

HIPAA PRIVACY RULE FAQs

STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

OCR HIPAA Privacy
TA 164.501.001
July 6, 2001

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) and promulgated by the Department of Health and Human Services (HHS). 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. 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.

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.
- 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:

- 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.

ORAL COMMUNICATIONS

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.

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 determining what is reasonable, the Department will take into account the concerns of covered

entities regarding potential effects on patient care and financial burden.

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.

PARENTS AND MINORS

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 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.

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.

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.

PAYMENT

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).

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.