3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.³⁸ A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

(6) Limited Data Set. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Authorized Uses and Disclosures

Authorization.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. 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 lab test, or disclosures to a pharmaceutical firm for their 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.

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.
- 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 HHS to investigate or determine the covered entity's compliance with the Privacy Rules, 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, for the lawful activities of a coroner or medical examiner or as required by law.

Marketing.

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 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 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 health care providers, 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. No authorization is needed, however, 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 Uses and Disclosures to the Minimum Necessary

Minimum Necessary.

A central aspect of the Privacy 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:

- (a) disclosure to or a request by a health care provider for treatment;
- (b) disclosure to an individual who is the subject of the information, or the individual’s personal representative;
- (c) use or disclosure made pursuant to an authorization;
- (d) disclosure to HHS for complaint investigation, compliance review or enforcement;
- (e) use or disclosure that is required by law; or
- (f) use or disclosure required for compliance with certain HIPAA Rules.

Access and Uses.

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 their 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.

Disclosures and Requests for Disclosures.

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.

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) a public official,
- (b) 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
- (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.

Notice and Other Individual Rights

Privacy Practices Notice

Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must 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 describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must 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. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.

Notice Distribution.

A covered health care provider with a direct treatment relationship with individuals must deliver a privacy practices notice to patients starting April 14, 2003 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* or *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 web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.⁵³ Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

Acknowledgement of Notice Receipt.

A covered health care 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 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.

Access.

Except in certain circumstances, individuals have the right to review and obtain a copy of their 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 that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. The Rule excepts from the right of access 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 an individual access in certain specified situations, such as when a health care 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 health care professional for a second opinion. Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment.

The 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, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, 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 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.

Disclosure Accounting.

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 its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures:

- (a) for treatment, payment, or health care operations;
- (b) to the individual or the individual's personal representative;
- (c) 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;
- (d) pursuant to an authorization;
- (e) of a limited data set;
- (f) for national security or intelligence purposes;
- (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or
- (h) 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 their written representation that an accounting would likely impede their 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 health care 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.

Confidential Communications Requirements

Health plans and covered health care providers 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 communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. 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

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Privacy Policies and Procedures.

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

Privacy Personnel.

A covered entity must designate a privacy official 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 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 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 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 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 to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

Retaliation and Waiver.

A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A covered entity may not require an individual to waive any right under the Privacy 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 their 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 Rule requires to be documented.

Fully-Insured Group Health Plan Exception.

The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the

- (1) ban on retaliatory acts and waiver of individual rights, and
- (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.

Other Provisions: Personal Representatives and Minors

Personal Representatives.

The Privacy 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 Rule. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy 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 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 health care professional in the exercise of professional judgment.

Enforcement and Penalties for Noncompliance

Civil Money Penalties.

HHS may impose civil money penalties on a covered entity of \$100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed \$25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Criminal Penalties.

A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of \$50,000 and up to one-year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

Compliance Dates

Compliance Schedule.

All covered entities, except “small health plans,” must be compliant with the Privacy Rule by April 14, 2003. Small health plans, however, have until April 14, 2004 to comply.

Small Health Plans.

A health plan with annual receipts of not more than \$5 million is a small health plan.