

Standards for Privacy of Individually Identifiable Health Information

[45 CFR Parts 160 and 164]

General Overview

The following is an overview that provides answers to general questions regarding the regulation entitled, *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), promulgated by the Department of Health and Human Services (HHS), and process for modifications to that rule. Detailed guidance on specific requirements in the regulation is presented in subsequent sections, each of which addresses a different standard.

The Privacy Rule provides the first comprehensive federal protection for the privacy of health information. All segments of the health care industry have expressed their support for the objective of enhanced patient privacy in the health care system. At the same time, HHS and most parties agree that privacy protections must not interfere with a patient's access to or the quality of health care delivery.

The guidance provided in this section and those that follow is meant to communicate as clearly as possible the privacy policies contained in the rule. Each section has a short summary of a particular standard in the Privacy Rule, followed by "Frequently Asked Questions" about that provision. In some cases, the guidance identifies areas of the Privacy Rule where a modification or change to the rule is necessary. These areas are summarized below in response to the question "What changes might you make to the final rule?" and discussed in more detail in the subsequent sections of this guidance. We emphasize that this guidance document is only the first of several technical assistance materials that we will issue to provide clarification and help covered entities implement the rule. We anticipate that there will be many questions that will arise on an ongoing basis which we will need to answer in future guidance. In addition, the Department will issue proposed modifications as necessary in one or more rulemakings to ensure that patients' privacy needs are appropriately met. The Department plans to work expeditiously to address these additional questions and propose modifications as necessary.

Frequently Asked Questions

Q: What does this regulation do?

A: The Privacy Rule became effective on April 14, 2001. Most health plans and health care providers that are covered by the new rule must comply with the new requirements by April 2003.

The Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.

First Guidance on the Final Rule

- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility requires disclosure of some forms of data - for example, to protect public health.

For patients - it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

- It enables patients to find out how their information may be used and what disclosures of their information have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Q: Why is this regulation needed?

A: In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of standards for the privacy of individually identifiable health information.

When it comes to personal information that moves across hospitals, doctors' offices, insurers or third party payers, and state lines, our country has relied on a patchwork of federal and state laws. Under the current patchwork of laws, personal health information can be distributed - without either notice or consent - for reasons that have nothing to do with a patient's medical treatment or health care reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card - or to an employer who may use it in personnel decisions. The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new federal privacy standards.

Health care providers have a strong tradition of safeguarding private health information. But in today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the rule provides clear standards for all parties regarding protection of personal health information.

Q: What does this regulation require the average provider or health plan to do?

A: For the average health care provider or health plan, the Privacy Rule requires activities, such as:

First Guidance on the Final Rule

- Providing information to patients about their privacy rights and how their information can be used.
- Adopting clear privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the final Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the rules provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
- The policies and procedures of small providers may be more limited under the rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

Q. Who must comply with these new privacy standards?

A: As required by Congress in HIPAA, the Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards are required to be adopted by the Secretary under HIPAA, such as electronic billing and fund transfers. These entities (collectively called "covered entities") are bound by the new privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give HHS the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits. The "Business Associate" section of this guidance provides a more detailed discussion of the covered entities' responsibilities when they engage others to perform essential functions or services for them.

Q: When will covered entities have to meet these standards?

A: As Congress required in HIPAA, most covered entities have two full years from the date that the regulation took effect - or, until April 14, 2003 - to come into compliance with these standards. Under the law, small health plans will have three full years - or, until April 14, 2004 - to come into compliance.

The HHS Office for Civil Rights (OCR) will provide assistance to help covered entities prepare to comply with the rule. OCR maintains a Web site with information on the new regulation, including guidance for industry, such as these frequently asked questions, at <http://www.hhs.gov/ocr/hipaa/>.

Q: Do you expect to make any changes to this rule before the compliance date?

A: We can and will issue proposed modifications to correct any unintended negative effects of the Privacy Rule on health care quality or on access to such care.

In February 2001, Secretary Thompson requested public comments on the final rule to help HHS assess the rule's real-world impact in health care delivery. During the 30-day comment period, we received more than 11,000 letters or comments - including some petitions with thousands of names. These comments are helping to guide the Department's efforts to clarify areas of the rule to eliminate uncertainties and to help covered entities begin their implementation efforts.

Q: What changes might you make in the final rule?

A: We continue to review the input received during the recent public comment period to determine what changes are appropriate to ensure that the rule protects patient privacy as intended without harming consumers' access to care or the quality of that care.

Examples of standards in the Privacy Rule for which we will propose changes are:

- *Phoned-in Prescriptions* - A change will permit pharmacists to fill prescriptions phoned in by a patient's doctor before obtaining the patient's written consent (see the "Consent" section of this guidance for more discussion).
- *Referral Appointments* - A change will permit direct treatment providers receiving a first time patient referral to schedule appointments, surgery, or other procedures before obtaining the patient's signed consent (see the "Consent" section of this guidance for more discussion).
- *Allowable Communications* - A change will increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care, including routine oral communications with family members, treatment discussions with staff involved in coordination of patient care, and using patient names to locate them in waiting areas (see the "Oral Communications" section of this guidance for more discussion).

First Guidance on the Final Rule

- *Minimum Necessary Scope* - A change will increase covered entities' confidence that certain common practices, such as use of sign-up sheets and X-ray lightboards, and maintenance of patient medical charts at bedside, are not prohibited under the rule (see the "Minimum Necessary" section of this guidance for more discussion).

In addition, HHS may reevaluate the Privacy Rule to ensure that parents have appropriate access to information about the health and well-being of their children. This issue is discussed further in the "Parents and Minors" section of this guidance.

Other changes to the Privacy Rule also may be considered as appropriate.

Q: How will you make any changes?

A: Any changes to the final rule must be made in accordance with the Administrative Procedures Act (APA). HHS intends to comply with the APA by publishing its rule changes in the *Federal Register* through a Notice of Proposed Rulemaking and will invite comment from the public. After reviewing and addressing those comments, HHS will issue a final rule to implement appropriate modifications.

Congress specifically authorized HHS to make appropriate modifications in the first year after the final rule took effect in order to ensure the rule could be properly implemented in the real world. We are working as quickly as we can to identify where modifications are needed and what corrections need to be made so as to give covered entities as much time as possible to implement the rule. Covered entities can and should begin the process of implementing the privacy standards in order to meet their compliance dates.

CONSENT [45 CFR § 164.506]

Background

The Privacy Rule establishes a federal requirement that most doctors, hospitals, or other health care providers obtain a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment, or health care operations (TPO). Today, many health care providers, for professional or ethical reasons, routinely obtain a patient's consent for disclosure of information to insurance companies or for other purposes. The Privacy Rule builds on these practices by establishing a uniform standard for certain health care providers to obtain their patients' consent for uses and disclosures of health information about the patient to carry out TPO.

General Provisions

- Patient consent is required before a covered health care provider that has a direct treatment relationship with the patient may use or disclose protected health information (PHI) for purposes of TPO. Exceptions to this standard are shown in the next bullet.
- Uses and disclosures for TPO may be permitted without prior consent in an emergency, when a provider is required by law to treat the individual, or when there are substantial communication barriers.
- Health care providers that have indirect treatment relationships with patients (such as laboratories that only interact with physicians and not patients), health plans, and health care clearinghouses may use and disclose PHI for purposes of TPO without obtaining a patient's consent. The rule permits such entities to obtain consent, if they choose.
- If a patient refuses to consent to the use or disclosure of their PHI to carry out TPO, the health care provider may refuse to treat the patient.
- A patient's written consent need only be obtained by a provider one time.
- The consent document may be brief and may be written in general terms. It must be written in plain language, inform the individual that information may be used and disclosed for TPO, state the patient's rights to review the provider's privacy notice, to request restrictions and to revoke consent, and be dated and signed by the individual (or his or her representative).

Individual Rights

- An individual may revoke consent in writing, except to the extent that the covered entity has taken action in reliance on the consent.
- An individual may request restrictions on uses or disclosures of health information for TPO. The covered entity need not agree to the restriction requested, but is bound by any restriction to which it agrees.
- An individual must be given a notice of the covered entity's privacy practices and may review that notice prior to signing a consent.

Administrative Issues

- A covered entity must retain the signed consent for 6 years from the date it was last in effect. The Privacy Rule does not dictate the form in which these consents are to be retained by the covered entity.
- Certain integrated covered entities may obtain one joint consent for multiple entities.
- If a covered entity obtains consent and also receives an authorization to disclose PHI for TPO, the covered entity may disclose information only in accordance with the more restrictive document, unless the covered entity resolves the conflict with the individual.
- Transition provisions allow providers to rely on consents received prior to April 14, 2003 (the compliance date of the Privacy Rule for most covered entities), for uses and disclosures of health information obtained prior to that date.

Frequently Asked Questions

Q. Are health plans or clearinghouses required to obtain an individual's consent to use or disclose PHI to carry out TPO?

A: No. Health plans and clearinghouses may use and disclose PHI for these purposes without obtaining consent. These entities are permitted to obtain consent. If they choose to seek individual consent for these uses and disclosures, the consent must meet the standards, requirements, and implementation specifications for consents set forth under the rule.

Q: Can a pharmacist use PHI to fill a prescription that was telephoned in by a patient's physician if the patient is a new patient to the pharmacy and has not yet provided written consent to the pharmacy?

A: The Privacy Rule, as written, does not permit this activity without prior patient consent. It poses a problem for first-time users of a particular pharmacy or pharmacy chain. The Department of Health and Human Services did not intend the rule to interfere with a pharmacist's normal activities in this way. The Secretary is aware of this problem, and will propose modifications to fix it to ensure ready patient access to high quality health care.

Q: Can direct treatment providers, such as a specialist or hospital, to whom a patient is referred for the first time, use PHI to set up appointments or schedule surgery or other procedures before obtaining the patient's written consent?

A: As in the pharmacist example above, the Privacy Rule, as written, does not permit uses of PHI prior to obtaining the patient's written consent for TPO. This unintended problem potentially exists in any circumstance when a patient's first contact with a direct treatment provider is not in person. As noted above, the Secretary is aware of this problem and will propose modifications to fix it.

Q: Will the consent requirement restrict the ability of providers to consult with other providers about a patient's condition?

A: No. A provider with a direct treatment relationship with a patient would have to have initially obtained consent to use that patient's health information for treatment purposes. Consulting with another health care provider about the patient's case falls within the definition of "treatment" and, therefore, is permissible. If the provider being consulted does not otherwise have a direct treatment relationship with the patient, that provider does not need to obtain the patient's consent to engage in the consultation.

Q: Does a pharmacist have to obtain a consent under the Privacy Rule in order to provide advice about over-the-counter medicines to customers?

A: No. A pharmacist may provide advice about over-the-counter medicines without obtaining the customers' prior consent, provided that the pharmacist does not create or keep a record of any PHI. In this case, the only interaction or disclosure of information is a conversation between the pharmacist and the customer. The pharmacist may disclose PHI about the customer to the customer without obtaining his or her consent (§ 164.502(a)(1)(i)), but may not otherwise use or disclose that information.

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 § 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 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: The rule provides an exception to the prior consent requirement for "emergency treatment situations." How will a provider know when the situation is an "emergency treatment situation" and, therefore, is exempt from the Privacy Rule's prior consent requirement?

A: Health care providers must exercise their professional judgment to determine whether obtaining a consent would interfere with the timely delivery of necessary health care. If, based on professional judgment, a provider reasonably believes at the time the patient presents for treatment that a delay involved in obtaining the patient's consent to use or disclose information would compromise the patient's care, the provider may use or disclose PHI that was obtained during the emergency treatment, without prior consent, to carry out TPO. The provider must attempt to obtain consent as soon as reasonably practicable after the provision of treatment. If the provider is able to obtain the patient's consent to use or disclose information before providing care, without compromising the patient's care, we require the provider to do so.

Q: Does the exception to the consent requirement regarding substantial barriers to communication with the individual affect requirements under Title VI of the Civil Rights Act of 1964 or the Americans with Disabilities Act?

A: No. The provision of the Privacy Rule regarding substantial barriers to communication does not affect covered entities' obligations under Title VI or the Americans with Disabilities Act. Entities that are covered by these statutes must continue to meet the requirements of the statutes. The Privacy Rule works in conjunction with these laws to remove impediments to access to necessary health care for all individuals.

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

A: A consent is a general document that gives health care providers, which have a direct treatment relationship with a patient, permission to use and disclose all PHI for TPO. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment on the individual providing this consent. One consent may cover all uses and disclosures for TPO by that provider, indefinitely. A consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information. Only doctors or other health care providers with a direct treatment relationship with a patient are required to obtain consent. Generally, a "direct treatment provider" is one that treats a patient directly, rather than based on the orders of another provider, and/or provides health care services or test results directly to patients. Other health care providers, health plans, and health care clearinghouses may use or disclose information for TPO without consent, or may choose to obtain a consent.

An authorization is a more customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. Covered entities may not condition treatment or coverage on the individual providing an authorization. An authorization is more detailed and specific than a consent. It covers only the uses and disclosures and only the PHI stipulated in the authorization; it has an expiration date; and, in some cases, it also states the purpose for which the information may be used or disclosed.

An authorization is required for use and disclosure of PHI not otherwise allowed by the rule. In general, this means an authorization is required for purposes that are not part of TPO and not described in § 164.510 (uses and disclosures that require an opportunity for the individual to agree or to object) or § 164.512 (uses and disclosures for which consent, authorization, or an opportunity to agree or to object is not required). Situations in which an authorization is required for TPO purposes are identified and discussed in the next question.

All covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a patient mailing list, to disclose information to an employer for employment decisions, or to disclose information for eligibility for life insurance. A covered entity will never need to obtain both an individual's consent and authorization for a single use or disclosure.

However, a provider may have to obtain consent and authorization from the same patient for different uses or disclosures. For example, an obstetrician may, under the consent obtained from the patient, send an appointment reminder to the patient, but would need authorization from the patient to send her name and address to a company marketing a diaper service.

Q: Would a covered entity ever need an authorization rather than a consent for uses or disclosures of PHI for TPO?

A: Yes. The Privacy Rule requires providers to obtain authorization and not consent to use or disclose PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes, for payment, or for health care operations purposes, except as specified in the Privacy Rule (§ 164.508(a)(2)). In addition, because the consent is only for a use or disclosure of PHI for the TPO purposes of the covered entity obtaining the consent, an authorization is also required if the disclosure is for the TPO purposes of an entity other than the provider who obtained the consent. For example, a health plan seeking payment for a particular service from a second health plan, such as in coordination of benefits or secondary payer situations, may need PHI from a physician who rendered the health care services. In this case, the provider typically has been paid, and the transaction is between the plans. Since the provider's disclosure is for the TPO purposes of the plan, it would not be covered by the provider's consent. Rather, an authorization, and not a consent, would be the proper document for the plan to use when requesting such a disclosure.

Q: Will health care providers be required to determine whether another covered entity has a more restrictive consent form before disclosing information to that entity for TPO purposes?

A: No. Generally, a consent permits only the covered entity that obtains the consent to use or disclose PHI for its own TPO purposes. Under the Privacy Rule, one covered entity is not bound by a consent or any restrictions on that consent agreed to by another covered entity, with one exception. A covered entity would be bound by the consent of another covered entity if the entities use a "joint consent," as permitted by the Privacy Rule (§ 164.506(f)).

In addition, it is possible for several entities to choose to be treated as a single covered entity under the rule, as "affiliated entities." Because affiliated entities are considered to be one covered entity under the rule, there would be only one consent and each entity would be bound by that consent (§ 164.504(d)).

Q: What is the interaction between "consent" and "notice"?

A: The consent and the notice of privacy practices are two distinct documents. A consent document is brief (may be less than one page). It must refer to the notice and must inform the individual that he has the opportunity to review the notice prior to signing the consent. The Privacy Rule does not require that the individual read the notice or that the covered entity explain each item in the notice before the individual provides consent. We expect that some patients will

simply sign the consent while others will read the notice carefully and discuss some of the practices with the covered entity.

Q: May consent for use or disclosure of PHI be provided electronically?

A: Yes. The covered entity may choose to obtain and store consents in paper or electronic form, provided that the consent meets all of the requirements under the Privacy Rule, including that it be signed by the individual. Paper is not required.

Q: Must a covered entity verify a signature on a consent form if the individual is not present when he signs it?

A: No.

Q: May consent be obtained by a health care provider only one time if there is a single connected course of treatment involving multiple visits?

A: Yes. A health care provider needs to obtain consent from a patient for use or disclosure of PHI only one time. This is true regardless of whether there is a connected course of treatment or treatment for unrelated conditions. A provider will need to obtain a new consent from a patient only if the patient has revoked the consent between treatments.

Q: If an individual consents to the use or disclosure of PHI for TPO purposes, obtains a health care service, and then revokes consent before the provider bills for such service, is the provider precluded from billing for such service?

A: No. A health care provider that provides a health care service to an individual after obtaining consent from the individual, may bill for such service even if the individual immediately revokes consent after the service has been provided. The Privacy Rule requires that an individual be permitted to revoke consent, but provides that the revocation is not effective to the extent that the health care provider has acted in reliance on the consent. Where the provider has obtained a consent and provided a health care service pursuant to that consent with the expectation that he or she could bill for the service, the health care provider has acted in reliance on the consent. The revocation would not interfere with the billing or reimbursement for that care.

Q: If covered providers that are affiliated or part of an organized health care arrangement are located in different states with different laws regarding uses and disclosures of health information (e.g., a chain of pharmacies), do they need to obtain a consent in each state that the patient obtains treatment?

A: No. The consent is general and only needs to be obtained by a covered entity (or by affiliated entities or entities that are part of an organized health care arrangement) one time. The Privacy Rule does not require that the consent include any details about state law, and therefore, does not require different consent forms in each state. State law may impose additional requirements for consent forms on covered entities.

Q: Must a revocation of a consent be in writing?

A: Yes.

Q: The Privacy Rule permits a covered entity to continue to use or disclose health information which it has on the compliance date pursuant to express legal permission obtained from an individual prior to the compliance date. Is a form, signed by a patient prior to the compliance date of the rule, that permits a provider to use or disclose information for the limited purpose of payment sufficient to meet these transition provision requirements?

A: Yes. A provider that obtains permission from a patient prior to the compliance date to use or disclose information for payment purposes may use the PHI about that patient collected pursuant to that permission for purposes of TPO. Under the transition provisions, if prior to the compliance date, a provider obtained a consent for the use or disclosure of health information for any one of the TPO purposes, the provider may use the health information collected pursuant to that consent for all three purposes after the compliance date (§ 164.532(b)). Thus, a provider that obtained consent for use or disclosure for billing purposes would be able to draw on the data obtained prior to the compliance date and covered by the consent form for all TPO activities to the extent not expressly excluded by the terms of the consent.

Q: Are health plans and health care clearinghouses required by the Privacy Rule to have some form of express legal permission to use and disclose health information obtained prior to the compliance date for TPO purposes?

A: No. Health plans and health care clearinghouses are not required to have express legal permission from individuals to use or disclose health information obtained prior to the compliance date for their own TPO purposes.

MINIMUM NECESSARY
[45 CFR §§ 164.502(b), 164.514(d)]

General Requirement

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do 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 authorization requested by the individual.
- Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the 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. We understand this guidance will not answer all questions pertaining to the minimum necessary standard, especially as applied to specific industry practices. As more questions arise with regard to application of the minimum necessary standard to particular circumstances, we will provide more detailed guidance and clarification on this issue.

Uses and Disclosures of, and Requests for PHI

For uses of PHI, the 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 PHI 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 PHI 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, covered entities must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of PHI necessary to accomplish the

First Guidance on the Final Rule

purpose of a non-routine disclosure. Non-routine disclosures must be reviewed on an individual basis in accordance with these criteria. When making non-routine requests for PHI, the covered entity must review each request so as to ask for only that information reasonably necessary for the purpose of the request.

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 for a disclosure permitted under § 164.512 of the rule.
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information.
- 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.

Treatment Settings

We understand that medical information must be conveyed freely and quickly in treatment settings, and thus understand the heightened concern that covered entities have about how the minimum necessary standard applies in such settings. Therefore, we are taking the following steps to clarify the application of the minimum necessary standard in treatment settings. First, we clarify some of the issues here, including the application of minimum necessary to specific practices, so that covered entities may begin implementation of the Privacy Rule. Second, we will propose corresponding changes to the regulation text, to increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care. We understand that issues of this importance need to be addressed directly and clearly to eliminate any ambiguities.

Frequently Asked Questions

Q: How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

A: The Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the rule requires covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and

procedures accordingly. This is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information.

The minimum necessary standard is intended to make covered entities evaluate their practices and enhance protections as needed to prevent unnecessary or inappropriate access to PHI. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, we expect that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately will limit access to personal health information without sacrificing the quality of health care.

Q: Won't the minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

A: No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

The Privacy Rule provides the covered entity with substantial discretion as to how to implement the minimum necessary standard, and appropriately and reasonably limit access to the use of identifiable health information within the covered entity. The rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity can develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Q: Do the minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training?

A: No. The definition of "health care operations" in the rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

Q: Must minimum necessary be applied to disclosures to third parties that are authorized by an individual?

A: No, unless the authorization was requested by a covered entity for its own purposes. The Privacy Rule exempts from the minimum necessary requirements most uses or disclosures that are authorized by an individual. This includes authorizations covered entities may receive directly from third parties, such as life, disability, or casualty insurers pursuant to the patient's

application for or claim under an insurance policy. For example, if a covered health care provider receives an individual's authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of § 164.508.

However, minimum necessary does apply to authorizations requested by the covered entity for its own purposes (see § 164.508(d), (e), and (f)).

Q: Are providers required to make a minimum necessary determination to disclose to federal or state agencies, such as the Social Security Administration (SSA) or its affiliated state agencies, for individuals' applications for federal or state benefits?

A: No. These disclosures must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements. Further, use of the provider's own authorization form is not required. Providers can accept an agency's authorization form as long as it meets the requirements of § 164.508 of the rule. For example, disclosures to SSA (or its affiliated state agencies) for purposes of determining eligibility for disability benefits are currently made subject to an individual's completed SSA authorization form. After the compliance date, the current process may continue subject only to modest changes in the SSA authorization form to conform to the requirements in § 164.508.

Q: Doesn't the minimum necessary standard conflict with the Transactions standards? Does minimum necessary apply to the standard transactions?

A: No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the subchapter. This includes all data elements that are required or situationally required in the standard transactions. However, in many cases, covered entities have significant discretion as to the information included in these transactions. This standard does apply to those optional data elements.

Q: Does the rule strictly prohibit use, disclosure, or requests of an entire medical record? Does the rule prevent use, disclosure, or requests of entire medical records without case-by-case justification?

A: No. The Privacy Rule does not prohibit use, disclosure, or requests of an entire medical record. A covered entity may use, disclose, or request an entire medical record, without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. In making

First Guidance on the Final Rule

non-routine requests, the covered entity may also establish and utilize criteria to assist in determining when to request the entire medical record.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment or disclosures to the individual.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, in order to comply with the minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the rule.

Q: Do the minimum necessary requirements prohibit covered entities from maintaining patient medical charts at bedside, require that covered entities shred empty prescription vials, or require that X-ray light boards be isolated?

A: No. The minimum necessary standards do not require that covered entities take any of these specific measures. Covered entities must, in accordance with other provisions of the Privacy Rule, take reasonable precautions to prevent inadvertent or unnecessary disclosures. For example, while the Privacy Rule does not require that X-ray boards be totally isolated from all other functions, it does require covered entities to take reasonable precautions to protect X-rays from being accessible to the public. We understand that these and similar matters are of special concern to many covered entities, and we will propose modifications to the rule to increase covered entities' confidence that these practices are not prohibited.

Q: Will doctors' and physicians' offices be allowed to continue using sign-in sheets in waiting rooms?

A: We did not intend to prohibit the use of sign-in sheets, but understand that the Privacy Rule is ambiguous about this common practice. We, therefore, intend to propose modifications to the rule to clarify that this and similar practices are permissible.

Q: What happens when a covered entity believes that a request is seeking more than the minimum necessary PHI?

A: In such a situation, the Privacy Rule requires a covered entity to limit the disclosure to the minimum necessary as determined by the disclosing entity. Where the rule permits covered entities to rely on the judgment of the person requesting the information, and if such reliance is reasonable despite the covered entity's concerns, the covered entity may make the disclosure as requested.

Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with the person making the request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

ORAL COMMUNICATIONS [45 CFR §§ 160.103, 164.501]

Background

The Privacy Rule applies to individually identifiable health information in all forms, electronic, written, oral, and any other. Coverage of oral (spoken) information ensures that information retains protections when discussed or read aloud from a computer screen or a written document. If oral communications were not covered, any health information could be disclosed to any person, so long as the disclosure was spoken.

Providers and health plans understand the sensitivity of oral information. For example, many hospitals already have confidentiality policies and concrete procedures for addressing privacy, such as posting signs in elevators that remind employees to protect patient confidentiality.

We also understand that oral communications must occur freely and quickly in treatment settings, and thus understand the heightened concern that covered entities have about how the rule applies. Therefore, we are taking a two-step approach to clarifying the regulation with respect to these communications. First, we provide some clarification of these issues here, so that covered entities may begin implementing the rule by the compliance date. Second, we will propose appropriate changes to the regulation text to clarify the regulatory basis for the policies discussed below in order to minimize confusion and to increase the confidence of covered entities that they are free to engage in communications as required for quick, effective, and high quality health care. We understand that issues of this importance need to be addressed directly and clearly in the Privacy Rule and that any ambiguities need to be eliminated.

General Requirements

- Covered entities must reasonably safeguard protected health information (PHI) - including oral information - from any intentional or unintentional use or disclosure that is in violation of the rule (see § 164.530(c)(2)). They must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. "Reasonably safeguard" means that covered entities must make reasonable efforts to prevent uses and disclosures not permitted by the rule. However, we do not expect reasonable safeguards to guarantee the privacy of PHI from any and all potential risks. In determining whether a covered entity has provided reasonable safeguards, the Department will take into account all the circumstances, including the potential effects on patient care and the financial and administrative burden of any safeguards.
- Covered entities must have policies and procedures that reasonably limit access to and use of PHI to the minimum necessary given the job responsibilities of the workforce and the nature of their business (see §§ 164.502(b), 164.514(d)). The minimum necessary standard does not apply to disclosures, including oral disclosures, among providers for treatment purposes. For a more complete discussion of the minimum necessary requirements, see the fact sheet and frequently asked questions titled "Minimum Necessary."

First Guidance on the Final Rule

- Many health care providers already make it a practice to ensure reasonable safeguards for oral information - for instance, by speaking quietly when discussing a patient's condition with family members in a waiting room or other public area, and by avoiding using patients' names in public hallways and elevators. 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.

Frequently Asked Questions

Q: If health care providers engage in confidential conversations with other providers or with patients, have they violated the rule if there is a possibility that they could be overheard?

A: The Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. We also understand that overheard communications are unavoidable. For example, in a busy emergency room, it may be necessary for providers to speak loudly in order to ensure appropriate treatment. The Privacy Rule is not intended to prevent this appropriate behavior. We would consider the following practices to be permissible, if reasonable precautions are taken to minimize the chance of inadvertent disclosures to others who may be nearby (such as using lowered voices, talking apart):

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.

We will propose regulatory language to reinforce and clarify that these and similar oral communications (such as calling out patient names in a waiting room) are permissible.

Q: Does the Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

A: No, the Privacy Rule does not require these types of structural changes be made to facilities. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. "Reasonable safeguards" mean that covered entities must make reasonable efforts to prevent uses and disclosures not permitted by the rule. The Department does not consider facility restructuring to be a requirement under this standard. In

First Guidance on the Final Rule

determining what is reasonable, the Department will take into account the concerns of covered entities regarding potential effects on patient care and financial burden.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

Covered entities must provide reasonable safeguards to avoid prohibited disclosures. The rule does not require that all risk be eliminated to satisfy this standard. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
- Providers could add curtains or screens to areas where oral communications often occur between doctors and patients or among professionals treating the patient.
- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms.

In assessing what is "reasonable," covered entities may consider the viewpoint of prudent professionals.

Q: Do covered entities need to provide patients access to oral information?

A: No. The Privacy Rule requires covered entities to provide individuals with access to PHI about themselves that is contained in their "designated record sets." The term "record" in the term "designated record set" does not include oral information; rather, it connotes information that has been recorded in some manner.

The rule does not require covered entities to tape or digitally record oral communications, nor retain digitally or tape recorded information after transcription. But if such records are maintained and used to make decisions about the individual, they may meet the definition of "designated record set." For example, a health plan is not required to provide a member access to

tapes of a telephone "advice line" interaction if the tape is only maintained for customer service review and not to make decisions about the member.

Q: Do covered entities have to document all oral communications?

A: No. The Privacy Rule does not require covered entities to document any information, including oral information, that is used or disclosed for treatment, payment or health care operations (TPO).

The rule includes, however, documentation requirements for some information disclosures for other purposes. For example, some disclosures must be documented in order to meet the standard for providing a disclosure history to an individual upon request. Where a documentation requirement exists in the rule, it applies to all relevant communications, whether in oral or some other form. For example, if a covered physician discloses information about a case of tuberculosis to a public health authority as permitted by the rule in § 164.512, then he or she must maintain a record of that disclosure regardless of whether the disclosure was made orally by phone or in writing.

Q: Did the Department change its position from the proposed rule by covering oral communications in the final Privacy Rule?

A: No. The proposed rule would have covered information in any form or medium, as long as it had at some point been maintained or transmitted electronically. Once information had been electronic, it would have continued to be covered as long as it was held by a covered entity, whether in electronic, written, or oral form.

The final Privacy Rule eliminates this nexus to electronic information. All individually identifiable health information of the covered entity is covered by the rule.

BUSINESS ASSOCIATES [45 CFR §§ 160.103, 164.502(e), 164.514(e)]

Background

By law, the Privacy Rule applies only to health plans, health care clearinghouses, and certain health care providers. In today's health care system, however, most health care providers and health plans do not carry out all of their health care activities and functions by themselves; they require assistance from a variety of contractors and other businesses. In allowing providers and plans to give protected health information (PHI) to these "business associates," the Privacy Rule conditions such disclosures on the provider or plan obtaining, typically by contract, satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of certain disclosures (e.g., if the business associate maintains the only copy of information, it must promise to cooperate with the covered entity to provide individuals access to information upon request). PHI may be disclosed to a business associate *only* to help the providers and plans carry out their health care functions - not for independent use by the business associate.

What is a "business associate"

- A business associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI.
- A business associate is not a member of the health care provider, health plan, or other covered entity's workforce.
- A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.
- The rule includes exceptions. The business associate requirements do not apply to covered entities who disclose PHI to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital.

Frequently Asked Questions

Q: Has the Secretary exceeded the statutory authority by requiring "satisfactory assurances" for disclosures to business associates?

A: No. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health care providers, health plans, and health care clearinghouses. It also grants the Department explicit authority to regulate the uses and disclosures of PHI maintained and transmitted by covered entities. Therefore, we do have the authority to condition the disclosure of PHI by a covered entity to a business associate on the covered entity's having a contract with that business associate.

Q: Has the Secretary exceeded the HIPAA statutory authority by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?

A: The Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the rule. The assurances that covered entities must obtain prior to disclosing PHI to business associates create a set of contractual obligations far narrower than the provisions of the rule, to protect information generally and help the covered entity comply with its obligations under the rule. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of PHI.

Q: Is it reasonable for covered entities to be held liable for the privacy violations of business associates?

A: A health care provider, health plan, or other covered entity is not liable for privacy violations of a business associate. Covered entities are not required to actively monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract.

Moreover, a business associate's violation of the terms of the contract does not, in and of itself, constitute a violation of the rule by the covered entity. The contract must obligate the business associate to advise the covered entity when violations have occurred.

If the covered entity becomes aware of a pattern or practice of the business associate that constitutes a material breach or violation of the business associate's obligations under its contract, the covered entity must take "reasonable steps" to cure the breach or to end the violation. Reasonable steps will vary with the circumstances and nature of the business relationship.

If such steps are not successful, the covered entity must terminate the contract if feasible. The rule also provides for circumstances in which termination is not feasible, for example, where there are no other viable business alternatives for the covered entity. In such circumstances where termination is not feasible, the covered entity must report the problem to the Department.

Only if the covered entity fails to take the kinds of steps described above would it be considered to be out of compliance with the requirements of the rule.

PARENTS AND MINORS

[45 CFR § 164.502(g)]

General Requirements

The Privacy Rule provides individuals with certain rights with respect to their personal health information, including the right to obtain access to and to request amendment of health information about themselves. These rights rest with that individual, or with the "personal representative" of that individual. In general, a person's right to control protected health information (PHI) is based on that person's right (under state or other applicable law, e.g., tribal or military law) to control the health care itself.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a "personal representative" of his or her minor child under the Privacy Rule and has the right to obtain access to health information about his or her minor child. This would also be true in the case of a guardian or other person acting *in loco parentis* of a minor.

There are exceptions in which a parent might not be the "personal representative" with respect to certain health information about a minor child. In the following situations, the Privacy Rule defers to determinations under other law that the parent does not control the minor's health care decisions and, thus, does not control the PHI related to that care.

- When state or other law does not require 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, the parent is not the minor's personal representative under the Privacy Rule. For example, when a state law provides an adolescent the right to consent to mental health treatment without the consent of his or her parent, and the adolescent obtains such treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment. The minor may choose to involve a parent in these health care decisions without giving up his or her right to control the related health information. Of course, the minor may always have the parent continue to be his or her personal representative even in these situations.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services. For example, courts 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. In order to not undermine these court decisions, the parent is not the personal representative under the Privacy Rule in these circumstances.

In the following situations, the Privacy Rule reflects current professional practice in determining that the parent is not the minor's personal representative with respect to the relevant PHI:

- When a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that conversation or relationship. For example, if a physician asks the parent of a 16-year old if the physician

First Guidance on the Final Rule

can talk with the child confidentially about a medical condition and the parent agrees, the parent would not control the PHI that was discussed during that confidential conference.

- When a physician (or other covered entity) reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

Relation to State Law

In addition to the provisions (described above) tying the right to control information to the right to control treatment, the Privacy Rule also states that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent (§ 160.202). This is true whether the state law authorizes or prohibits such disclosure. Thus, if a physician believes that disclosure of information about a minor would endanger that minor, but a state law requires disclosure to a parent, the physician may comply with the state law without violating the Privacy Rule. Similarly, a provider may comply with a state law that requires disclosure to a parent and would not have to accommodate a request for confidential communications that would be contrary to state law.

Frequently Asked Questions

Q: Does the Privacy Rule allow parents the right to see their children's medical records?

A: The Privacy Rule generally allows parents, as their minor children's personal representatives, to have access to information about the health and well-being of their children when state or other underlying law allows parents to make treatment decisions for the child. There are two exceptions: (1) when the parent agrees that the minor and the health care provider may have a confidential relationship, the provider is allowed to withhold information from the parent to the extent of that agreement; and (2) when the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the provider is permitted not to treat the parent as the child's personal representative with respect to health information.

Secretary Thompson has stated that he is reassessing these provisions of the regulation.

Q: Does the Privacy Rule provide rights for children to be treated without parental consent?

A: No. The Privacy Rule does not address consent to treatment, nor does it preempt or change state or other laws that address consent to treatment. The Rule addresses access to health information, not the underlying treatment.

Q: If a child receives emergency medical care without a parent's consent, can the parent get all information about the child's treatment and condition?

First Guidance on the Final Rule

A: Generally, yes. Even though the parent did not provide consent to the treatment in this situation, under the Privacy Rule, the parent would still be the child's personal representative. This would not be so only when the minor provided consent (and no other consent is required) or the treating physician suspects abuse or neglect or reasonably believes that releasing the information to the parent will endanger the child.

HEALTH-RELATED COMMUNICATIONS AND MARKETING
[45 CFR §§ 164.501, 164.514(e)]

General Requirements

The Privacy Rule addresses the use and disclosure of protected health information (PHI) for marketing purposes in the following ways:

- Defines what is "marketing" under the rule;
- Removes from that definition certain treatment or health care operations activities;
- Set limits on the kind of marketing that can be done as a health care operation; and
- Requires individual authorization for all other uses or disclosures of PHI for marketing purposes.

What Is Marketing

The Privacy Rule defines "marketing" as "a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service." To make this definition easier for covered entities to understand and comply with, we specified what "marketing" is not, as well as generally defined what it is. As questions arise about what activities are "marketing" under the Privacy Rule, we will provide additional clarification regarding such activities.

Communications That Are Not Marketing

The Privacy Rule carves out activities that are not considered marketing under this definition. In recommending treatments or describing available services, health care providers and health plans are advising us to purchase goods and services. To prevent any interference with essential treatment or similar health-related communications with a patient, the rule identifies the following activities as not subject to the marketing provision, even if the activity otherwise meets the definition of marketing. (Written communications for which the covered entity is compensated by a third party are not carved out of the marketing definition.)

Thus, a covered entity is not "marketing" when it:

- Describes the participating providers or plans in a network. For example, a health plan is not marketing when it tells its enrollees about which doctors and hospitals are preferred providers, which are included in its network, or which providers offer a particular service. Similarly, a health insurer notifying enrollees of a new pharmacy that has begun to accept its drug coverage is not engaging in marketing.
- Describes the services offered by a provider or the benefits covered by a health plan. For example, informing a plan enrollee about drug formulary coverage is not marketing.

First Guidance on the Final Rule

Furthermore, it is not marketing for a covered entity to use an individual's PHI to tailor a health-related communication to that individual, when the communication is:

- Part of a provider's treatment of the patient and for the purpose of furthering that treatment. For example, recommendations of specific brand-name or over-the-counter pharmaceuticals or referrals of patients to other providers are not marketing.
- Made in the course of managing the individual's treatment or recommending alternative treatment. For example, reminder notices for appointments, annual exams, or prescription refills are not marketing. Similarly, informing an individual who is a smoker about an effective smoking-cessation program is not marketing, even if that program is offered by someone other than the provider or plan making the recommendation.

Limitations on Marketing Communications

If a communication is marketing, a covered entity may use or disclose PHI to create or make the communication, pursuant to any applicable consent obtained under § 164.506, only in the following circumstances:

- It is a face-to-face communication with the individual. For example, sample products may be provided to a patient during an office visit.
- It involves products or services of nominal value. For example, a provider can distribute pens, toothbrushes, or key chains with the name of the covered entity or a health care product manufacturer on it.
- It concerns the health-related products and services of the covered entity or a third party, and only if the communication:
 - Identifies the covered entity that is making the communication. Thus, consumers will know the source of these marketing calls or materials.
 - States that the covered entity is being compensated for making the communication, when that is so.
 - Tells individuals how to opt out of further marketing communications, with some exceptions as provided in the rule. The covered entity must make reasonable efforts to honor requests to opt-out.
 - Explains why individuals with specific conditions or characteristics (e.g., diabetics, smokers) have been targeted, if that is so, and how the product or service relates to the health of the individual. The covered entity must also have made a determination that the product or service may be of benefit to individuals with that condition or characteristic.

For all other communications that are "marketing" under the Privacy Rule, the covered entity must obtain the individual's authorization to use or disclose PHI to create or make the marketing communication.

Business Associates

Disclosure of PHI for marketing purposes is limited to disclosure to business associates that undertake marketing activities on behalf of the covered entity. No other disclosure for marketing is permitted. Covered entities may not give away or sell lists of patients or enrollees without obtaining authorization from each person on the list. As with any disclosure to a business associate, the covered entity must obtain the business associate's agreement to use the PHI only for the covered entity's marketing activities. A covered entity may not give PHI to a business associate for the business associate's own purposes.

Frequently Asked Questions

Q: Does this rule expand the ability of providers, plans, marketers and others to use my PHI to market goods and services to me? Does the Privacy Rule make it easier for health care businesses to engage in door-to-door sales and marketing efforts?

A: No. The provisions described above impose limits on the use or disclosure of PHI for marketing that do not exist in most states today. For example, the rule requires patients' authorization for the following types of uses or disclosures of PHI for marketing:

- Selling PHI to third parties for their use and re-use. Under the rule, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines.
- Disclosing PHI to outsiders for the outsiders' independent marketing use. Under the rule, doctors may not provide patient lists to pharmaceutical companies for those companies' drug promotions.

These activities can occur today with no authorization from the individual. In addition, for the marketing activities that are allowed by the rule without authorization from the individual, the Privacy Rule requires covered entities to offer individuals the ability to opt-out of further marketing communications.

Similarly, under the business associate provisions of the rule, a covered entity may not give PHI to a telemarketer, door-to-door salesperson, or other marketer it has hired unless that marketer has agreed by contract to use the information only for marketing on behalf of the covered entity. Today, there may be no restrictions on how marketers re-use information they obtain from health plans and providers.

Q: Can telemarketers gain access to PHI and call individuals to sell goods and services?

A: Under the rule, unless the covered entity obtains the individual's authorization, it may only give health information to a telemarketer that it has hired to undertake marketing on its behalf. The telemarketer must be a business associate under the rule, which means that it must agree by contract to use the information only for marketing on behalf of the covered entity, and not to market its own goods or services (or those of another third party). The caller must identify the covered entity that is sponsoring the marketing call. The caller must provide individuals the opportunity to opt-out of further marketing.

Q: When is an authorization required from the patient before a provider or health plan engages in marketing to that individual?

A: An authorization for use or disclosure of PHI for marketing is always required, unless one of the following three exceptions apply:

- The marketing occurs during an in-person meeting with the patient (e.g., during a medical appointment).
- The marketing concerns products or services of nominal value.
- The covered entity is marketing health-related products and services (of either the covered entity or a third party), the marketing identifies the covered entity that is responsible for the marketing, and the individual is offered an opportunity to opt-out of further marketing. In addition, the marketing must tell people if they have been targeted based on their health status, and must also tell people when the covered entity is compensated (directly or indirectly) for making the communication.

Q: How can I distinguish between activities for treatment, payment or health care operations (TPO) versus marketing activities?

A: There is no need for covered entities to make this distinction. In recommending treatments, providers and health plans advise us to purchase good and services. The overlap between "treatment," "health care operations," and "marketing" is unavoidable. Instead of creating artificial distinctions, the rule imposes requirements that do not require such distinctions. Specifically:

- If the activity is included in the rule's definition of "marketing," the rule's provisions restricting the use or disclosure of PHI for marketing purposes will apply, whether or not that communication also meets the rule's definition of "treatment," "payment," or "health care operations." For these communications, the individual's authorization is required before a covered entity may use or disclose PHI for marketing unless one of the exceptions to the authorization requirement (described above) applies.
- The rule exempts certain activities from the definition of "marketing." If an activity falls into one of the definition's exemptions, the marketing rules do not apply. In these cases, covered entities may engage in the activity without first obtaining an authorization if the activity meets the definition of "treatment," "payment," or "health care operations." These exemptions are described above, in the section titled "Communications That Are Not Marketing," and are designed to ensure that nothing in this rule interferes with treatment activities.

Q: Do disease management, health promotion, preventive care, and wellness programs fall under the definition of "marketing"?

A: Whether these kinds of activities fall under the rule's definition of "marketing" depends on the specifics of how the activity is conducted. The activities currently undertaken under these rubrics

First Guidance on the Final Rule

are diverse. Covered entities must examine the particular activities they undertake, and compare these to the activities that are exempt from the definition of "marketing."

Q: Can contractors (business associates) use PHI to market to individuals for their own business purposes?

A: The Privacy Rule prohibits health plans and covered health care providers from giving PHI to third parties for the third party's own business purposes, absent authorization from the individuals. Under the statute, this regulation cannot govern contractors directly.

First Guidance on the Final Rule

RESEARCH

[45 CFR §§ 164.501, 164.508(f), 164.512(i)]

Background

The Privacy Rule establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes. A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with §§ 164.502(d), 164.514(a)-(c) of the rule) without regard to the provisions below.

The Privacy Rule also defines the means by which individuals/human research subjects are informed of how medical information about themselves will be used or disclosed and their rights with regard to gaining access to information about themselves, when such information is 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 (codified for the Department of Health and Human Services (HHS) at Title 45 Code of Federal Regulations Part 46) and/or the Food and Drug Administration's (FDA) human subjects protection regulations, which have some provisions that are similar to, but more stringent than and separate from, the Privacy Rule's provisions for research.

Using and Disclosing PHI for Research

In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose PHI 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 PHI without authorization by the research participant, a covered entity must obtain one of the following:

- 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 Institutional Review Board (IRB) or a Privacy Board. 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 it is not practicable to obtain research participants' authorization.

or

- Representations from the researcher, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to

First Guidance on the Final Rule

research, that the researcher will not remove any PHI from the covered entity, *and* representation that PHI for which access is sought is necessary for the research purpose. This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.

or

- Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI 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.

A covered entity may use or disclose PHI 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:

- A statement that the alteration or waiver of authorization was approved by an IRB or Privacy Board that was composed as stipulated by the Privacy Rule;
- A statement identifying 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 following eight criteria:
 - The use or disclosure of PHI involves no more than minimal risk to the individuals;
 - The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
 - The research could not practicably be conducted without the alteration or waiver;
 - The research could not practicably be conducted without access to and use of the PHI;
 - The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
 - There is an adequate plan to protect the identifiers from improper use and disclosure;
 - There is 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
 - There are adequate written assurances that the PHI 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 PHI would be permitted by this subpart.
- A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board;

First Guidance on the Final Rule

- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as stipulated by the Privacy Rule; and
- The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

Research Use/Disclosure With Individual Authorization:

The Privacy Rule also permits covered entities to use and disclose PHI 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 PHI.

To use or disclose PHI created from a research study that includes treatment (e.g., a clinical trial), additional research-specific elements must be included in the authorization form required under § 164.508, which describe how PHI created for the research study will be used or disclosed. For example, if the covered entity/researcher intends to seek reimbursement from the research subject's health plan for the routine costs of care associated with the protocol, the authorization must describe types of information that will be provided to the health plan. This authorization may be combined with the traditional informed consent document used in research.

The Privacy Rule permits, but does not require, the disclosure of PHI for specified public policy purposes in § 164.512. With few exceptions, the covered entity/researcher may choose to limit its right to disclose information created for a research study that includes treatment to purposes narrower than those permitted by the rule, in accordance with his or her own professional standards.

Frequently Asked Questions

Q: Will the rule hinder medical research by making doctors and others less willing and/or able to share information about individual patients?

A: We do not believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to participate in research when they know their information is protected. For example, in genetic studies at the National Institutes of Health (NIH), nearly 32 percent of eligible people offered a test for breast cancer risk decline to take it. The overwhelming majority of those who refuse cite concerns about health insurance discrimination and loss of privacy as the reason. The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

The Privacy Rule will require some covered health care providers and health plans to change their current practices related to documenting research uses and disclosures. It is possible that some covered health care providers and health plans may conclude that the rule's requirements

for research uses and disclosures are too burdensome and will choose to limit researchers' access to PHI. We believe few providers will take this route, however, because the Common Rule includes similar, and more stringent requirements, that have not impaired the willingness of researchers to undertake federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires IRB review for all research proposals under its purview, even if informed consent is to be sought. The Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of PHI for research purposes is to be altered or waived.

Q: Are some of the criteria so subjective that inconsistent determinations may be made by IRBs and Privacy Boards reviewing similar or identical research projects?

A: Under the Privacy Rule, IRBs and Privacy Boards need to use their judgment as to whether the waiver criteria have been satisfied. Several of the waiver criteria are closely modeled on the Common Rule's criteria for the waiver of informed consent and for the approval of a research study. Thus, it is anticipated that IRBs already have experience in making the necessarily subjective assessments of risks and benefits. While IRBs or Privacy Boards may reach different determinations, the assessment of the waiver criteria through this deliberative process is a crucial element in the current system of safeguarding research participants' privacy. The entire system of local IRBs is, in fact, predicated on a deliberative process that permits local IRB autonomy. The Privacy Rule builds upon this principle; it does not change it.

In addition, for multi-site research that requires PHI from two or more covered entities, the Privacy Rule permits covered entities to accept documentation of IRB or Privacy Board approval from a single IRB or Privacy Board.

Q: Does the Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing PHI?

A: No. The Privacy Rule does not address conditions for enrollment in a research study. Therefore, the Privacy Rule in no way prohibits researchers from conditioning enrollment in a research study on the execution of an authorization for the use of pre-existing health information.

Q: Does the Privacy Rule permit the creation of a database for research purposes through an IRB or Privacy Board waiver of individual authorization?

A: Yes. A covered entity may use or disclose PHI without individuals' authorizations for the creation of a research database, provided the covered entity obtains documentation that an IRB or Privacy Board has determined that the specified waiver criteria were satisfied. PHI maintained in such a research database could be used or disclosed for future research studies as permitted by the Privacy Rule - that is, for future studies in which individual authorization has been obtained or where the rule would permit research without an authorization, such as pursuant to an IRB or Privacy Board waiver.

Q: Will IRBs be able to handle the additional responsibilities imposed by the Privacy Rule?

A: Recognizing that some institutions may not have IRBs, or that some IRBs may not have the expertise needed to review research that requires consideration of risks to privacy, the Privacy Rule permits the covered entity to accept documentation of waiver of authorization from an alternative body called a Privacy Board-which could have fewer members, and members with different expertise than IRBs.

In addition, for research that is determined to be of no more than minimal risk, IRBs and Privacy Boards could use an expedited review process, which permits covered entities to accept documentation when only one or more members of the IRB or Privacy Board have conducted the review.

Q: By establishing new waiver criteria and authorization requirements, hasn't the Privacy Rule, in effect, modified the Common Rule?

A: No. Where both the Privacy Rule and the Common Rule apply, both regulations must be followed. The Privacy Rule regulates only the content and conditions of the documentation that covered entities must obtain before using or disclosing PHI for research purposes.

Q: Is documentation of IRB *and* Privacy Board approval required before a covered entity would be permitted to disclose PHI for research purposes without an individual's authorization?

A: No. The Privacy Rule requires documentation of waiver approval by either an IRB *or* a Privacy Board, not both.

Q: Does a covered entity need to create an IRB or Privacy Board before using or disclosing PHI for research?

A: No. The IRB or Privacy Board could be created by the covered entity or the recipient researcher, or it could be an independent board.

Q: What does the Privacy Rule say about a research participant's right of access to research records or results?

A: With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained in a "designated record set." A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. Research records or results maintained in a designated record set are accessible to research participants unless one of the Privacy Rule's permitted exceptions applies.

One of the permitted exceptions applies to PHI created or obtained by a covered health care provider/researcher for a clinical trial. The Privacy Rule permits the individual's access rights in

these cases to be suspended *while the clinical trial is in progress*, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the health care provider/researcher must inform the research participant that the right to access PHI will be reinstated at the conclusion of the clinical trial.

Q: Are the Privacy Rule's requirements regarding patient access in harmony with the Clinical Laboratory Improvements Amendments of 1988 (CLIA)?

A: Yes. The Privacy Rule does not require clinical laboratories that are also covered health care providers to provide an individual access to information if CLIA prohibits them from doing so. CLIA permits clinical laboratories to provide clinical laboratory test records and reports only to "authorized persons," as defined primarily by state law. The individual who is the subject of the information is not always included as an authorized person. Therefore, the Privacy Rule includes an exception to individuals' general right to access PHI about themselves if providing an individual such access would be in conflict with CLIA.

In addition, for certain research laboratories that are exempt from the CLIA regulations, the Privacy Rule does not require such research laboratories if they are also a covered health care provider to provide individuals with access to PHI because doing so may result in the research laboratory losing its CLIA exemption.

Q: Do the Privacy Rule's requirements for authorization and the Common Rule's requirements for informed consent differ?

A: Yes. Under the Privacy Rule, a patient's authorization will be used for the use and disclosure of PHI for research purposes. In contrast, an individual's informed consent as required by the Common Rule and FDA's human subjects regulations is a consent to participate in the research study as a whole, not simply a consent for the research use or disclosure of PHI. For this reason, there are important differences between the Privacy Rule's requirements for individual authorization, and the Common Rule's and FDA's requirements for informed consent. Where the Privacy Rule, the Common Rule, and/or FDA's human subjects regulations are applicable, each of the applicable regulations will need to be followed.

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

[45 CFR §§ 160.300; 164.512(b); 164.512(f)]

Background

Under the 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, 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 Privacy Rule itself. In order to ensure covered entities protect patients' privacy as required, the rule provides that health plans, hospitals, and other covered entities cooperate with the Department's efforts to investigate complaints or otherwise ensure compliance. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the privacy protections and access rights for consumers under this rule.

Frequently Asked Questions

Q: Does the rule require my doctor to send my medical records to the government?

A: No. The rule does not require a physician or any other covered entity to send medical information to the government for a government data base or similar operation. This rule does not require or allow any new government access to medical information, with one exception: the rule does give OCR the authority to investigate complaints and to otherwise ensure that covered entities comply with the rule.

OCR has been assigned the responsibility of enforcing the Privacy Rule. As is typical in many enforcement settings, OCR may need to look at how a covered entity handled medical records and other personal health information. The Privacy Rule limits disclosure to OCR to information that is "pertinent to ascertaining compliance." OCR will maintain stringent controls to safeguard any individually identifiable health information that it receives. If covered entities could avoid or ignore enforcement requests, consumers would not have a way to ensure an independent review of their concerns about privacy violations under the rule.

Q: Why would a Privacy Rule require covered entities to turn over anybody's personal health information as part of a government enforcement process?

A: An important ingredient in ensuring compliance with the Privacy Rule is the Department's responsibility to investigate complaints that the rule has been violated and to follow up on other information regarding noncompliance. At times, this responsibility entails seeing personal health

information, such as when an individual indicates to the Department that they believe a covered entity has not properly handled their medical records.

What information would be needed depends on the circumstances and the alleged violations. The Privacy Rule limits OCR's access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information would be needed. For instance, OCR may need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

Examples of investigations that may require OCR to have access to protected health information (PHI) include:

- Allegations that a covered entity refused to note a request for correction in a patient's medical record, or did not provide complete access to a patient's medical records to that patient.
- Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals' authorization when required by the rule. OCR may need to review information in the marketing department that contains personal health information, to determine whether a violation has occurred.

Q: Will this rule make it easier for police and law enforcement agencies to get my medical information?

A: No. The rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists. Today, law enforcement officers obtain health information for many purposes, sometimes without a warrant or other prior process. The rule establishes new procedures and safeguards to restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement. In most states, such permission is not required today.

Where state law imposes additional restrictions on disclosure of health information to law enforcement, those state laws continue to apply. This rule sets a national floor of legal protections; it is not a set of "best practices."

Even in those circumstances when disclosure to law enforcement is permitted by the rule, the Privacy Rule does not require covered entities to disclose any information. Some other federal or state law may require a disclosure, and the Privacy Rule does not interfere with the operation of

these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.

Q: Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

A: No. All states have laws that require providers to report cases of specific diseases to public health officials. The Privacy Rule allows disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births, investigating the occurrence and cause of injury and disease, and monitoring adverse outcomes related to food, drugs, biological products, and dietary supplements.

Q: How does the rule affect my rights under the federal Privacy Act?

A: The Privacy Act of 1974 protects personal information about individuals held by the federal government. Covered entities that are federal agencies or federal contractors that maintain records that are covered by the Privacy Act not only must obey the Privacy Rule's requirements but also must comply with the Privacy Act.

PAYMENT [45 CFR 164.501]

General Requirements

As provided for by the Privacy Rule, a covered entity may use and disclose protected health information (PHI) for payment purposes. "Payment" is a defined term that encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and for 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).

Frequently Asked Questions

Q: Does the 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 PHI about the individual: name and address; date of birth; social security number; payment history; 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.

We are not aware of any conflict in the consumer credit reporting disclosures permitted by the Privacy Rule and FCRA. The Privacy Rule permits uses and disclosures by the covered entity or its business associate as may be required by FCRA or other law. Therefore, we do not believe there would be a conflict between the Privacy Rule and legal duties imposed on data furnishers by FCRA.

Q: Does the Privacy Rule prevent health plans and providers from using debt collection agencies? Does the 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. 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 under a business associate agreement are governed by other provisions of the rule, including consent (where consent is required) and the minimum necessary requirements.

We are not aware of any conflict between the Privacy Rule and the Fair Debt Collection Practices Act. Where a use or disclosure of PHI 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 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." 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. 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.