STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

[*45 CFR Parts 160 and 164*]

Introduction

This guidance explains and answers questions about key elements of the requirements of the HIPAA *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule). The Department of Health and Human Services (HHS) published the Privacy Rule on December 28, 2000, and adopted modifications of the Rule on August 14, 2002.

The Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) provides the first comprehensive Federal protection for the privacy of health information. All segments of the health care industry have expressed support for the objective of enhanced patient privacy in the health care system. The Privacy Rule, as modified, is carefully balanced to provide strong privacy protections that do not interfere with patient access to, or the quality of, health care delivery.

The guidance that follows is meant to communicate as clearly as possible the privacy policies contained in the Privacy Rule. For a particular segment in the Privacy Rule, the guidance will provide a brief explanation of the segment and how the Rule works, followed by a link to the "Frequently Asked Questions" about that provision. You can see all of the Privacy Rule "Frequently Asked Questions" if you CLICK HERE; or you can go to http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php, then select "Privacy of Health Information/HIPAA" from the Category dropdown list and click the Search button. The guidance does not address all of the relevant provisions in the Rule, although we anticipate adding segments in the future as we develop guidance on more Privacy Rule standards. We will also be adding to the "Frequently Asked Questions" on an ongoing basis as new questions arise. HHS plans to work expeditiously to address these additional questions to facilitate understanding of the Rule and to encourage voluntary compliance with its requirements. However, for a full understanding of one's rights and responsibilities under the Rule, it is important to consult the Rule itself.

The Privacy Rule Standards Addressed

General Overview
Incidental Uses and Disclosures (45 CFR 164.502(a))
Minimum Necessary (45 CFR 164.502(b), 164.514(d))
Personal Representatives (45 CFR 164.502(g))
Business Associates (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e))
Uses and Disclosures for Treatment, Payment, and Health Care Operations (45 CFR 164.506)

Marketing (45 CFR 164.501, 164.508(a))
Public Health (45 CFR 164.512(b))
Research (45 CFR 164.501, 164.508, 164.512(i), 164.514(e), 164.528, 164.532)
Workers' Compensation Laws (45 CFR 164.512(*l*))
Notice (45 CFR 164.520)
Government Access (45 CFR Part 160, Subpart C, 164.512(f))

GENERAL OVERVIEW OF STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

[*45 CFR Part 160 and Subparts A and E of Part 164*]

The following overview provides answers to general questions regarding the *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), promulgated by the Department of Health and Human Services (HHS).

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions that required HHS to adopt national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

In response to the HIPAA mandate, HHS published a final regulation in the form of the Privacy Rule in December 2000, which became effective on April 14, 2001. This Rule set national standards for the protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions electronically. By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. Failure to timely implement these standards may, under certain circumstances, trigger the imposition of civil or criminal penalties.

Secretary Tommy Thompson called for an additional opportunity for public comment on the Privacy Rule to ensure that the Privacy Rule achieves its intended purpose without adversely affecting the quality of, or creating new barriers to, patient care. After careful consideration of these comments, in March 2002 HHS published proposed modifications to the Rule, to improve workability and avoid unintended consequences that could have impeded patient access to delivery of quality health care. Following another round of public comment, in August 2002, the Department adopted as a final Rule the modifications necessary to ensure that the Privacy Rule worked as intended.

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.

FAQs on Privacy Rule: General Topics

INCIDENTAL USES AND DISCLOSURES

[*45 CFR 164.502(a)(1)(iii)*]

Background

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally. For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

How the Rule Works

General Provision. 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)(1)(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. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. 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. Covered entities should also take into account the potential effects on patient care and may consider other issues,

such as the financial and administrative burden of implementing particular safeguards.

Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information – for instance:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets or records rooms; or
- By providing additional security, such as passwords, on computers maintaining personal information.

Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

Minimum Necessary. Covered entities also must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. The minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. For example, a physician is not required to apply the minimum necessary standard when discussing a patient's medical chart information with a specialist at another hospital. See 45 CFR 164.502(b) and 164.514(d), and the fact sheet and frequently asked questions on this web site about the minimum necessary standard, for more information.

An incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not permitted under the Privacy Rule.

For example:

- The minimum necessary standard requires that a covered entity limit who within the entity has access to protected health information, based on who needs access to

perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's conversation about a patient's condition, would be an unlawful use or disclosure under the Privacy Rule.

FAQs on Incidental Uses and Disclosures

MINIMUM NECESSARY

[*45 CFR 164.502(b), 164.514(d)*]

Background

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. 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.

How the Rule Works

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we

will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

Uses and Disclosures of, and Requests for, Protected Health Information. For uses of protected health information, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification.

For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required.

For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly.

Of course, where protected health information is disclosed to, or requested by, health care providers for treatment purposes, the minimum necessary standard does not apply.

Reasonable Reliance. In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).

- Another covered entity.

- A professional who is a workforce member or business associate of the covered entity holding the information and who states that the information requested is the minimum necessary for the stated purpose.

- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The Rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

FAQs on Minimum Necessary

PERSONAL REPRESENTATIVES

[*45 CFR 164.502(g)*]

Background

The HIPAA Privacy Rule establishes a foundation of Federally-protected rights which permit individuals to control certain uses and disclosures of their protected health information. Along with these rights, the Privacy Rule provides individuals with the ability to access and amend this information, and the right to an accounting of certain disclosures. The Department recognizes that there may be times when individuals are legally or otherwise incapable of exercising their rights, or simply choose to designate another to act on their behalf with respect to these rights. Under the Rule, a person authorized (under State or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative." Section 164.502(g) provides when, and to what extent, the personal representative must be treated as the individual for purposes of the Rule. In addition to these formal designations of a personal representative, the Rule at 45 CFR 164.510(b) addresses situations in which persons are involved in the individual's health care but are not expressly authorized to act on the individual's behalf.

How the Rule Works

General Provisions. Except as otherwise provided in 45 CFR 164.502(g), the Privacy Rule requires covered entities to treat an individual's personal representative 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.

The personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise the individual's rights. For instance, covered entities must provide the individual's personal representative with an accounting of disclosures in accordance with 45 CFR 164.528, as well as provide the personal representative access to the individual's protected health information in accordance with 45 CFR 164.524 to the extent such information is relevant to such representation. In addition to exercising the individual's rights under the Rule, a personal representative may also authorize disclosures of the individual's protected health information.

In general, the scope of the personal representative's authority to act for the individual under the Privacy Rule derives from his or her authority under applicable law to make health care decisions for the individual. Where the person has broad authority to act on the behalf of a living individual in making decisions related to health care, such as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the covered entity must treat the personal representative as the individual for

all purposes under the Rule, unless an exception applies. (See below with respect to abuse, neglect or endangerment situations, and the application of State law in the context of parents and minors). Where the authority to act for the individual is limited or specific to particular health care decisions, the personal representative is to be treated as the individual only with respect to protected health information that is relevant to the representation. For example, a person with an individual's limited health care power of attorney regarding only a specific treatment, such as use of artificial life support, is that individual's personal representative only with respect to protected health information that relates to that health care decision. The covered entity should not treat that person as the individual for other purposes, such as to sign an authorization for the disclosure of protected health information for marketing purposes. Finally, where the person has authority to act on the behalf of a deceased individual or his estate, which does not have to include the authority to make decisions related to health care, the covered entity must treat the personal representative as the individual for all purposes under the Rule. State or other law should be consulted to determine the authority of the personal representative to receive or access the individual's protected health information.

Who Must Be Recognized as the Individual's Personal Representative. The following chart displays who must be recognized as the personal representative for a category of individuals:

If the Individual Is:	The Personal Representative Is:
An Adult or An Emancipated Minor	A person with legal authority to make health care decisions on behalf of the individual *Examples*: Health care power of attorney Court appointed legal guardian General power of attorney
An Unemancipated Minor	A parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child *Exceptions*: See parents and minors discussion below.
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions)

Examples: Executor of the estate
Next of kin or other family member
Durable power of attorney

Parents and Unemancipated Minors. The Privacy Rule defers to State or other applicable laws that address the ability of a parent, guardian, or other person acting *in loco parentis* (collectively, "parent") to obtain health information about a minor child. In most cases under the Rule, the parent is the personal representative of the minor child and can exercise the minor's rights with respect to protected health information, because the parent usually has the authority to make health care decisions about his or her minor child. Regardless of whether a parent is the personal representative, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child's protected health information when and to the extent it is expressly permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child's protected health information to a parent, or providing a parent with access to, such information when and to the extent it is expressly prohibited under State or other laws (including relevant case law). Thus, State and other applicable law governs when such law explicitly requires, permits, or prohibits the disclosure of, or access to, the health information about a minor child.

The Privacy Rule specifies three circumstances in which the parent is not the "personal representative" with respect to certain health information about his or her minor child. These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under State or other laws, or standards of professional practice. In these situations, the parent does not control the minor's health care decisions, and thus under the Rule, does not control the protected health information related to that care. The three exceptional circumstances when a parent is not the minor's personal representative are:

- **When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service;**

  Example: A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent's consent.

- **When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor**;

  Example: A court may grant authority to make health care decisions for the minor

to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

- **When a parent agrees to a confidential relationship between the minor and the physician**.

  Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

Even in these exceptional circumstances, where the parent is not the "personal representative" of the minor, the Privacy Rule defers to State or other laws that require, permit, or prohibit the covered entity to disclose to a parent, or provide the parent access to, a minor child's protected health information. Further, in these situations, if State or other law is silent or unclear concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent with access to the minor's health information, if doing so is consistent with State or other applicable law, and provided the decision is made by a licensed health care professional in the exercise of professional judgment.

Abuse, Neglect, and Endangerment Situations. When a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual. For example, if a physician reasonably believes that disclosing information about an incompetent elderly individual to the individual's personal representative would endanger that individual, the Privacy Rule permits the physician to decline to make such disclosure.

FAQs on Personal Reps/Parents and Minors

BUSINESS ASSOCIATES

[*45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)*]

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. 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. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Provision. 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.

What Is a "Business Associate?" A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

- A member of the covered entity's workforce is not a business associate.
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a

business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

- *Business associate functions and activities include*: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

- *Business associate services are*: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

See the definition of "business associate" at 45 CFR 160.103.

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.

Business Associate Contracts. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the

business associate;

- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and

- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Sample business associate contract language is available on the HHS OCR Privacy of Health Information website at http://www.hhs.gov/ocr/hipaa/contractprov.html.

Transition Provisions for Existing Contracts. Covered entities (other than small health plans) that have an existing contract (or other written agreement) with a business associate prior to October 15, 2002, are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with the Privacy Rule, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under the Rule.

See 45 CFR 164.532(d) and (e).

Exceptions to the Business Associate Standard. The Privacy Rule includes the following exceptions to the business associate standard. See 45 CFR 164.502(e). In these situations, a covered entity is not required to have a business associate contract or other written agreement in place before protected health information may be disclosed to the person or entity.

- Disclosures by a covered entity to a health care provider for treatment of the individual.

  For example:

  - A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
  - A physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.
  - A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.

- Disclosures to a health plan sponsor, such as an employer, by a group health plan, or by the health insurance issuer or HMO that provides the health insurance benefits or coverage for the group health plan, provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 CFR 164.504(f) have been met.

- The collection and sharing of protected health information by a health plan that is a public benefits program, such as Medicare, and an agency other than the agency administering the health plan, such as the Social Security Administration, that collects protected health information to determine eligibility or enrollment, or determines eligibility or enrollment, for the government program, where the joint activities are authorized by law.

<u>Other Situations in Which a Business Associate Contract Is NOT Required.</u>

- When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.

- With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

- With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents.

- Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.

- Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.

- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.

- To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.

- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.

FAQs on Business Associates

USES AND DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

[*45 CFR 164.506*]

Background

The HIPAA Privacy Rule establishes a foundation of Federal protection for personal health information, carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care. As such, the 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.

Ready access to treatment and efficient payment for health care, both of which require use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers and health plans, are essential to support treatment and payment. Many individuals expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's health care business. To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the 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.

How the Rule Works

What are Treatment, Payment, and Health Care Operations? The core health care activities of "Treatment," "Payment," and "Health Care Operations" are defined in the Privacy Rule at 45 CFR 164.501.

- "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

- "Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or

provide reimbursement for the provision of health care.

In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
- Utilization review activities; and
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

- "Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include:

  - Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
  - Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
  - Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
  - Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
  - Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other

Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

General Provisions at 45 CFR 164.506. 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.

Uses and Disclosures of Psychotherapy Notes. Except when psychotherapy notes are used by the originator to carry out treatment, or by the covered entity for certain other limited health care operations, uses and disclosures of psychotherapy notes for treatment, payment, and health care operations require the individual's authorization. See 45 CFR 164.508(a)(2).

Minimum Necessary. A covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. A covered entity also is required to develop role-based access

policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs. However, covered entities are not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes. See the fact sheet and frequently asked questions on this web site about the minimum necessary standard for more information.

Consent. A covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers.

A "consent" document is not a valid permission to use or disclose protected health information for a purpose that requires an "authorization" under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of protected health information.

Right to Request Privacy Protection. Individuals have the right to request restrictions on how a covered entity will use and disclose protected health information about them for treatment, payment, and health care operations. A covered entity is not required to agree to an individual's request for a restriction, but is bound by any restrictions to which it agrees. See 45 CFR 164.522(a).

Individuals also may request to receive confidential communications from the covered entity, either at alternative locations or by alternative means. For example, an individual may request that her health care provider call her at her office, rather than her home. A *health care provider* must accommodate an individual's reasonable request for such confidential communications. A *health plan* must accommodate an individual's reasonable request for confidential communications, if the individual clearly states that not doing so could endanger him or her. See 45 CFR 164.522(b).

Notice. Any use or disclosure of protected health information for treatment, payment, or health care operations must be consistent with the covered entity's notice of privacy practices. A covered entity is required to provide the individual with adequate notice of its privacy practices, including the uses or disclosures the covered entity may make of the individual's information and the individual's rights with respect to that information. See the fact sheet and frequently asked questions on this web site about the notice standard for more information.

FAQs on Treatment/Payment/Health Care Operations

MARKETING

[*45 CFR 164.501, 164.508(a)(3)*]

Background

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. So as not to interfere with core health care functions, the Rule distinguishes marketing communications from those communications about goods and services that are essential for quality health care.

How the Rule Works

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.

What is "Marketing"? The 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." This definition of marketing has certain exceptions, as discussed below.

Examples of "marketing" communications requiring prior authorization are:

- A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for $39, when the communication is not for the purpose of providing treatment advice.
- A communication from a health insurer promoting a home and casualty insurance product offered by the same company.

What Else is "Marketing"? Marketing also means: "An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service." This part of the definition to marketing has no exceptions. The individual must authorize these marketing communications before they can occur.

Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

For example, it is "marketing" when:

- A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors.

- A drug manufacturer receives a list of patients from a covered health care provider and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patients.

What is NOT "Marketing"? The Privacy Rule carves out exceptions to the definition of marketing under the following three categories:

(1) A communication is not "marketing" if it is made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:

  - The entities participating in a health care provider network or health plan network;
  - Replacement of, or enhancements to, a health plan; and
  - Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

  This exception to the marketing definition permits communications by a covered entity about its own products or services.

  For example, under this exception, it is not "marketing" when:

- A hospital uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or magnetic resonance image machine) through a general mailing or publication.
- A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.

(2) A communication is not "marketing" if it is made for treatment of the individual.

For example, under this exception, it is not "marketing" when:

- A pharmacy or other health care provider mails prescription refill reminders to patients, or contracts with a mail house to do so.
- A primary care physician refers an individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.

(3) A communication is not "marketing" if it is made for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

For example, under this exception, it is not "marketing" when:

- An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.
- A hospital social worker shares medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home.

For any of the three exceptions to the definition of marketing, the activity must otherwise be permissible under the Privacy Rule, and a covered entity may use a business associate to make the communication. As with any disclosure to a business associate, the covered entity must obtain the business associate's agreement to use the protected health information only for the communication activities of the covered entity.

Marketing Authorizations and When Authorizations are NOT Necessary. Except as discussed below, any communication that meets the definition of marketing is not permitted, unless the covered entity obtains an individual's authorization. To determine what constitutes an acceptable "authorization,"

see 45 CFR 164.508. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. See 45 CFR 164.508(a)(3).

A communication does not require an authorization, even if it is marketing, if it is in the form of a face-to-face communication made by a covered entity to an individual; or a promotional gift of nominal value provided by the covered entity.

For example, no prior authorization is necessary when:

- A hospital provides a free package of formula and other baby products to new mothers as they leave the maternity ward.

- An insurance agent sells a health insurance policy in person to a customer and proceeds to also market a casualty and life insurance policy as well.

FAQs on Marketing Uses and Disclosures

DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES

[*45 CFR 164.512(b)*]

Background

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose protected health information without authorization for specified public health purposes.

How the Rule Works

General Public Health Activities. The Privacy 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. See 45 CFR 164.512(b)(1)(i). Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority. See 45 CFR 164.512(b)(1)(i). Covered entities who are also a public health authority may use, as well as disclose, protected health information for these public health purposes. See 45 CFR 164.512(b)(2).

A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. 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).

Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. See 45 CFR 164.502(b). For disclosures to a public health authority,

covered entities may reasonably rely on a minimum necessary determination made by the public health authority in requesting the protected health information. See 45 CFR 164.514(d)(3)(iii)(A). For routine and recurring public health disclosures, covered entities may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of protected health information that may be disclosed for such purposes. See 45 CFR 164.514(d)(3)(i).

Other Public Health Activities. The Privacy Rule recognizes the important role that persons or entities other than public health authorities play in certain essential public health activities. Accordingly, the Rule permits covered entities to disclose protected health information, without authorization, to such persons or entities for the public health activities discussed below.

- Child abuse or neglect. Covered entities may disclose protected health information to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive such reports. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization. Likewise, a covered entity could report such cases to the police department when the police department is authorized by law to receive such reports. See 45 CFR 164.512(b)(1)(ii). See also 45 CFR 512(c) for information regarding disclosures about adult victims of abuse, neglect, or domestic violence.

- Quality, safety or effectiveness of a product or activity regulated by the FDA. Covered entities may disclose protected health information to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples of purposes or activities for which such disclosures may be made include, but are not limited to:

  - Collecting or reporting adverse events (including similar reports regarding food and dietary supplements), product defects or problems (including problems regarding use or labeling), or biological product deviations;
  - Tracking FDA-regulated products;
  - Enabling product recalls, repairs, replacement or lookback (which includes locating and notifying individuals who received recalled or withdrawn products or products that are the subject of lookback); and
  - Conducting post-marketing surveillance.

See 45 CFR 164.512(b)(1)(iii). The "person" subject to the jurisdiction of the FDA does not have to be a specific individual. Rather, it can be an individual or an entity, such as a partnership, corporation, or association. Covered entities may identify the party or parties responsible for an FDA-regulated product from the product label, from written material that accompanies the product (know as labeling), or from sources of labeling, such as the Physician's Desk Reference.

- Persons at risk of contracting or spreading a disease. A covered entity may disclose protected health information to a person who is at risk of contracting or spreading a disease or condition if other law authorizes the covered entity to notify such individuals as necessary to carry out public health interventions or investigations. For example, a covered health care provider may disclose protected health information as needed to notify a person that (s)he has been exposed to a communicable disease if the covered entity is legally authorized to do so to prevent or control the spread of the disease. See 45 CFR 164.512(b)(1)(iv).

- Workplace medical surveillance. A covered health care provider who provides a health care service to an individual at the request of the individual's employer, or provides the service in the capacity of a member of the employer's workforce, may disclose the individual's protected health information to the employer for the purposes of workplace medical surveillance or the evaluation of work-related illness and injuries to the extent the employer needs that information to comply with OSHA, the Mine Safety and Health Administration (MSHA), or the requirements of State laws having a similar purpose. The information disclosed must be limited to the provider's findings regarding such medical surveillance or work-related illness or injury. The covered health care provider must provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the worksite if that is where the service is provided). See 45 CFR 164.512(b)(1)(v).

FAQs on Public Health Uses and Disclosures

RESEARCH

[*45 CFR 164.501, 164.508, 164.512(i)*]
[See also *45 CFR 164.514(e), 164.528, 164.532*]

Background

The HIPAA Privacy Rule establishes the conditions under which protected health information may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See 45 CFR 164.501. A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with 45 CFR 164.502(d), and 164.514(a)-(c) of the Rule) without regard to the provisions below.

The Privacy Rule also defines the means by which individuals will be informed of uses and disclosures of their medical information for research purposes, and their rights to access information about them held by covered entities. Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research. Currently, most research involving human subjects operates under the Common Rule (45 CFR Part 46, Subpart A) and/or the Food and Drug Administration's (FDA) human subject protection regulations (21 CFR Parts 50 and 56), which have some provisions that are similar to, but separate from, the Privacy Rule's provisions for research. These human subject protection regulations, which apply to most Federally-funded and to some privately funded research, include protections to help ensure the privacy of subjects and the confidentiality of information. The Privacy Rule builds upon these existing Federal protections. More importantly, the Privacy Rule creates equal standards of privacy protection for research governed by the existing Federal human subject regulations and research that is not.

How the Rule Works

In the course of conducting research, 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.

Research Use/Disclosure Without Authorization. To use or disclose protected health information without authorization by the research participant, a covered entity must obtain one of the following:

- Documented Institutional Review Board (IRB) or Privacy Board Approval. Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an IRB or a Privacy Board. See 45 CFR 164.512(i)(1)(i). This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required.

  A covered entity may use or disclose protected health information for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board, provided it has obtained documentation of *all* of the following:

  - Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
  - A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
  - A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
  - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
  - The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

  The following three criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule:

  - The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    - an adequate plan to protect the identifiers from improper use and disclosure;
    - an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as

required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

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

- Preparatory to Research. Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, *and* representation that protected health information for which access is sought is necessary for the research purpose. See 45 CFR 164.512(i)(1)(ii). This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.

- Research on Protected Health Information of Decedents. Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being 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 being sought. See 45 CFR 164.512(i)(1)(iii).

- Limited Data Sets with a Data Use Agreement. A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the resercher for research, public health, or health care operations. See 45 CFR 164.514(e). A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual. The data use agreement must:

  - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
  - Limit who can use or receive the data; and
  - Require the recipient to agree to the following:
    - **S** Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;

- **S** Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;
- **S** Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
- **S** Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
- **S** Not to identify the information or contact the individual.

Research Use/Disclosure With Individual Authorization. The Privacy Rule also permits covered entities to use or disclose protected health information for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be sought for most clinical trials and some records research. In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of protected health information.

To use or disclose protected health information with authorization by the research participant, the covered entity must obtain an authorization that satisfies the requirements of 45 CFR 164.508. The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:

- Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the "end of the research study;" and

- An authorization for the use or disclosure of protected health information for research may be combined with a consent to participate in the research, or with any other legal permission related to the research study.

Accounting for Research Disclosures. In general, the Privacy Rule gives individuals the right to receive an accounting of certain disclosures of protected health information made by a covered entity. See 45 CFR 164.528. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same

person or entity for a single purpose. See 45 CFR 164.528(b)(3). Among the types of disclosures that are exempt from this accounting requirement are:

- Research disclosures made pursuant to an individual's authorization;

- Disclosures of the limited data set to researchers with a data use agreement under 45 CFR 164.514(e).

In addition, for disclosures of protected health information for research purposes without the individual's authorization pursuant to 45 CFR164.512(i), and that involve at least 50 records, the Privacy Rule allows for a simplified accounting of such disclosures by covered entities. Under this simplified accounting provision, covered entities may provide individuals with a list of all protocols for which the patient's protected health information may have been disclosed under 45 CFR 164.512(i), as well as the researcher's name and contact information. Other requirements related to this simplified accounting provision are found in 45 CFR 164.528(b)(4).

Transition Provisions. Under the Privacy Rule, a covered entity may use and disclose protected health information that was created or received for research, either before or after the compliance date, if the covered entity obtained any one of the following prior to the compliance date:

- An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

- The informed consent of the individual to participate in the research; or

- A waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA's human subject protection regulations at 21 CFR 50.24.

However, if a waiver of informed consent was obtained prior to the compliance date, but informed consent is subsequently sought after the compliance date, the covered entity must obtain the individual's authorization as required at 45 CFR 164.508. For example, if there was a temporary waiver of informed consent for emergency research under the FDA's human subject protection regulations, and informed consent was later sought after the compliance date, individual authorization would be required before the covered entity could use or disclose protected health information for the research after the waiver of informed consent was no longer valid.

The Privacy Rule allows covered entities to rely on such express legal permission, informed consent, or IRB-approved waiver of informed consent, which they create or receive before the

applicable compliance date, to use and disclose protected health information for specific research studies, as well as for future unspecified research that may be included in such permission.

FAQs on Research Uses and Disclosures

DISCLOSURES FOR WORKERS' COMPENSATION PURPOSES

[*45 CFR 164.512(l)*]

Background

The HIPAA Privacy 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. Generally, this health information is obtained from health care providers who treat these individuals and who may be covered by the Privacy Rule. The Privacy Rule recognizes the legitimate need of insurers and other entities involved in the workers' compensation systems to have access to individuals' health information as authorized by State or other law. Due to the significant variability among such laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes in a number of different ways.

How the Rule Works

Disclosures Without Individual Authorization. The Privacy Rule permits covered entities to disclose protected health information to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the individual's authorization:

- As authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. This includes programs established by the Black Lung Benefits Act, the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act. See 45 CFR 164.512(*l*).

- To the extent the disclosure is required by State or other law. The disclosure must comply with and be limited to what the law requires. See 45 CFR 164.512(a).

- For purposes of obtaining payment for any health care provided to the injured or ill worker. See 45 CFR 164.502(a)(1)(ii) and the definition of "payment" at 45 CFR 164.501.

Disclosures With Individual Authorization. In addition, covered entities may disclose protected

health information to workers' compensation insurers and others involved in workers' compensation systems where the individual has provided his or her authorization for the release of the information to the entity. The authorization must contain the elements and otherwise meet the requirements specified at 45 CFR 164.508.

Minimum Necessary. Covered entities are required reasonably to limit the amount of protected health information disclosed under 45 CFR 164.512(l) to the minimum necessary to accomplish the workers' compensation purpose. Under this requirement, protected health information may be shared for such purposes to the full extent authorized by State or other law.

In addition, covered entities are required reasonably to limit the amount of protected health information disclosed for payment purposes to the minimum necessary. Covered entities are permitted to disclose the amount and types of protected health information that are necessary to obtain payment for health care provided to an injured or ill worker.

Where a covered entity routinely makes disclosures for workers' compensation purposes under 45 CFR 164.512(*l*) or for payment purposes, the covered entity may develop standard protocols as part of its minimum necessary policies and procedures that address the type and amount of protected health information to be disclosed for such purposes.

Where protected health information is requested by a State workers' compensation or other public official, covered entities are permitted to reasonably rely on the official's representations that the information requested is the minimum necessary for the intended purpose. See 45 CFR 164.514(d)(3)(iii)(A).

Covered entities are not required to make a minimum necessary determination when disclosing protected health information as required by State or other law, or pursuant to the individual's authorization. See 45 CFR 164.502(b).

The Department will actively monitor the effects of the Privacy Rule, and in particular, the minimum necessary standard, on the workers' compensation systems and consider proposing modifications, where appropriate, to ensure that the Rule does not have any unintended negative effects that disturb these systems.

Refer to the fact sheet and frequently asked questions on this web site about the minimum necessary standard, or to 45 CFR 164.502(b) and 164.514(d), for more information.

FAQs on Workers' Compensation Disclosures

NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

[*45 CFR 164.520*]

Background

The HIPAA 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. Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of these rights and practices. The notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health plans and health care providers and exercise their rights.

How the Rule Works

General Rule. The Privacy 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 obligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices.

The Privacy Rule does not require the following covered entities to develop a notice:

- Health care clearinghouses, if the only protected health information they create or receive is as a business associate of another covered entity. See 45 CFR 164.500(b)(1).
- A correctional institution that is a covered entity (e.g., that has a covered health care provider component).
- A group health plan that provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs, and that does not create or receive protected health information other than summary health information or enrollment or disenrollment information.

See 45 CFR 164.520(a).

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.

The notice must include an effective date. See 45 CFR 164.520(b) for the specific requirements for developing the content of the notice.

A covered entity is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices. See 45 CFR 164.520(b)(3), 164.520(c)(1)(i)(C) for health plans, and 164.520(c)(2)(iv) for covered health care providers with direct treatment relationships with individuals.

Providing the Notice.

- A covered entity must make its notice available to any person who asks for it.
- A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.
- *Health Plans* must also:
  - Provide the notice to individuals then covered by the plan no later than April 14, 2003 (April 14, 2004, for small health plans) and to new enrollees at the time of enrollment.
  - Provide a revised notice to individuals then covered by the plan within 60 days of a material revision.
  - Notify individuals then covered by the plan of the availability of and how to

obtain the notice at least once every three years.

- *Covered Direct Treatment Providers* must also:

  - 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.
  - In an emergency treatment situation, provide the notice as soon as it is reasonably practicable to do so after the emergency situation has ended. In these situations, providers are not required to make a good faith effort to obtain a written acknowledgment from individuals.
  - 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.

- A covered entity may e-mail the notice to an individual if the individual agrees to receive an electronic notice.

See 45 CFR 164.520(c) for the specific requirements for providing the notice.

Organizational Options.

- Any covered entity, including a hybrid entity or an affiliated covered entity, may choose to develop more than one notice, such as when an entity performs different types of covered functions (i.e., the functions that make it a health plan, a health care provider, or a health care clearinghouse) and there are variations in its privacy practices among these covered functions. Covered entities are encouraged to provide individuals with the most specific notice possible.

- Covered entities that participate in an organized health care arrangement may choose to

produce a single, joint notice if certain requirements are met. For example, the joint notice must describe the covered entities and the service delivery sites to which it applies. If any one of the participating covered entities provides the joint notice to an individual, the notice distribution requirement with respect to that individual is met for all of the covered entities. See 45 CFR 164.520(d).

FAQs on Notice of Privacy Practices

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

[*45 CFR Part 160, Subpart C; 164.512(f)*]

Background

Under the HIPAA Privacy Rule, government-operated health plans and health care providers must meet substantially the same requirements as private ones for protecting the privacy of individual identifiable health information. For instance, government-run health plans, such as Medicare and Medicaid plans, must take virtually the same steps to protect the claims and health information that they receive from beneficiaries as private insurance plans or health maintenance organizations (HMO). In addition, all Federal agencies must also meet the requirements of the Privacy Act of 1974, which restricts what information about individual citizens – including any personal health information – can be shared with other agencies and with the public.

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.

FAQs on Disclosures for Rule Enforcement

FAQs on Disclosures for Law Enforcement Purposes

FAQs on Privacy Rule: General Topics