

**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.

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

Frequently Asked Questions

- Q: My State requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection?**
- A:** No. The Privacy Rule does not prohibit a covered entity from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with State law requirements.
- Q: How does the HIPAA Privacy Rule change the laws concerning consent for treatment?**
- A:** The Privacy Rule relates to uses and disclosures of protected health information, not to whether a patient consents to the health care itself. As such, the Privacy Rule does not affect informed consent for treatment, which is addressed by State law.
- Q: Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?**
- A:** Yes. The pharmacist is using the protected health information for treatment purposes, and the HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.
- Q: Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?**
- A:** Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.
- Q: Are health care providers restricted from consulting with other providers about a patient's condition without the patient's written authorization?**
- A:** No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule's definition of "treatment" and, therefore, is permissible. In addition, a

health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider's treatment of the individual. See 45 CFR 164.506.

Q: Does the HIPAA Privacy Rule restrict pharmacists from giving advice about over-the-counter medicines to customers?

A: No. A pharmacist may provide advice to customers about over-the-counter medicines. The Privacy Rule permits a covered entity to disclose protected health information about an individual to the individual. See 45 CFR 164.502(a)(1)(i).

Q: Can a patient have a friend or family member pick up a prescription for her?

A: Yes. A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription. See 45 CFR 164.510(b). For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual's care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.

Q: What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule?

A: The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an "authorization" is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases,

the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

Q: May a health care provider disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS)?

A: Yes, the HIPAA Privacy Rule permits a provider to disclose protected health information to a health plan for the quality-related health care operations of the health plan, provided that the health plan has or had a relationship with the individual who is the subject of the information, and the protected health information requested pertains to the relationship. See 45 CFR 164.506(c)(4). Thus, a provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, so long as the period for which information is needed overlaps with the period for which the individual is or was enrolled in the health plan.

Q: Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient (e.g., spouses or guardians) regarding payment of a bill?

A: Yes. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a covered entity (e.g., a collection agency), to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a covered entity, or its business associate, may contact persons other than the individual as necessary to obtain payment for health care services. See 45 CFR 164.506(c) and the definition of "payment" at 45 CFR 164.501. However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of protected health information. See 45 CFR 164.502(b), 164.514(d), and 164.522.

Q: Does the HIPAA Privacy Rule prevent reporting to consumer credit reporting agencies or otherwise create any conflict with the Fair Credit Reporting Act (FCRA)?

A: No. The Privacy Rule's definition of "payment" includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following protected health information about the individual: name and address; date of birth; social security number; payment history; and account number. In addition, disclosure of the name and address of the health care provider or health plan making the report is allowed. The

covered entity may perform this payment activity directly, or may carry out this function through a third party, such as a collection agency, under a business associate arrangement.

The Privacy Rule permits uses and disclosures by the covered entity or its business associate as may be required by the Fair Credit Reporting Act (FCRA) or other law. Therefore, the Department does not believe there is a conflict between the Privacy Rule and legal duties imposed on data furnishers by FCRA.

Q: Does the HIPAA Privacy Rule prevent health plans and providers from using debt collection agencies? Does the Privacy Rule conflict with the Fair Debt Collection Practices Act?

A: The Privacy Rule permits covered entities to continue to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the “payment” definition. See the definition of “payment” at 45 CFR 164.501. Through a business associate arrangement, the covered entity may engage a debt collection agency to perform this function on its behalf. Disclosures to collection agencies are governed by other provisions of the Privacy Rule, such as the business associate and minimum necessary requirements.

The Department is not aware of any conflict between the Privacy Rule and the Fair Debt Collection Practices Act. Where a use or disclosure of protected health information is necessary for the covered entity to fulfill a legal duty, the Privacy Rule would permit such use or disclosure as required by law.

Q: Are location information services of collection agencies, which are required under the Fair Debt Collection Practices Act, permitted under the HIPAA Privacy Rule?

A: “Payment” is broadly defined as activities by health plans or health care providers to obtain premiums or obtain or provide reimbursements for the provision of health care. The activities specified are by way of example and are not intended to be an exclusive listing. Billing, claims management, collection activities and related data processing are expressly included in the definition of “payment.” See the definition of “payment” at 45 CFR 164.501. Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity. See 45 CFR 164.501. The covered entity and its business associate would also have to comply with any limitations placed on location information services by the Fair Debt Collection Practices Act.

Q: Does the HIPAA Privacy Rule permit an eye doctor to confirm a contact

prescription received by a mail-order contact company?

A: Yes. The disclosure of protected health information by an eye doctor to a distributor of contact lenses for the purpose of confirming a contact lens prescription is a treatment disclosure, and is permitted under the Privacy Rule at 45 CFR 164.506.

Q: Does a physician need a patient’s written authorization to send a copy of the patient’s medical record to a specialist or other health care provider who will treat the patient?

A: No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider for that provider’s treatment of the individual. See 45 CFR 164.506 and the definition of “treatment” at 45 CFR 164.501.

Q: Is a hospital permitted to contact another hospital or health care facility, such as a nursing home, to which a patient will be transferred for continued care, without the patient’s authorization?

A: Yes. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider for that provider’s treatment or payment purposes, as well as to another covered entity for certain health care operations of that entity. See 45 CFR 164.506 and the definitions of “treatment,” “payment,” and “health care operations” at 45 CFR 164.501.

Q: When an ambulance service delivers a patient to a hospital, is it permitted to report its treatment of the patient and the patient’s medical history to the hospital, without the patient’s authorization?

A: Yes. The HIPAA Privacy Rule permits an ambulance service or other health care provider to disclose protected health information about an individual, without the individual’s authorization, to another health care provider, such as a hospital, for that provider’s treatment of the individual. See 45 CFR 164.506 and the definition of “treatment” at 45 CFR 164.501.

Q: How does the HIPAA Privacy Rule apply to professional liability insurance? Specifically, how can professional liability insurers continue to arrange for and maintain medical liability insurance for health care providers covered by the Rule?

A: The Privacy Rule permits a covered health care provider to disclose information for

“health care operations” purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within “business management and general administrative activities” under the definition of “health care operations.” Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes. See 45 CFR 164.502(a)(1)(ii) and the definition of “health care operations” at 45 CFR 164.501.