STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

[*45 CFR Parts 160 and 164*]

Introduction

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

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

The guidance that follows is meant to communicate as clearly as possible the privacy policies contained in the Privacy Rule. For a particular segment in the Privacy Rule, the guidance will provide a brief explanation of the segment and how the Rule works, followed by "Frequently Asked Questions" about that provision. The guidance does not address all of the relevant provisions in the Rule, although we anticipate adding segments in the future as we develop guidance on more Privacy Rule standards. We will also be adding to the "Frequently Asked Questions" on an ongoing basis as new questions arise. HHS plans to work expeditiously to address these additional questions to facilitate understanding of the Rule and to encourage voluntary compliance with its requirements. However, for a full understanding of one's rights and responsibilities under the Rule, it is important to consult the Rule itself.

The Privacy Rule Standards Addressed

General Overview
Incidental Uses and Disclosures (45 CFR 164.502(a))
Minimum Necessary (45 CFR 164.502(b), 164.514(d))
Personal Representatives (45 CFR 164.502(g))
Business Associates (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e))
Uses and Disclosures for Treatment, Payment, and Health Care Operations (45 CFR 164.506)
Marketing (45 CFR 164.501, 164.508(a))
Public Health (45 CFR 164.512(b))
Research (45 CFR 164.501, 164.508, 164.512(i), 164.514(e), 164.528, 164.532)

Workers' Compensation Laws (45 CFR 164.512(*l*))
Notice (45 CFR 164.520)
Government Access (45 CFR Part 160, Subpart C, 164.512(f))
Miscellaneous FAQs

GENERAL OVERVIEW OF STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

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

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

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

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

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

The Privacy Rule establishes, for the first time, a foundation of Federal protections for the privacy of protected health information. The Rule does not replace Federal, State, or other law that grants individuals even greater privacy protections, and covered entities are free to retain or adopt more protective policies or practices.

GENERAL OVERVIEW

Frequently Asked Questions

Q: What does the HIPAA Privacy Rule do?

A: Most health plans and health care providers that are covered by the new Rule must comply with the new requirements by April 14, 2003.

The HIPAA 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 supports 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.

X It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.

X It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.

X It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.

X It empowers individuals to control certain uses and disclosures of their health information.

Q: Why is the HIPAA Privacy Rule needed?

A: In enacting HIPAA, Congress mandated the establishment of Federal 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 patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient's permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could 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. However, 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 the protection of personal health information.

Q: Generally, what does the HIPAA Privacy Rule 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:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing 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 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 Rule 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 HIPAA privacy standards?

A: As required by Congress in HIPAA, the Privacy Rule covers:

- Health plans

- Health care clearinghouses

- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been 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 the Department of Health and Human Services (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. See the fact sheet and frequently asked questions on this web site about the standards on "Business Associates" for 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 HIPAA privacy standards?

A: As Congress required in HIPAA, most covered entities have until April 14, 2003 to come into compliance with these standards, as modified by the August, 2002 final Rule. Small health plans will have an additional year – until April 14, 2004 – to come into compliance.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is providing assistance to help covered entities prepare to comply with the Rule. For example, OCR maintains a web site with helpful information, such as the Guidance, Frequently Asked Questions, sample "business associate" contract provisions, significant reference documents, and other technical assistance information for consumers and the health care industry, at http://www.hhs.gov/ocr/hipaa/.

Q: What were the major modifications to the HIPAA Privacy Rule that the Department of Health and Human Services (HHS) adopted in August 2002?

A: Based on the information received through public comments, testimony at public hearings, meetings at the request of industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieve unintended administrative burdens created by the Privacy Rule.

Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:

- Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual's consent for these activities;
- The notice of privacy practices that covered entities must provide to patients;
- Uses and disclosures for marketing purposes;

- Minimum necessary uses and disclosures;
- Parents as the personal representatives of unemancipated minors;
- Uses and disclosures for research purposes; and
- Transition provisions, including business associate contracts.

In addition to these key areas, the modifications included changes to certain other provisions where necessary to clarify the Privacy Rule, and a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

For more information about the final modifications to the Privacy Rule, see the Fact Sheet entitled, *Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule*. This Fact Sheet can be found at http://www.hhs.gov/news/press/2002pres/20020809.html.

Q: Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?

A: The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care. The following are some examples of how the consent requirement would have posed barriers to health care:

- Pharmacists would not have been able to fill a prescription, search for potential drug interactions, determine eligibility, or verify coverage before the individual arrived at the pharmacy to pick up the prescription if the individual had not already provided consent under the Privacy Rule.
- Hospitals would not have been able to use information from a referring physician to schedule and prepare for procedures before the individual presented at the hospital for such procedure, or the patient would have had to make a special trip to the hospital to sign the consent form.
- Providers who do not provide treatment in person (such as a provider prescribing over the telephone) may have been unable to provide care because they would have had difficulty obtaining prior written consent to use protected health information at the first service delivery.

- Emergency medical providers were concerned that, even if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if that would be inconsistent with the appropriate practice of emergency medicine.

- Emergency medical providers were also concerned that the requirement that they attempt to obtain consent as soon as reasonably practicable after an emergency would have required significant efforts and administrative burden which might have been viewed as harassing by patients, because these providers typically do not have ongoing relationships with individuals.

To eliminate such barriers to health care, mandatory consent was replaced with the voluntary consent provision that permits health care providers to obtain consent for treatment, payment and healthcare operations, at their option, and enables them to obtain consent in a manner that does not disrupt needed treatment. Although consent is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumers' access to care or the quality of that care. Further, the individual's right to request restrictions on the use or disclosure of his or her protected health information is retained in the Rule as modified.

Q: Did the final modifications to the HIPAA Privacy Rule alter the compliance date(s) for covered entities?

A: No. The compliance dates for the Privacy Rule, as modified, remain April 14, 2003, for most health plans, covered health care providers, and health care clearinghouses, and April 14, 2004, for small health plans. Under HIPAA, compliance with a modification to an existing standard or implementation specification is required by a date set by the Secretary, but not earlier than 180 days from the adoption of the modification. By publishing the modifications to the Privacy Rule in August 2002, the original compliance date of April 2003 is maintained for the entire Rule, as modified.

Q: Will the Department of Health and Human Services (HHS) make future changes to the HIPAA Privacy Rule and, if so, how will these changes be made?

A: Under HIPAA, HHS has the authority to modify the privacy standards as the Secretary may deem appropriate. However, a standard can be modified only once in a 12-month period.

As a general rule, future modifications to the Privacy Rule must be made in accordance with the Administrative Procedure Act (APA). HHS will comply with the APA by publishing proposed rule changes, if any, 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 modified final rule.

INCIDENTAL USES AND DISCLOSURES

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

Background

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

How the Rule Works

General Provision. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied *reasonable safeguards* and implemented the *minimum necessary standard*, where applicable, with respect to the primary use or disclosure. See 45 CFR 164.502(a)(1)(iii). An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

Reasonable Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Many health care providers and professionals have long made it a practice to ensure

reasonable safeguards for individuals' health information – for instance:

X By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;

X By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;

X By isolating or locking file cabinets or records rooms; or

X By providing additional security, such as passwords, on computers maintaining personal information.

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

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

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

For example:

X The minimum necessary standard requires that a covered entity limit who within the entity has access to protected health information, based on who needs access to perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's

conversation about a patient's condition, would be an unlawful use or disclosure under the Privacy Rule.

INCIDENTAL USES AND DISCLOSURES

Frequently Asked Questions

Q: Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

A: Yes. The HIPAA 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. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

X Health care staff may orally coordinate services at hospital nursing stations.

X Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.

X A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.

X A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.

X Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.

X A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired,

such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

Q: Does the HIPAA 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 protected health information. This standard requires that covered entities 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.

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

X Private rooms.

X Soundproofing of rooms.

X Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.

X Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

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

X Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.

X In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, 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, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or among professionals treating the patient.

X Hospitals could ensure that areas housing patient files are supervised or locked.

Q: May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

A: Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. See 45 CFR 164.510(b)(3).

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, the Department considers a request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be

reasonable requests, absent extenuating circumstances. See 45 CFR 164.522(b).

Q: May physicians offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

A: Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Q: Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?

A: No. The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices. Covered entities must implement reasonable safeguards to protect an individual's privacy. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to protected health information. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual's privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms.

  Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient

visible to anyone who walks by.

- Announcing patient names and other information over a facility's public announcement system.

  Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

- Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

  Possible safeguards may include: if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

  The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

Q: A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

A: Yes, the Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. See 45 CFR 164.502(a)(1)(iii). As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied. Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances. See 45 CFR 164.530(c).

Q: A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?

A: The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or health care operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate. See 45 CFR 164.502(a)(1)(iii). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances.

Q: May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?

A: Yes. Disclosures of protected health information in a group therapy setting are treatment disclosures and, thus, may be made without an individual's authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual's care. Where the individual is present during the disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual's agreement to participate in group therapy or family discussions is a good basis for inferring the individual's agreement.

Q: Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?

A: No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule. See 45 CFR 164.528(a)(1).

Q: Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

A: No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

X A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.

X A health plan employee discussing a patient's health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

Q: Is a covered entity required to prevent any incidental use or disclosure of protected health information?

A: No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures. See 45 CFR 164.530(c)(2).

MINIMUM NECESSARY

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

Background

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

How the Rule Works

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

X Disclosures to or requests by a health care provider for treatment purposes.

X Disclosures to the individual who is the subject of the information.

X Uses or disclosures made pursuant to an individual's authorization.

X Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.

X Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.

X Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum

necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

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

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

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

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

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

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

X Another covered entity.

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

X 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.

MINIMUM NECESSARY

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 HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information 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 protected health information 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 an absolute 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 and plans today to limit the unnecessary sharing of medical information.

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

Q: Won't the HIPAA Privacy Rule's 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.

Uses of protected health information for treatment are not exempt from the minimum necessary standard. However, the Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to 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 may 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 HIPAA Privacy Rule's 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 Privacy 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 the HIPAA Privacy Rule's minimum necessary standard be applied to uses or disclosures that are authorized by an individual?

A: No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. 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 45 CFR 164.508.

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 HIPAA Privacy Rule's minimum necessary requirements. Furthermore, 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 45 CFR 164.508 of the Privacy 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 45 CFR 164.508.

Q: Doesn't the HIPAA Privacy Rule's minimum necessary standard conflict with the HIPAA transactions standards?

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 transactions standards, including disclosures of all data elements that are required or situationally required in those transactions. See 45 CFR 164.502(b)(2)(vi). However, covered entities have significant discretion as to the information included in the transactions as optional data elements. Therefore, the minimum necessary standard does apply to the optional data elements. The transactions standard adopted for the outpatient pharmacy sector is an example of a standard that uses optional data elements. The health plan, or payer, currently specifies which of the optional data elements are needed for payment of its particular pharmacy claims. The health plan or its business associates must apply the minimum necessary standard when requesting this information. In this example, a pharmacist may reasonably rely on the health plan's request for information as the minimum necessary for the intended disclosure. For example, as part of a routine protocol, the name of the individual may be requested by the payer as the minimum necessary to validate the identity of the claimant or for drug interaction or other patient safety reasons.

Q: Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time an entire medical record is disclosed?

A: No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and 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 and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes.

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 purposes or disclosures to the individual who is the subject of the protected health information.

Q: A provider might have a patient's medical record that contains older portions of a medical record that were created by another or previous provider. Will the HIPAA

Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

A: Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to protected health information 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. In this case, appropriate training of employees may be sufficient. 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 Privacy Rule.

Q: Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of protected health information it makes to another covered entity?

A: Covered entities are required to apply the minimum necessary standard to their own requests for protected health information. One covered entity may reasonably rely on another covered entity's request as the minimum necessary, and then does not need to engage in a separate minimum necessary determination. See 45 CFR 164.514(d)(3)(iii). However, if a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered

entities to negotiate a resolution of the dispute as to the amount of information needed. Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with another covered entity making a 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.

Q: May a covered entity accept documentation of an external Institutional Review Board's (IRB) waiver of authorization for purposes of reasonably relying on the request as the minimum necessary?

A: Yes. The HIPAA Privacy Rule explicitly permits a covered entity to reasonably rely on a researcher's documentation of an Institutional Review Board (IRB) or Privacy Board waiver of authorization pursuant to 45 CFR 164.512(i) that the information requested is the minimum necessary for the research purpose. See 45 CFR 164.514(d)(3)(iii). This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or from one that is associated with the covered entity.

Q: Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

A: A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

PERSONAL REPRESENTATIVES
[*45 CFR 164.502(g)*]

Background

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

How the Rule Works

General Provisions. Except as otherwise provided in 45 CFR 164.502(g), the Privacy Rule requires covered entities to treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.

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

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

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

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

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

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

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

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

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

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

Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

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

Example: A physician asks the parent of a 16-year-old if the physician can

talk with the child confidentially about a medical condition and the parent agrees.

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

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

PERSONAL REPRESENTATIVES

Frequently Asked Questions

Q. Does the HIPAA Privacy Rule change the way in which an individual can grant another person health care power of attorney?

A. No. Nothing in the Privacy Rule changes the way in which an individual grants another person power of attorney for health care decisions. State law (or other law) regarding health care powers of attorney continue to apply. The intent of the provisions regarding personal representatives was to complement, not interfere with or change, current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions which give others the ability to exercise the rights of, or make treatment decisions related to, an individual. The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under other law, the ability to exercise the rights of that individual with respect to health information.

Q. If someone has health care power of attorney for an individual, can they obtain access to that individual's medical record?

A. Yes, an individual that has been given a health care power of attorney will have the right to access the medical records of the individual related to such representation to the extent permitted by the HIPAA Privacy Rule at 45 CFR 164.524. However, when a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual.

Q. Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?

A. The HIPAA Privacy Rule treats an adult or emancipated minor's personal representative as the individual for purposes of the Rule regarding the health care matters that relate to the representation, including the right of access under 45 CFR 164.524. The scope of access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual's protected health information regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to protected health information that may be

relevant to making decisions within the personal representative's authority. For example, if a personal representative's authority is limited to authorizing artificial life support, then the personal representative's access to protected health information is limited to that information which may be relevant to decisions about artificial life support.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor's personal representative as the individual. Specifically, the Privacy Rule does not require a covered entity to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults and both emancipated and unemancipated minors who may be subject to abuse or neglect by their personal representatives.

Q: How can family members of a deceased individual obtain the deceased individual's protected health information that is relevant to their own health care?

A: The HIPAA Privacy Rule recognizes that a deceased individual's protected health information may be relevant to a family member's health care. The Rule provides two ways for a surviving family member to obtain the protected health information of a deceased relative. First, disclosures of protected health information for treatment purposes—even the treatment of another individual—do not require an authorization; thus, a covered entity may disclose a decedent's protected health information, without authorization, to the health care provider who is treating the surviving relative. Second, a covered entity must treat a deceased individual's legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual or his estate, as a personal representative with respect to protected health information relevant to such representation. Therefore, if it is within the scope of such personal representative's authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.

Q: Does the HIPA Privacy Rule address when a person may not be the appropriate person to control an individual's protected health information?

A: Generally, no. The Rule defers to State and other laws that address the fitness of a person to act on an individual's behalf. However, a covered entity does not have to treat a personal representative as the individual when it reasonably believes, in the exercise of professional judgment, the individual is subject to domestic violence, abuse or neglect by the personal representative, or doing so would otherwise endanger the individual.

Q: Does a power of attorney given to a person for purposes other than health care, such as a power of attorney to close on real estate, authorize that person to access an individual's health information as that individual's personal representative?

A: No. Except with respect to decedents, a covered entity must treat a personal representative as the individual only when that person has authority under other law to act on the individual's behalf on matters related to health care. A power of attorney that does not include decisions related to health care in its scope would not authorize the holder to exercise the individual's rights under the HIPAA Privacy Rule. Further, a covered entity does not have to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

With respect to personal representatives of deceased individuals, the Privacy Rule requires a covered entity to treat the personal representative as the individual as long as the person has the authority under law to act for the decedent or the estate. The power of attorney would have to be valid after the individual's death to qualify the holder as the personal representative of the decedent.

Q: May adults with mental retardation control their protected health information if they are able to authorize uses and disclosures of their protected health information?

A: Individuals may control their protected health information under the HIPAA Privacy Rule to the extent State or other law permits them to act on their own behalf. Further, even if an individual is deemed incompetent under State or other law to act on his or her own behalf, covered entities may decline a request by a personal representative for protected health information if the individual objects to the disclosure (or for any other reason), and the disclosure is merely permitted, but not required, under the Rule.

However, covered entities must make disclosures that are required under the Rule (i.e., disclosures to the Secretary under subpart C of part 160 regarding enforcement of the Rule, and to the individual under 45 CFR 164.524 and 164.528 with respect to the individual's right of access to his or her protected health information and an accounting of disclosures, respectively). Consequently, with respect to the individual's right of access to protected health information and for an accounting of disclosures, covered entities must provide the individual's personal representative access to the individual's protected health information or an accounting of disclosures upon the request of the personal representative, unless the covered entity, in the exercise of professional judgment, believes doing so would not be in the best interest of the individual because of

a reasonable belief that the individual may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. The Rule allows a specified time period before a covered entity must act on such a request; and during this interim period, an individual and his personal representative will have an opportunity to resolve any dispute they may have concerning the request.

Q: How does a covered entity identify an individual's personal representative?

A: State or other law determines who is authorized to act on an individual's behalf, thus the Privacy Rule does not address how personal representatives should be identified. Covered entities should continue to identify personal representatives the same way they have in the past. However, the HIPAA Privacy Rule does require covered entities to verify a personal representative's authority in accordance with 45 CFR 164.514(h).

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

A. Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are: (1) when the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law; (2) when the minor obtains care at the direction of a court or a person appointed by the court; and (3) when, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship. However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases, the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

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?

A: Generally, yes. Even though the parent did not consent to the treatment in this situation, the parent would be the child's personal representative under the HIPAA Privacy Rule. This would not be so when the parent does not have authority to act for the child (e.g., parental rights have been terminated), when expressly prohibited by State or other applicable law, or when the covered entity, in the exercise of professional judgment, believes that providing such information would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

Q: Does the HIPAA 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, and disclosure of, health information, not the underlying treatment.

Q. When an individual reaches the age of majority or becomes emancipated, who controls the protected health information concerning health care services rendered while the individual was an unemancipated minor?

A: The individual who is the subject of the protected health information can exercise all rights granted by the HIPAA Privacy Rule with respect to all protected health information about him or her, including information obtained while the individual was an unemancipated minor consistent with State or other law. Generally, the parent would no longer be the personal representative of his or her child once the child reaches the age of majority or becomes emancipated, and therefore, would no longer control the health information about his or her child. Of course, any individual can have a personal representative – which may include a parent – who can exercise rights on his or her behalf.

Q. May a psychologist continue his practice to notify a parent before treating his or her minor child, even though the minor child is able to consent to such health care under State law?

A. The HIPAA Privacy Rule would defer to State or other applicable law that addresses the disclosure of health information to a parent about a minor child. If the minor child is permitted, under State law, to consent to such health care without the consent of her parent and does consent to such care, the provider may notify the parent when the State

law explicitly requires or permits the health provider to do so. If State law permits the minor child to consent to such health care without parental consent, but is silent on parental notification, the provider would need the child's permission to notify a parent.

BUSINESS ASSOCIATES

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

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Provision. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

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

X A member of the covered entity's workforce is not a business associate.

X A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

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

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

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

Examples of Business Associates.

X A third party administrator that assists a health plan with claims processing.

X A CPA firm whose accounting services to a health care provider involve access to protected health information.

X An attorney whose legal services to a health plan involve access to protected health information.

X A consultant that performs utilization reviews for a hospital.

X A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.

X An independent medical transcriptionist that provides transcription services to a physician.

X A pharmacy benefits manager that manages a health plan's pharmacist network.

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

X Describe the permitted and required uses of protected health information by the business associate;

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

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

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

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

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

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

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

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

For example:

< A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical

chart for treatment purposes.

< A physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.

< A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.

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

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

Other Situations in Which a Business Associate Contract Is NOT Required.

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

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

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

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

OHCA.

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

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

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

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

BUSINESS ASSOCIATES

Frequently Asked Questions

Q: Has the Secretary exceeded the HIPAA 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 plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity's having a written 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 HIPAA 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 protected health information 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.

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. 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 protected health information.

Q: What are a covered entity's obligations under the HIPAA Privacy Rule with respect to protected health information held by a business associate during the contract transition period?

A: During the contract transition period, covered entities must observe the following responsibilities with respect to protected health information held by their business associates:

X Make information available to the Secretary, including information held by a

business associate, as necessary for the Secretary to determine compliance by the covered entity.

X Fulfill an individual's rights to access and amend his or her protected health information contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.

X Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of protected health information by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose protected health information to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.

Q: I have an existing contract with a business associate that will renew automatically before April 14, 2003. Does this automatic renewal mean I have to modify the contract by April 14, 2003, to make it compliant with the HIPAA Privacy Rule's business associate contract provisions or can I still take advantage of the transition period?

A: Evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002, are eligible for the transition period. The automatic renewal of a contract itself does not terminate qualification for the transition period, or the transition period itself. Renewal or modification for the purposes of the transition provisions requires action by the parties involved. For example, an automatic inflation adjustment to the price of a contract does not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before April 14, 2003.

Q: Is a covered entity liable for, or required to monitor, the actions of its business associates?

A: No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health

information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

Q: Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule?

A: No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at 45 CFR 164.504(e).

Q: Are accreditation organizations business associates of the covered entities they accredit?

A: Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of "business associate" at 45 CFR 160.103. Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See 45 CFR 164.514(e). If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

Q: Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

A: No. Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103. However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by Rule, that is, with an individual's authorization pursuant to 45 CFR 164.508, without an individual's authorization as permitted by 45 CFR 164.512(i), or as a limited data set provided that a data use agreement is in place as permitted by 45 CFR 164.514(e).

Q: When is a health care provider a business associate of another health care provider?

A: The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

Q: May a covered entity share protected health information directly with another covered entity's business associate?

A: Yes. If the HIPAA Privacy Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

Q: Are covered entities that engage in joint activities under an organized health care arrangement (OHCA) required to have business associate contracts with each other?

A: No. Covered entities that participate in an OHCA are permitted to share protected health information for the joint health care activities of the OHCA without entering into business associate contracts with each other. Of course, each such entity is independently required to observe its obligations under the HIPAA Privacy Rule with respect to

protected health information.

Q: Is a business associate contract required with organizations or persons where inadvertent contact with protected health information may result – such as in the case of janitorial services?

A: A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule. See 45 CFR 164.502(a)(1).

If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.

Q: Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

A: No, plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate". Under the HIPAA Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See the definition of "business associate" at 45 CFR 160.103.

Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See 45 CFR 164.502(a)(1).

Q. Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

A: No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

Q: Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?

A: The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard protected health information, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting, as provided for by 45 CFR 164.524, 164.526, and 164.528. With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must make such protected health information available if and when needed by the covered entity to provide an individual with access to the information. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the designated record set, or part thereof.

Under 45 CFR 164.526, a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must amend protected health information in such records (or copies) when requested by the covered entity. The covered entity itself is responsible for addressing requests from individuals

for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

Under 45 CFR 164.528, the Privacy Rule requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.

Q: Would a business associate contract in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's business associate contract requirements?

A: Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including business associate contracts, to qualify as written documents for purposes of meeting the Rule's requirements. However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

Q: Do physicians with hospital privileges have to enter into business associate contracts with the hospital?

A: No. The hospital and such physicians participate in what the HIPAA Privacy Rule defines as an organized health care arrangement (OHCA). Thus, they may use and disclose protected health information for the joint health care activities of the OHCA without entering into a business associate agreement.

Q: Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data?

A: Yes. See 45 CFR 164.514(e)(3)(ii). For example, if a researcher needs county data, but the covered entity's data contains only the postal address of the individual, a business associate may be used to convert the covered entity's geographical information into that needed by the researcher. In addition, the covered entity may hire the intended recipient of the limited data set as the business associate for this purpose in accordance with the

business associate requirements. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the recipient's request. However, the data recipient, as a business associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data use agreement and business associate contract?

A: Yes. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the covered entity is providing the recipient with protected health information that includes direct identifiers, a business associate agreement would be required in addition to the data use agreement to protect the information. For example, the agreement must require that the recipient agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Q: If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

A: No. Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement. For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.

Q: Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

A: A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered

entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

Q: Is a physician or other provider considered to be a business associate of a health plan or other payer?

A: Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "business associate" at 45 CFR 160.103.

Q: Is a health insurance issuer or HMO who provides health insurance or health coverage to a group health plan a business associate of the group health plan?

A: A health insurance issuer or HMO does not become a business associate simply by providing health insurance or health coverage to a group health plan. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an organized health care arrangement (OHCA), with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA. However, where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the joint activity of providing insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services.

Q: Is a reinsurer a business associate of a health plan?

A: Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.

Q: Is a software vendor a business associate of a covered entity?

A: The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity. For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate. See the definition of "workforce" at 45 CFR 160.103.

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

[*45 CFR 164.506*]

Background

The HIPAA Privacy Rule establishes a foundation of Federal protection for personal health information, carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care. As such, the Rule generally prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities.

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

How the Rule Works

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

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

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

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

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

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

- < Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- < Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- < Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- < Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- < Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- < Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

General Provisions at 45 CFR 164.506. A covered entity may, without the individual's authorization:

X Use or disclose protected health information for its own treatment, payment, and health care operations activities.

For example:

< A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.
< A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
< A health plan may use protected health information to provide customer service to its enrollees.

X A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule).

For example:

< A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
< A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred.

X A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information.

For example:

< A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.
< A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment services.

X A covered entity may disclose protected health information to another covered entity for certain health care operation activities of the entity that receives the

information if:

< Each entity either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship; and
< The disclosure is for a quality-related health care operations activity (i.e., the activities listed in paragraphs (1) and (2) of the definition of "health care operations" at 45 CFR 164.501) or for the purpose of health care fraud and abuse detection or compliance.

For example:

< A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.

X A covered entity that participates in an organized health care arrangement (OHCA) may disclose protected health information about an individual to another covered entity that participates in the OHCA for any joint health care operations of the OHCA.

For example:

< The physicians with staff privileges at a hospital may participate in the hospital's training of medical students.

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

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

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

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

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

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

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

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

Frequently Asked Questions

Q: My State requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection?

A: No. The Privacy Rule does not prohibit a covered entity from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with State law requirements.

Q: How does the HIPAA Privacy Rule change the laws concerning consent for treatment?

A: The Privacy Rule relates to uses and disclosures of protected health information, not to whether a patient consents to the health care itself. As such, the Privacy Rule does not affect informed consent for treatment, which is addressed by State law.

Q: Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?

A: Yes. The pharmacist is using the protected health information for treatment purposes, and the HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

Q: Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?

A: Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

Q: Are health care providers restricted from consulting with other providers about a patient's condition without the patient's written authorization?

A: No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule's definition of "treatment" and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected

health information about an individual to a health care provider for that provider's treatment of the individual. See 45 CFR 164.506.

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

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

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

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

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

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

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

providing an authorization.

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

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

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

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

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

A: No. The Privacy Rule's definition of "payment" includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following protected health information about the individual: name and address; date of birth; social security number; payment history; and account number. In addition, disclosure of the name and address of the health care provider or health plan making the report is allowed. The covered entity may perform this payment activity directly, or may carry out this function through a third party, such as a collection agency, under a business associate arrangement.

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

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

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

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

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

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

Q: Does the HIPAA Privacy Rule permit an eye doctor to confirm a contact prescription received by a mail-order contact company?

A: Yes. The disclosure of protected health information by an eye doctor to a distributor of contact lenses for the purpose of confirming a contact lens prescription is a treatment

disclosure, and is permitted under the Privacy Rule at 45 CFR 164.506.

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

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

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

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

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

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

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

A: The Privacy Rule permits a covered health care provider to disclose information for "health care operations" purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within "business management and general administrative activities" under the definition

of "health care operations." Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes. See 45 CFR 164.502(a)(1)(ii) and the definition of "health care operations" at 45 CFR 164.501.

MARKETING

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

Background

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

How the Rule Works

The Privacy Rule addresses the use and disclosure of protected health information for marketing purposes by:

- Defining what is "marketing" under the Rule;
- Excepting from that definition certain treatment or health care operations activities;
- Requiring individual authorization for all uses or disclosures of protected health information for marketing purposes with limited exceptions.

What is "Marketing"? The Privacy Rule defines "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Generally, if the communication is "marketing," then the communication can occur only if the covered entity first obtains an individual's "authorization." This definition of marketing has certain exceptions, as discussed below.

Examples of "marketing" communications requiring prior authorization are:

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

What Else is "Marketing"? Marketing also means: "An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to

the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service." This part of the definition to marketing has no exceptions. The individual must authorize these marketing communications before they can occur.

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

For example, it is "marketing" when:

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

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

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

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

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

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

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

< A hospital uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray

machine or magnetic resonance image machine) through a general mailing or publication.

< A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.

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

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

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

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

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

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

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

Marketing Authorizations and When Authorizations are NOT Necessary. Except as discussed below, any communication that meets the definition of marketing is not permitted, unless the covered entity obtains an individual's authorization. To determine what constitutes an acceptable "authorization," see 45 CFR 164.508. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. See 45 CFR 164.508(a)(3).

A communication does not require an authorization, even if it is marketing, if it is in the

form of a face-to-face communication made by a covered entity to an individual; or a promotional gift of nominal value provided by the covered entity.

For example, no prior authorization is necessary when:

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

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

MARKETING

Frequently Asked Questions

Q: Does the HIPAA Privacy Rule expand the ability of providers, plans, marketers and others to use my protected health information 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 Privacy Rule's limitations on the use or disclosure of protected health information for marketing purposes do not exist in most States today. For example, the Rule requires patients' authorization for the following types of uses or disclosures of protected health information for marketing:

- Selling protected health information to third parties for their use and re-use. Thus, under the Rule, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines without an authorization.

- Disclosing protected health information 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 without an authorization.

Without these Privacy Rule restrictions, these activities could occur with no authorization from the individual in most jurisdictions. In addition, if a State law provided additional limitations on disclosures of information for related activities, the Privacy Rule generally would not interfere with those laws.

Moreover, under the "business associate" provisions of the Privacy Rule, a covered entity may not give protected health information to a telemarketer, door-to-door salesperson, or other third party it has hired to make permitted communications (for example, about a covered entities' own goods and services) unless that third party has agreed by contract to use the information only for communicating on behalf of the covered entity. Without the Privacy Rule, there may be no restrictions on how third parties re-use information they obtain from health plans and providers. See the fact sheet and frequently asked questions on this web site about the business associate standard for more information.

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

A: No. While covered entities may share protected health information with their contractors who meet the definition of "business associates" under the HIPAA Privacy Rule, that

definition is limited to contractors that obtain protected health information to perform or assist in the performance of certain health care operations *on behalf of* covered entities. Thus, business associates, with limited exceptions, cannot use protected health information for their own purposes. Although, under the HIPAA statute, the Privacy Rule cannot govern contractors directly, the Rule does set clear parameters for how covered entities may contract with business associates. See 45 CFR 164.502(e) and 164.504(e), and the definition of "business associate" at 45 CFR 160.103.

Further, the Privacy Rule expressly prohibits health plans and covered health care providers from selling protected health information to third parties for the third party's own marketing activities, without authorization. So, for example, a pharmacist cannot, without patient authorization, sell a list of patients to a pharmaceutical company, for the pharmaceutical company to market its own products to the individuals on the list.

Q: Can telemarketers gain access to protected health information and call individuals to sell goods and services?

A: Under the HIPAA Privacy Rule, a covered entity can share protected health information with a telemarketer only if the covered entity has either obtained the individual's prior written authorization to do so, or has entered into a business associate relationship with the telemarketer for the purpose of making a communication that is not marketing, such as to inform individuals about the covered entity's own goods or services.

If the telemarketer is a business associate under the Privacy Rule, it must agree by contract to use the information only for communicating on behalf of the covered entity, and not to market its own goods or services (or those of another third party).

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

A: The HIPAA Privacy Rule expressly requires an authorization for uses or disclosures of protected health information for ALL marketing communications, except in two circumstances: (1) when the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value.

If the marketing communication involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

Q: How can I distinguish between activities for treatment or health care operations versus marketing activities?

A: The overlap among common usages of the terms "treatment," "healthcare operations," and "marketing" is unavoidable. For instance, in recommending treatments, providers and health plans sometimes advise patients to purchase goods and services. Similarly, when a health plan explains to its members the benefits it provides, it too is encouraging the use or purchase of goods and services.

The HIPAA Privacy Rule defines these terms specifically, so they can be distinguished. For example, the Privacy Rule excludes treatment communications and certain health care operations activities from the definition of "marketing." If a communication falls under one of the definition's exceptions, the marketing rules do not apply. In these cases, covered entities may engage in the activity without first obtaining an authorization. See the fact sheet on this web site about marketing, as well as the definition of "marketing" at 45 CFR 164.501, for more information.

However, if a health care operation communication does not fall within one of these specific exceptions to the marketing definition, and the communication falls under the definition of "marketing," the Privacy Rule's provisions restricting the use or disclosure of protected health information for marketing purposes will apply. For these marketing communications, the individual's authorization is required before a covered entity may use or disclose protected health information.

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

A: Generally, no. To the extent the disease management or wellness program is operated by the covered entity directly or by a business associate, communications about such programs are not marketing because they are about the covered entity's own health-related services. So, for example, a hospital's Wellness Department could start a weight-loss program and send a flyer to all patients seen in the hospital over the past year who meet the definition of obese, even if those individuals were not specifically seen for obesity when they were in the hospital.

Moreover, a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the definition of "marketing." Such communications may include population-based activities in the areas of health education or disease prevention. Examples of general health promotional material include mailings reminding women to get an annual mammogram; mailings providing information about how to lower cholesterol, new developments in health care (e.g., new diagnostic tools), support groups, organ donation, cancer prevention, and health fairs.

Q: Is it "marketing" for a covered entity to describe products or services that are

provided by the covered entity to its patients, or to describe products or services that are included in the health plan's plan of benefits to members of the health plan?

A: No. The HIPAA Privacy Rule excludes from the definition of "marketing" communications made to describe a covered entity's health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication. Thus, it would not be marketing for a physician who has developed a new anti-snore device to send a flyer describing it to all of her patients (whether or not each patient has actually sought treatment for snoring). Nor would it be marketing for an ophthalmologist or health plan to send existing patients or members discounts for eye-exams or eye-glasses available only to the patients and members. Similarly, it would not be marketing for an insurance plan to send its members a description of covered benefits, payment schedules, and claims procedures.

Q: Is it marketing for a covered entity to describe the entities participating in a health care provider network or a health plan network?

A: No. The HIPAA Privacy Rule excludes from the definition of "marketing," communications by a covered entity to describe the entities participating in a health care provider network or a health plan network. Thus, it would not be marketing for a health plan or insurer to mail its members or enrollees a list of health care providers in the health plan network or for an independent physicians association to send its patients a preferred provider list.

Q: Is it marketing for an insurance plan or health plan to send enrollees notices about changes, replacements, or improvements to existing plans?

A: No. The HIPAA Privacy Rule excludes from the definition of "marketing," communications about replacements of, or enhancements to, a health plan. Therefore, notices about changes in deductibles, co-pays and types of coverage, such as prescription drugs, are not marketing. Likewise, a notice to a family warning that a student reaching the age of majority on a parental policy will lose coverage, then offering continuation coverage, would not be considered marketing. Nor are special health care policies such as guaranteed issue products and conversion policies considered marketing. Similarly, notices from a health plan about its long term care benefits would not be considered marketing.

It would be considered marketing, however, for a health plan to send to its members promotional material about insurance products that are considered to be "excepted benefits" (described in section 2791(c)(1) of the Public Health Service Act), such as accident only policies. It would likewise be marketing for health plans to describe other

lines of insurance, such as life insurance policies. Generally, such communications require authorizations.

Q: Can health plans communicate about health-related products or services to enrollees that add value to, but are not part of, a plan of benefits?

A: Yes. The provision of value-added items or services (VAIS) is a common practice, particularly for managed care organizations. Under the HIPAA Privacy Rule, communications may qualify under the marketing exception for a communication about a health plan's plan of benefits, even if the VAIS are not considered plan benefits for the Adjusted Community Rate purposes. To qualify for this exclusion, however, the VAIS must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare + Choice or other managed care organizations for eyeglasses may be considered part of the plan's benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably "add value" to the plan's membership and not merely be a pass-through of a discount or item available to the public at large.

So, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for eyeglasses and contact lenses without obtaining authorizations if the discount were only available through membership in the managed care organization. However, such communications would need an authorization if the members would be able to obtain such discounts directly from the eyeglass store. Similarly, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for a prescription drug card benefit or for a health/fitness club membership, which is not available to consumers on the open market. On the other hand, a Medicare+Choice or other managed care organization would need an authorization to notify its members of a discount to a movie theater available only to its members.

Q: Can a doctor or pharmacy be paid to make a prescription refill reminder without a prior authorization under the HIPAA Privacy Rule?

A: Yes. It is not marketing for a doctor to make a prescription refill reminder even if a third party pays for the communication. The prescription refill reminder is considered treatment. The communication is therefore excluded from the definition of marketing and does not require a prior authorization. Similarly, it is not marketing when a doctor or pharmacy is paid by a pharmaceutical company to recommend an alternative medication to patients. Communications about alternative treatments are excluded from the definition of marketing and do not require a prior authorization. The simple receipt of remuneration does not transform a treatment communication into a commercial promotion of a product or service.

Furthermore, covered entities may use a legitimate business associate to assist them in making such permissible communications. For instance, if a pharmacist that has been paid by a third party contracts with a mail house to send out prescription refill reminders to the pharmacist's patients, neither the mail house nor the pharmacist needs a prior authorization. However, a covered entity would require an authorization if it sold protected health information to a third party for the third party's marketing purposes.

Q: Are appointment reminders allowed under the HIPAA Privacy Rule without authorizations?

A: Yes, appointment reminders are considered part of treatment of an individual and, therefore, can be made without an authorization.

Q: What are examples of "alternative treatments" that are excepted from the HIPAA Privacy Rule's definition of "marketing"?

A: Alternative treatments are treatments that are within the range of treatment options available to an individual. For example, it would be an alternative treatment communication if a doctor, in response to an inquiry from a patient with skin rash about the range of treatment options, mails the patient a letter recommending that the patient purchase various ointments and medications described in brochures enclosed with the letter. Alternative treatment could also include alternative medicine. Thus, alternative treatments would include communications by a nurse midwife who recommends or sells vitamins and herbal preparations, dietary and exercise programs, massage services, music or other alternative types of therapy to her pregnant patients.

Q: Are prior authorizations required when a doctor or health plan distributes promotional gifts of nominal value?

A: No. In a specific exception, the HIPAA Privacy Rule allows covered entities to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services. This authorization exception generally applies to items and services of a third party, whether or not they are health-related, or items and services of the covered entity that are not health-related. A covered doctor, for instance, may send patients items such as pens, note-pads, and cups embossed with a health plan's logo without prior authorization. Similarly, dentists may give patients free toothbrushes, floss and toothpaste.

Q: Are health care providers required to seek a prior authorization before discussing a product or service with a patient, or giving a product or service to a patient, in a

face-to-face encounter?

A: No. In face-to-face encounters, the HIPAA Privacy Rule allows covered entities to give or discuss products or services, even when not health-related, to patients without a prior authorization. This exception prevents unnecessary intrusion into the doctor-patient relationship. Physicians may give out free pharmaceutical samples, regardless of their value. Similarly, hospitals may give infant supplies to new mothers. Moreover, the face-to-face exception would allow providers to leave general circulation materials in their offices for patients to pick up during office visits.

Q: Must insurance agents that are business associates of a health plan seek a prior authorization before talking to a customer in a face-to-face encounter about the insurance company's other lines of business?

A: No. In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals.

Q: What effect do the "marketing" provisions of the HIPAA Privacy Rule have on Federal or State fraud and abuse statutes?

A: The Privacy Rule makes it clear that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other Federal or State statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. Examples of such laws include the anti-kickback statute (section 1128B(b) of the Social Security Act), safe harbor regulations (42 CFR Parts 411 and 424), and HIPAA statute on self-referral (section 1128C of the Social Security Act). The definition of "marketing" is applicable solely to the Privacy Rule and the permissions granted by the Rule are only for a covered entity's use or disclosure of protected health information. In particular, although the Privacy Rule defines the term "marketing" to exclude communications to an individual to recommend, purchase, or use a product or service as part of the treatment of the individual or for case management or care coordination of that individual, such communication by a health care professional may violate the anti-kickback statute. Similar examples of pharmacist communications with patients relating to the marketing of products on behalf of pharmaceutical companies were identified by the Office of the Inspector General (OIG) as problematic in a 1994 Special Fraud Alert (December 19, 1994, 59 FR 65372). Other violations have involved home health nurses and physical therapists acting as marketers for durable medical equipment companies. Although a particular communication under the Privacy Rule may not require patient authorization because it is not "marketing," or may require patient authorization because it is

"marketing" as the Rule defines it, the arrangement may nevertheless violate other statutes and regulations administered by the Department of Health and Human Services, Department of Justice, or other Federal or State agencies.

Q: May covered entities use information regarding specific clinical conditions of individuals in order to communicate about products or services for such conditions without a prior authorization?

A: Yes, if the communication is for the individual's treatment or for case management, care coordination, or the recommendation of alternative therapies. The HIPAA Privacy Rule permits the use of clinical information to the extent it is reasonably necessary for these communications. Similarly, population-based activities in the areas of health education or disease prevention are not considered marketing when they promote health in a general manner. Again clinical information may be used for such communications, such as in targeting a public education campaign.

Q: Are communications concerning information to beneficiaries about government programs or government-sponsored programs "marketing" under the HIPAA Privacy Rule?

A: No. Communications about government and government-sponsored programs do not fall within the definition of "marketing." There is no commercial component to communications about benefits available through public programs. Therefore, a covered entity is permitted to use and disclose protected health information to communicate about eligibility for such programs as Medicare, Medicaid, or the State Children's Health Insurance Program (SCHIP).

DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES

[*45 CFR 164.512(b)*]

Background

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

How the Rule Works

General Public Health Activities. The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i). Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority. See 45 CFR 164.512(b)(1)(i). Covered entities who are also a public health authority may use, as well as disclose, protected health information for these public health purposes. See 45 CFR 164.512(b)(2).

A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. See 45 CFR 164.502(b). For disclosures to a public health authority, covered entities may reasonably rely on a minimum necessary determination made by the public health authority in requesting the protected health information. See 45 CFR 164.514(d)(3)(iii)(A). For routine and recurring

public health disclosures, covered entities may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of protected health information that may be disclosed for such purposes. See 45 CFR 164.514(d)(3)(i).

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

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

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

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

  See 45 CFR 164.512(b)(1)(iii). The "person" subject to the jurisdiction of the FDA does not have to be a specific individual. Rather, it can be an individual or an entity, such as a partnership, corporation, or association. Covered entities may identify the party or parties responsible for an FDA-regulated product from the

product label, from written material that accompanies the product (know as labeling), or from sources of labeling, such as the Physician's Desk Reference.

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

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

DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES

Frequently Asked Questions

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 HIPAA Privacy Rule permits 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 protected health information 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 (including dietary supplements), drugs, biological products, and medical devices. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Q: Does the public health provision of the HIPAA Privacy Rule require covered entities to make public health disclosures?

A: No. The Privacy Rule's public health provision permits, but does not require, covered entities to make such disclosures. This provision is intended to allow covered entities to continue current voluntary reporting practices that are critically important to public health and safety. The Rule also permits covered entities to disclose protected health information when State or other law requires covered entities to make disclosures for public health purposes. For instance, many State laws require health care providers to report certain diseases, cases of child abuse, births, or deaths, and the Privacy Rule permits covered entities to disclose protected health information, without authorization, to make such reports. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Q: May covered entities disclose facially identifiable protected health information, such as name, address, and social security number, for public health purposes?

A: Yes. The HIPAA Privacy Rule permits covered entities to disclose the amount and type of protected health information that is needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to 45 CFR 164.512(a) of the Rule. For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure. For routine or recurring public health disclosures, a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes. Covered entities may also rely on the requesting public health authority's determination of the minimally necessary information. See the fact sheet and frequently asked questions on this web site about the public health and minimum necessary standards for more information.

Q: Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information to authorities such as the National Institutes of Health (NIH)?

A: The definition of a "public health authority" requires that an agency's official mandate include the responsibility for public health matters. The mandate can be responsibility for public health matters, generally, or it can be for specific public health programs. Furthermore, an agency's official mandate does not have to be exclusively or primarily for public health. Therefore, to the extent a government agency has public health matters as part of its official mandate, it qualifies as a public health authority. For instance, various Department of Health and Human Service agencies, such as NIH and the Health Resources and Services Administration (HRSA), are authorized by law to assist the Secretary of Health and Human Services in carrying out the purposes of section 301 of the Public Health Service Act. Those agencies are public health authorities under the Rule, even if they have other non-public health mandates. To the extent a public health authority is authorized by law to collect or receive information for the public health purposes specified in the public health provision, covered entities may disclose protected health information to such public health authorities without authorization pursuant to the public health provision. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Q: To whom may covered entities make public health disclosures regarding a product regulated by the Food and Drug Administration (FDA) when more than one person is identified on the product label?

A: Covered entities may identify persons responsible for an FDA-regulated product by using the product label, the literature that accompanies the product, or other sources of labeling,

such as the Physician's Desk Reference. If multiple persons are named, covered entities may choose any of the persons named by these sources. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Q: Is a covered entity permitted to disclose protected health information under the HIPAA Privacy Rule's public health provision when the link between an adverse event and a product regulated by the Food and Drug Administration (FDA) is only suspected?

A: Yes. In most instances when a covered entity makes an adverse event report to a person responsible for an FDA-regulated product, the covered entity will suspect, but not know, the product is the cause of the event. Determining whether the product is related to the adverse event almost always requires follow up with the covered entity which in turn may need further contact with the patient. FDA and product manufacturers receive a great deal of important information about the safety of regulated products from these reports. To limit such reports to those instances where the covered entity is convinced of the link between the product and the event would reduce the amount of useful safety, quality and effectiveness data available to the agency as well as to product manufacturers. This would limit significantly FDA's ability to protect the public health by helping to assure that only safe and effective products are marketed in the U.S. Accordingly, covered entities may disclose the minimum amount of protected health information that is reasonably necessary to report suspected adverse events associated with an FDA-regulated product. See the fact sheet and frequently asked questions on this web site about the public health and minimum necessary standards for more information.

Q: Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information without authorization to a manufacturer of a product regulated by the Food and Drug Administration (FDA) for use by the manufacturer to assess the effectiveness of its marketing campaign?

A: No. The public health provision is intended to facilitate the flow of information that is essential to the FDA's public health mission. The provision does not permit covered entities to disclose protected health information to a manufacturer for the manufacturer's commercial purposes, or for any other non-public health purpose. For example, the Rule does not permit a covered entity to provide a drug manufacturer with a list of persons who prefer a different flavored cough syrup over the flavor of the manufacturer's product. Rather, this provision permits covered entities to disclose protected health information as necessary to continue current voluntary reporting of adverse events and similar reports that are necessary to ensure the quality, safety, or effectiveness of an FDA-regulated product. For instance, a covered entity would be permitted to report a concern to a drug manufacturer that its cough syrup might be unsafe based on the belief that a difference in the taste could be due to drug tampering or a manufacturing problem. Likewise, a

covered health care provider would be permitted to disclose protected health information to a drug manufacturer to report that the failure of a patient's medical condition to improve may be due to the drug's ineffectiveness. In making such a report, the covered entity may disclose the protected health information that is reasonably necessary to achieve the purpose of the report. See the fact sheet and frequently asked questions on this web site about the public health and minimum necessary standards for more information.

Q: Does the HIPAA Privacy Rule's public health provision permit covered health care providers to disclose protected health information concerning the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations to an individual's employer?

A: The public health provision permits covered health care providers to disclose an individual's protected health information to the individual's employer without authorization in very limited circumstances. First, the covered health care provider must provide the health care service to the individual at the request of the individual's employer or as a member of the employer's workforce. Second, the health care service provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. Third, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information. For example, OSHA requires employers to monitor employees' exposures to certain substances and to take specific actions when an employee's exposure level exceeds a specified limit. A covered entity which tests an individual for such an exposure level at the request of the individual's employer may disclose that test result to the employer without authorization.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the protected health information the employer needs to meet such legal obligation may be disclosed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there).

When a health care service does not meet the above requirements, covered entities may not disclose an individual's protected health information to the individual's employer without an authorization, unless the disclosure is otherwise permitted without authorization by other provisions of the Rule. However, nothing in the Rule prohibits an

employer from conditioning employment on an individual providing an authorization for the disclosure of such information.

RESEARCH

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

Background

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

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

How the Rule Works

In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule.

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

- Documented Institutional Review Board (IRB) or Privacy Board Approval.

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

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

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

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

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

health information would be permitted by this subpart;

< The research could not practicably be conducted without the waiver or alteration; and

< The research could not practicably be conducted without access to and use of the protected health information.

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

• Research on Protected Health Information of Decedents. Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, *and*, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).

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

< Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;

< Limit who can use or receive the data; and

< Require the recipient to agree to the following:

S Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;

S Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;

S Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which

the recipient becomes aware;

- Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
- Not to identify the information or contact the individual.

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

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

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

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

Accounting for Research Disclosures. In general, the Privacy Rule gives individuals the right to receive an accounting of certain disclosures of protected health information made by a covered entity. See 45 CFR 164.528. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose. See 45 CFR 164.528(b)(3). Among the types of disclosures that are exempt from this accounting requirement are:

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

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

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

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

- An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
- The informed consent of the individual to participate in the research; or
- A waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA's human subject protection regulations at 21 CFR 50.24.

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

The Privacy Rule allows covered entities to rely on such express legal permission, informed consent, or IRB-approved waiver of informed consent, which they create or receive before the applicable compliance date, to use and disclose protected health information for specific research studies, as well as for future unspecified research that may be included in such permission.

RESEARCH

Frequently Asked Questions

Q: Will the HIPAA Privacy Rule hinder medical research by making doctors and others less willing and/or able to share with researchers 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 authorize disclosures of their information for research and to participate in research when they know their information is protected. For example, in genetic studies conducted at the National Institutes of Health, nearly 32 percent of eligible people offered a test for breast cancer risk declined 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 protected health information. We believe few providers will take this route, however, because the Common Rule includes similar, and more rigorous requirements, that have not impaired the willingness of researchers to undertake Federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires an Institutional Review Board (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 protected health information for research purposes is to be altered or waived. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.

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

A: Under the HIPAA 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. 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. Nonetheless, the Department will consider issuing guidance as necessary and appropriate to address concerns that may arise during implementation of these provisions. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.

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

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 HIPAA Privacy Rule permit the creation of a database for research purposes through an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization?

A: Yes. A covered entity may use or disclose protected health information 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. Protected health information maintained by a covered entity 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. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: Can researchers continue to access existing databanks or repositories that are maintained by covered entities, even if those databases were created prior to the compliance date without patient permission or without a waiver of informed consent by an Institutional Review Board (IRB)?

A: Yes. Under the HIPAA Privacy Rule, covered entities may use or disclose protected

health information from existing databases or repositories for research purposes either with individual authorization as required at 45 CFR 164.508, or with a waiver of individual authorization as permitted at 45 CFR 164.512(i). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review Boards.

Q: How does the Rule help Institutional Review Boards (IRB) handle the additional responsibilities imposed by the HIPAA 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. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

In addition, the Rule allows an IRB to use expedited review procedures as permitted by the Common Rule to review and approve requests for waiver of authorizations. Similarly, the Rule permits Privacy Boards to use an expedited review process when the research involves no more than a minimal privacy risk to the individuals. An expedited review process permits covered entities to accept documentation of waiver of authorization when only one or more members of the IRB or Privacy Board have conducted the review. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.

Q: By establishing new waiver criteria and authorization requirements, hasn't the HIPAA 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 protected health information for research purposes. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.

Q: Is documentation of Institutional Review Board (IRB) *and* Privacy Board approval required by the HIPAA Privacy Rule before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization?

A: No. The HIPAA Privacy Rule requires documentation of waiver approval by either an

IRB *or* a Privacy Board, not both. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: Does the HIPAA Privacy Rule require a covered entity to create an Institutional Review Board (IRB) or Privacy Board before using or disclosing protected health information 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. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: What does the HIPAA 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 by a covered entity or its business associate 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. While it may be unlikely that a researcher would be maintaining a designated record set, any research records or results that are actually maintained by the covered entity as part of a designated record set would be accessible to research participants unless one of the Privacy Rule's permitted exceptions applies.

One of the permitted exceptions applies to protected health information 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 protected health information will be reinstated at the conclusion of the clinical trial.

Q: Are the HIPAA 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 protected health information 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 protected health information because doing so may result in the research laboratory losing its CLIA exemption.

Q: Do the HIPAA 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 is for the use and disclosure of protected health information for research purposes. In contrast, an individual's informed consent, as required by the Common Rule and the Food and Drug Administration's (FDA) 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 protected health information. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule. 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. However, the Privacy Rule's authorization elements are compatible with the Common Rule's informed consent elements. Thus, both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule. For example, the Privacy Rule allows the research authorization to state that the authorization will be valid until the conclusion of the research study, or to state that the authorization will not have an expiration date or event. This is compatible with the Common Rule's requirement for an explanation of the expected duration of the research subject's participation in the study. It should be noted that 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.

Q: When is a researcher a covered health care provider under HIPAA?

A: A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102, 160.103. For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide

health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf. For further assistance in determining covered entity status, see the "decision tool" at www.hhs.gov/ocr/hipaa/.

Q: When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule?

A: A covered entity that qualifies as a hybrid entity, meaning that the entity is a single legal entity that performs both covered and non-covered functions, may choose whether it wants to be a hybrid entity. If such a covered entity decides not to be a hybrid entity then it, and all of its components, are subject to the Privacy Rule in its entirety. Therefore, if a researcher is an employee or workforce member of a covered entity that has decided not to be a hybrid entity, the researcher is part of the covered entity and is, therefore, subject to the Privacy Rule.

If a covered entity decides to be a hybrid entity, it must define and designate as its health care component(s) those parts of the entity that engage in covered functions. "Covered functions" are those functions of a covered entity that make the entity a health plan, a health care provider, or a health care clearinghouse. Thus, research components of a hybrid entity that function as health care providers and engage in standard electronic transactions must be included in the hybrid entity's health care component(s), and be subject to the Privacy Rule.

However, research components that function as health care providers, but do not engage in standard electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity's health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are not subject to the Privacy Rule.

Q: If a research subject revokes his or her authorization to have protected health information used or disclosed for research, does the HIPAA Privacy Rule permit a researcher/covered health care provider to continue using the protected health information already obtained prior to the time the individual revoked his or her authorization?

A: Covered entities may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. An individual may not revoke an authorization to the extent the covered entity has acted in reliance on the authorization. For research uses and disclosures, this reliance exception at 45 CFR 164.508(b)(5)(i) permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. For example, the reliance exception would permit the continued use and disclosure of protected health information to account for a subject's withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the Food and Drug Administration, to conduct investigations of scientific misconduct, or to report adverse events.

However, the reliance exception would not permit a covered entity to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization.

Q: Can the preparatory research provision of the HIPAA Privacy Rule at 45 CFR 164.512(i)(1)(ii) be used to recruit individuals into a research study?

A: The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. See 45 CFR 164.502(a)(1)(i). Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.
However, a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board as permitted at 45 CFR164.512(i)(1)(i). The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes

of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.

Q: Does the HIPAA Privacy Rule require documentation of Institutional Review Board (IRB) or Privacy Board approval of an alteration or waiver of individual authorization before a covered entity may use or disclose protected health information for any of the following provisions: (1) for preparatory research at 45 CFR 164.512(i)(1)(ii), (2) for research on the protected health information of decedents at 45 CFR 164.512(i)(1)(iii), or (3) a limited data set with a data use agreement as stipulated at 45 CFR 164.514(e)?

A: No. Documentation of IRB or Privacy Board approval of an alteration or waiver of individual authorization is only needed before a covered entity may use or disclose protected health information under 45 CFR 164.512(i)(1)(i). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: If research subjects' consent was obtained before the compliance date, but the Institutional Review Board (IRB) subsequently modifies the informed consent document after the compliance date and requires that subjects be reconsented, is authorization now required from these previously enrolled research subjects under the HIPAA Privacy Rule?

A: Yes. If informed consent or reconsent (ie., asked to sign a revised consent or another informed consent) is obtained from research subjects after the compliance date, the covered entity must obtain individual authorization as required at 45 CFR 164.508 for the use or disclosure of protected health information once the consent obtained before the compliance date is no longer valid for the research. The revised informed consent document may be combined with the authorization elements required by 45 CFR 164.508. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review Boards.

Q: Can covered entities continue to disclose adverse event reports that contain protected health information to the Department of Health and Human Services (HHS) Office for Human Research Protections?

A: Yes. The Office for Human Research Protections is a public health authority under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to report adverse events to the Office for Human Research Protections

either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for public health activities as permitted at 45 CFR 164.512(b).

Q: Can covered entities continue to disclose protected health information to the HHS Office for Human Research Protections for purposes of determining compliance with the HHS regulations for the protection of human subjects (45 CFR Part 46)?

A: Yes. The Office for Human Research Protections is a health oversight agency under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to the Office for Human Research Protections for such compliance investigations either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for health oversight activities as permitted at 45 CFR 164.512(d).

DISCLOSURES FOR WORKERS' COMPENSATION PURPOSES

[*45 CFR 164.512(l)*]

Background

The HIPAA Privacy Rule does not apply to entities that are either workers' compensation insurers, workers' compensation administrative agencies, or employers, except to the extent they may otherwise be covered entities. However, these entities need access to the health information of individuals who are injured on the job or who have a work-related illness to process or adjudicate claims, or to coordinate care under workers' compensation systems. Generally, this health information is obtained from health care providers who treat these individuals and who may be covered by the Privacy Rule. The Privacy Rule recognizes the legitimate need of insurers and other entities involved in the workers' compensation systems to have access to individuals' health information as authorized by State or other law. Due to the significant variability among such laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes in a number of different ways.

How the Rule Works

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

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

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

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

Disclosures With Individual Authorization. In addition, covered entities may disclose protected health information to workers' compensation insurers and others involved in workers' compensation systems where the individual has provided his or her authorization for the release

of the information to the entity. The authorization must contain the elements and otherwise meet the requirements specified at 45 CFR 164.508.

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

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

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

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

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

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

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

DISCLOSURES FOR WORKERS' COMPENSATION PURPOSES

Frequently Asked Questions

Q: Won't the HIPAA Privacy Rule's minimum necessary standard impede the ability of workers' compensation insurers, State administrative agencies, and employers to obtain the health information needed to pay injured or ill workers the benefits guaranteed them under the State workers' compensation system?

A: No. The Privacy Rule is not intended to impede the flow of health information to those who need it to process or adjudicate claims, or coordinate care, for injured or ill workers under workers' compensation systems. The minimum necessary standard generally requires covered entities to make reasonable efforts to limit uses and disclosures of, as well as requests for, protected health information to the minimum necessary to accomplish the intended purpose. For disclosures of protected health information made for workers' compensation purposes under 45 CFR 164.512(*l*), the minimum necessary standard permits covered entities to disclose information to the full extent authorized by State or other law. In addition, where protected health information is requested by a State workers' compensation or other public official for such purposes, covered entities are permitted reasonably to rely on the official's representations that the information requested is the minimum necessary for the intended purpose. See 45 CFR 164.514(d)(3)(iii)(A).

For disclosures of protected health information for payment purposes, covered entities may disclose the type and amount of information necessary to receive payment for any health care provided to an injured or ill worker.

The minimum necessary standard does not apply to disclosures that are required by State or other law or made pursuant to the individual's authorization.

Q: Does an individual have a right under the HIPAA Privacy Rule to restrict the protected health information his or her health care provider discloses for workers' compensation purposes?

A: Individuals do not have a right under the Privacy Rule at 45 CFR 164.522(a) to request that a covered entity restrict a disclosure of protected health information about them for workers' compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers' compensation or similar law. See 45 CFR 164.522(a) and 164.512(a) and (*l*).

Q: Does the HIPAA Privacy Rule permit a health care provider to disclose an injured or ill worker's protected health information without his or her authorization when

requested for purposes of adjudicating the individual's workers' compensation claim?

A: Covered entities are permitted to disclose protected health information for such purposes as authorized by, and to the extent necessary to comply with, workers' compensation law. See 45 CFR 164.512(*l*). In addition, the Privacy Rule generally permits covered entities to disclose protected health information in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process. See 45 CFR 164.512(e).

Q: I am a health care provider and my State law says I have to provide a workers' compensation insurer, upon request, with an injured workers' records that relate to treatment or hospitalization for which compensation is being sought. Am I permitted to disclose the information required by my State law?

A: Yes. The HIPAA Privacy Rule permits a covered entity to disclose protected health information as necessary to comply with State law. No minimum necessary determination is required. See 45 CFR 164.512(a) and 164.502(b).

Q: My State law says I may disclose records, relating to the treatment I provided to an injured worker, to a workers' compensation insurer for purposes of determining the amount of or entitlement to payment under the workers' compensation system. Am I allowed to share this information under the HIPAA Privacy Rule?

A: Yes. A covered entity is permitted to disclose an individual's protected health information as necessary to comply with and to the full extent authorized by workers' compensation law. See 45 CFR 164.512(*l*).

Q: My State law says I may provide information regarding an injured workers' previous condition, which is not directly related to the claim for compensation, to an employer or insurer if I obtain the workers' written release. Am I permitted to make this disclosure under the HIPAA Privacy Rule?

A: A covered entity may disclose protected health information where the individual's written authorization has been obtained, consistent with the Privacy Rule's requirements at 45 CFR 164.508. Thus, a covered entity would be permitted to make the above disclosure if the individual signed such an authorization.

NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

[*45 CFR 164.520*]

Background

The HIPAA Privacy Rule gives individuals a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of these rights and practices. The notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health plans and health care providers and exercise their rights.

How the Rule Works

General Rule. The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices.

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

X Health care clearinghouses, if the only protected health information they create or receive is as a business associate of another covered entity. See 45 CFR 164.500(b)(1).

X A correctional institution that is a covered entity (e.g., that has a covered health care provider component).

X A group health plan that provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs, and that does not create or receive protected health information other than summary health information or enrollment or disenrollment information.

See 45 CFR 164.520(a).

Content of the Notice. Covered entities are required to provide a notice in *plain language* that describes:

X How the covered entity may use and disclose protected health information about

an individual.

X The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.

X The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.

X Whom individuals can contact for further information about the covered entity's privacy policies.

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

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

Providing the Notice.

X A covered entity must make its notice available to any person who asks for it.

X A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.

X *Health Plans* must also:

- < Provide the notice to individuals then covered by the plan no later than April 14, 2003 (April 14, 2004, for small health plans) and to new enrollees at the time of enrollment.
- < Provide a revised notice to individuals then covered by the plan within 60 days of a material revision.
- < Notify individuals then covered by the plan of the availability of and how to obtain the notice at least once every three years.

X *Covered Direct Treatment Providers* must also:

- < Provide the notice to the individual no later than the date of first service

delivery (after the April 14, 2003 compliance date of the Privacy Rule) and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.

< When first service delivery to an individual is provided over the Internet, through e-mail, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the individual's first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.

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

< Make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the provider's office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.

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

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

Organizational Options.

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

X Covered entities that participate in an organized health care arrangement may choose to produce a single, joint notice if certain requirements are met. For example, the joint notice must describe the covered entities and the service delivery sites to which it applies. If any one of the participating covered entities provides the joint notice to an individual, the notice distribution requirement with respect to that individual is met for all of the covered entities. See 45 CFR

164.520(d).

NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

Frequently Asked Questions

Q: Are hospitals or other health care providers required to provide their notices to patients they treat in an emergency?

A: Hospitals and other covered health care providers with a direct treatment relationship with individuals are not required to provide their notices to patients at the time they are providing emergency treatment. In these situations, the HIPAA Privacy Rule requires only that providers give patients a notice when it is practical to do so after the emergency situation has ended. In addition, where notice is delayed by an emergency treatment situation, the Privacy Rule does not require that providers make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice.

Q: If a health care provider chooses to obtain an individual's consent to use or disclose protected health information about them, does the provider also have to make a good faith effort to obtain the individual's acknowledgment of the notice?

A: Yes. The HIPAA Privacy Rule requires that a covered health care provider with a direct treatment relationship with individuals make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider's notice, regardless of whether the provider also chooses to obtain the individuals' consent. However, those providers that choose to obtain consent from individuals have discretion to design one form that includes both a consent and the acknowledgment of receipt of the notice.

Q: Can covered entities distribute their notices as part of other mailings or distributions?

A: Yes. The HIPAA Privacy Rule provides covered entities with discretion in this area; no special or separate mailings or distributions are required to satisfy the Privacy Rule's notice distribution requirements. Thus, a health plan distributing its notice through the mail, in accordance with 45 CFR 164.520(c)(1), may do so as part of another mailing to the individual (e.g., by including the notice with Summary Plan Descriptions). Similarly, a covered entity that e-mails its notice to an individual, in accordance with 45 CFR 164.520(c)(3), may include additional materials in the e-mail. No separate e-mail is required. However, the Privacy Rule continues to prohibit covered entities from combining the notice in a single document with an authorization form (see 45 CFR 164.508(b)(3)); and direct treatment providers, other than in emergency situations, must provide the notice at or before the date of first service delivery, and must make a good

faith effort to obtain the individual's written acknowledgment of receipt of the notice.

Q: Does the HIPAA Privacy Rule require a health care provider to obtain a new acknowledgment of receipt of the notice from patients if the facility changes its privacy policy?

A: No. A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgment of receipt of the notice only at the time the provider first gives the notice to the individual--that is, at first service delivery. See 45 CFR 164.520(c)(2).

Q: Does the HIPAA Privacy Rule permit health care providers to obtain an electronic acknowledgment of the notice from individuals?

A: Yes. For notice delivered electrically, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice. A provider who gives his paper notice to a patient during a face-to-face encounter with the individual at first service delivery may also obtain an electronic acknowledgment from the individual, provided that the individual's acknowledgment is in writing. Thus, a receptionist's notation in the provider's computer system of the individual's receipt of the notice would not be considered a valid written acknowledgment of the individual.

Q: Does the HIPAA Privacy Rule require a business associate to create a notice of privacy practices?

A: No. However, a covered entity must ensure through its contract with the business associate that the business associate's uses and disclosures of protected health information and other actions are consistent with the covered entity's privacy policies, as stated in covered entity's notice. Also, a covered entity may use a business associate to distribute its notice to individuals.

Q: Are covered entities permitted to give individuals a "layered" notice?

A: Yes. Covered entities may use a "layered" notice to implement the HIPAA Privacy Rule's requirements, so long as the elements required by 45 CFR 164.520(b) are included in the document that is provided to the individual. For example, a covered entity may satisfy the notice requirements by providing the individual with both a short notice that briefly summarizes the individual's rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all of the elements required by the Privacy Rule. Providing the notice in this fashion is a helpful tool to assure that more individuals will realize that important information is contained in the notice. In addition to ensuring the notice is in plain language (as required by the Privacy Rule), covered

entities are encouraged to develop notices that maximize readability and clarity.

Q: Are health plans required to make a good faith effort to obtain from their enrollees a written acknowledgment of receipt of the notice?

A: No. Under the HIPAA Privacy Rule, only covered health care providers that have a direct treatment relationship with individuals are required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice. See 45 CFR 164.520(c)(2)(ii).

Q: How are health care providers supposed to provide the notice to individuals and obtain their written acknowledgment of the notice when the first treatment encounter is over the phone or in some other manner that is not face-to-face?

A: The HIPAA Privacy Rule is intended to be flexible enough to address the various types of relationships that covered health care providers may have with the individuals they treat, including those treatment situations that are not face-to-face. For example, a health care provider who first treats a patient over the phone satisfies the notice provision requirements of the Privacy Rule by mailing the notice to the individual the same day, if possible. To satisfy the requirement that the provider also make a good faith effort to obtain the individual's acknowledgment of the notice, the provider may include a tear-off sheet or other document with the notice that requests that the acknowledgment be mailed back to the provider. The health care provider is not in violation of the Rule if the individual chooses not to mail back an acknowledgment; and a file copy of the form sent to the patient would be adequate documentation of the provider's good faith effort to obtain the acknowledgment.

Where a health care provider's initial contact with the patient is simply to schedule an appointment or a procedure, the notice provision and acknowledgment requirements may be satisfied at the time the individual arrives at the provider's facility for his or her appointment.

For service provided electronically, the notice must be sent electronically automatically and contemporaneously in response to the individual's first request for service. In this situation, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice.

Q: We participate in an organized health care arrangement (OHCA). How are we to comply with the HIPAA Privacy Rule's requirements for providing notices and obtaining individuals' acknowledgments of the notice?

A: Health care providers and other covered entities that participate in an organized health care arrangement (OHCA) may use a single, joint notice that covers all of the

participating covered entities (provided that the conditions at 45 CFR 164.520(d) are met), or may each maintain separate notices. Where a joint notice is provided to an individual by any one of the covered entities to which the joint notice applies, the Privacy Rule's requirements for providing the notice are satisfied for all others covered by the joint notice. If the joint notice is provided to an individual by a direct treatment provider participating in the OHCA, the provider must make a good faith effort to obtain the individual's written acknowledgment of receipt of the joint notice. Where the joint notice is provided to the individual by a participating covered entity other than a direct treatment provider, no acknowledgment need be obtained.

However, where covered entities participating in an OHCA choose to maintain separate notices, each covered entity from which an individual obtains services must provide its notice to the individual in accordance with the applicable requirements of 45 CFR 164.520(c). In addition, each direct treatment provider within the OHCA must make a good faith effort to obtain the individual's acknowledgment of the notice he or she provides.

Q: Does a health plan have to provide a copy of its notice to each dependent receiving coverage under a policy?

A: No. A health plan satisfies the HIPAA Privacy Rule's requirements for providing the notice by distributing its notice only to the named insured of a policy under which coverage is provided both to the named insured and his or her dependents. See 45 CFR 164.520(c)(1)(iii).

Q: For group health plan products, can the health plan send its notice to the administrator of the group product or the plan sponsor for them to distribute to each employee enrolled in the plan?

A: The HIPAA Privacy Rule requires a health plan to distribute its notice to each individual covered by the plan. Health plans may arrange to have another person or entity, for example, a group administrator or a plan sponsor, distribute the notice on their behalf. However, if the other person or entity fails to distribute the notice to the plan's enrollees, the health plan may be in violation of the Privacy Rule.

Q: As a pediatrician, am I required to give my notice of privacy practices to the children I treat?

A: The HIPAA Privacy Rule requires a covered health care provider with a direct treatment relationship with the individual to provide the notice to the individual receiving treatment no later than the date of first service delivery. In cases where the individual has a personal representative, as is generally the case when a parent brings a child in for

treatment, the provider satisfies the notice distribution requirements by providing the notice to the personal representative (e.g., the child's parent), and making a good faith effort to obtain the personal representative's acknowledgment of the notice. In the limited cases where the parent is not the personal representative of the unemancipated minor, such as when the minor is authorized under State law to consent to the treatment and does so, the provider must give its notice to the minor and make a good faith effort to obtain the minor's acknowledgment of the notice. See 45 CFR 164.502(g)(3) and 164.520(c)(2).

Q: Are health care providers required by the HIPAA Privacy Rule to post their entire notice at their facility or may they post just a brief description of the notice?

A: Covered health care providers that maintain an office or other physical site where they provide health care directly to individuals are required to post their entire notice at the facility in a clear and prominent location. The Privacy Rule, however, does not prescribe any specific format for the posted notice, just that it include the same information that is distributed directly to the individual. Covered health care providers have discretion to design the posted notice in a manner that works best for their facility, which may be to simply post a copy of the pages of the notice that is provided directly to individuals.

Q: Can a covered entity bypass obtaining an individual's authorization for a use or disclosure not permitted by the HIPAA Privacy Rule simply by informing individuals of the use or disclosure through its notice of privacy practices?

A: No. A covered entity's notice is not a substitute for an individual's authorization. Covered entities are required to obtain the individual's written authorization for any use or disclosure of protected health information not permitted or required by the Privacy Rule. See 45 CFR 164.508. Simply including in the notice a description of such a use or disclosure does not obviate the need for the covered entity to obtain the individual's prior written authorization, when that authorization is required by the Rule. Instead, the notice must reflect the uses and disclosures a covered entity may make without the individual's authorization, as permitted by Privacy Rule, as well as state that any other uses or disclosures only will be made with the individual's written authorization. See 45 CFR 164.520(b).

Q: Is our medical practice required to notify patients through the mail of any changes to our notice?

A: No. The HIPAA Privacy Rule does not require a covered health care provider to mail out its revised notice or otherwise notify patients by mail of changes to the notice. Rather, when a covered health care provider with a direct treatment relationship with individuals makes a change to his notice, he must make the notice available upon request to patients

or other persons on or after the effective date of the revision, and, if he maintains a physical service delivery site, post the revised notice in a clear and prominent location in his facility. See 45 CFR 164.520(c)(2)(iv). In addition, the provider must ensure that the current notice, in effect at that time, is provided to patients at first service delivery, and made available on his customer service web site, if he has one. See 45 CFR 164.520(c).

Q: Is a physician required to give her notice to every patient or can she just post the notice in her waiting room and give a copy to those patients who ask for it?

A: The HIPAA Privacy Rule requires a covered health care provider with direct treatment relationships with individuals to give the notice to every individual no later than the date of first service delivery to the individual and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where she provides health care directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy. See 45 CFR 164.520(c) for other notice provision requirements.

Q: It is common practice for hospitals and other health care providers to collect preoperative information over the phone from a new patient prior to the day of surgery in order to determine whether the patient has any special medical concerns or issues that need to be addressed. Does the HIPAA Privacy Rule prohibit this practice if the patient has not yet received or acknowledged the provider's notice?

A: No, the Privacy Rule does not prohibit this practice. Where a health care provider's initial contact with a patient is simply to schedule an appointment or a procedure, or to collect information in anticipation of an appointment or a procedure, the Privacy Rule's requirements for providing the notice and obtaining a patient's acknowledgment of the notice may be satisfied at the time the individual arrives at the provider's facility for his or her appointment or procedure.

Q: Is a pharmacist permitted to have customers acknowledge receipt of the notice by signing or initialing the log book that they already sign when they pick up prescriptions?

A: Yes, provided that the individual is clearly informed on the log book of what they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else that also appears on the log book (such as a waiver to consult with the pharmacist). The HIPAA Privacy Rule provides covered health care providers with discretion to design an acknowledgment process that works best for their businesses.

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

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

Background

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

The only new authority for government involves enforcement of the protections in the Privacy Rule itself. To ensure that covered entities protect patients' privacy as required, the Rule requires that health plans, hospitals, and other covered entities cooperate with efforts by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to investigate complaints or otherwise ensure compliance.

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

Frequently Asked Questions

Q: Does the HIPAA Privacy 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 the Department of Health and Human Services Office for Civil Rights (OCR) the authority to investigate complaints that Privacy Rule protections or rights have been violated, and otherwise to ensure that covered entities comply with the Rule.

For enforcement purposes, OCR may need to look at how a covered entity handled medical records and other personal health information, as is typical in many enforcement settings. This investigative authority is needed so that the Rule can be enforced, and to ensure the independent review of consumers' concerns over privacy violations. Even so, the Privacy Rule limits disclosures 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 HIPAA 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 of Health and Human Services' (HHS) 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 HHS Office for Civil Rights' (OCR) access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information may be needed. For instance, OCR would 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 include:

X 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.

X 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 HIPAA Privacy 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, since the Rule establishes new procedures and safeguards that 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: Does the HIPAA Privacy Rule create a government database with all individuals' personal health information?

A: No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation.

Q: How does the HIPAA Privacy 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.

MISCELLANEOUS
FREQUENTLY ASKED QUESTIONS
ABOUT THE HIPAA PRIVACY RULE

Q: If I believe that my privacy rights have been violated, when can I submit a complaint?

A: By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, "covered entities") have until April 14, 2003, to comply with the HIPAA Privacy Rule. (Small health plans have until April 14, 2004, to comply). Activities occurring before April 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions. After that date, a person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically. This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The Secretary may waive this 180-day time limit if good cause is shown. See 45 CFR 160.306 and 164.534. OCR will provide further information on its web site about how to file a complaint (www.hhs.gov/ocr/hipaa/).

In addition, after the compliance dates above, individuals have a right to file a complaint directly with the covered entity. Individuals should refer to the covered entity's notice of privacy practices for more information about how to file a complaint with the covered entity.

Q: If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

A: The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.

Q: Does the HIPAA Privacy Rule protect genetic information?

A: Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See 45 C.F.R 160.103 and 164.501.

Q: A provider might have a patient's medical record that contains older portions of a medical record that were created by another/previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

A: Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Q: Can a physician's office FAX patient medical information to another physician's office?

A: The HIPAA Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician's office, and placing the fax machine in a secure location to prevent unauthorized access to the information. See 45 CFR164.530(c).

Q: Are hospitals able to inform the clergy about parishioners in the hospital?

A: Yes, the HIPAA Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual's name; location in the facility; health condition expressed in general terms; and religious affiliation. The facility may disclose this directory information to members of the clergy. Thus, for example, a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure. Directory information, except for religious affiliation, may be disclosed only to other persons who ask for the individual by name. When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object to being included in the facility's directory, these disclosures may still occur, if such disclosure is consistent with any known prior expressed preference of the individual and the disclosure is in the individual's best interest as determined in the professional judgment of the provider. See 45 CFR 164.510(a).

Q: Are State, county or local health departments required to comply with the HIPAA

Privacy Rule?

A: Yes, if a State, county or local health department performs functions that make it a covered entity, or otherwise meets the definition of a covered entity. For example, a state Medicaid program is a covered entity (i.e., a health plan) as defined in the Privacy Rule. Some health departments operate health care clinics and thus are health care providers. If these health care providers transmit health information electronically in connection with a transaction covered in the HIPAA Transactions Rule, they are covered entities. For more information, see the definitions of covered entity, health care provider, health plan and health care clearinghouse in 45 CFR 160.103. See also, the "Covered Entity Decision Tools" posted at **http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp**. These tools address the question of whether a person, business or agency is a covered health care provider, health care clearinghouse or health plan.

If the health department performs some covered functions (i.e., those activities that make it a provider that conducts certain transactions electronically, a health plan or a health care clearinghouse) and other non-covered functions, it may designate those components (or parts thereof) that perform covered functions as the health care component(s) of the organization and thereby become a type of covered entity known as a "hybrid entity." Most of the requirements of the Privacy Rule apply only to the hybrid entity's health care component(s). If a health department elects to be a hybrid entity, there are restrictions on how its health care component(s) may disclose protected health information to other components of the health department. See 45 CFR 164.504 (a) – (c) for more information about hybrid entities.

Q: Are the following types of insurance covered under HIPAA: long/short term disability; workers compensation; automobile liability that includes coverage for medical payments?

A: No, the listed types of policies are not health plans. The HIPAA Administrative Simplification regulations specifically exclude from the definition of a "health plan" any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 CFR 160.103. As described in the statute, excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs:

- Coverage only for accident, or disability income insurance, or any combination thereof.

- Coverage issued as a supplement to liability insurance.

- Liability insurance, including general liability insurance and automobile liability insurance.
- Workers' compensation or similar insurance.
- Automobile medical payment insurance.
- Credit-only insurance.
- Coverage for on-site medical clinics
- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Q: Is an entity that is acting as a third party administrator to a group health plan a covered entity?

A: No, providing services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as by providing group health insurance). See 45 CFR 160.103.

Q: The Social Security Administration (SSA) collects medical records for the Social Security Income (SSI) disability program. Is SSA a covered entity (e.g., a health plan)?

A: The SSA is not a covered entity. The collection of individually identifiable health information is not a factor in determining whether an entity is a covered entity. Covered entities are defined in HIPAA; they are (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule. These terms are defined in detail at 45 CFR 160.103.

Q: Is the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA) that was enacted in December 2001?

A: No, the compliance dates for the Privacy Rule is April 14, 2003, or, for small health plans, April 14, 2004. ASCA does not apply to the HIPAA Privacy Rule. Rather, ASCA delays compliance with the Transaction and Code Set standards adopted by the HIPAA Transactions Rule for covered entities that file a compliance plan. More information about ASCA can be found on the web site for the Centers for Medicare and Medicaid

Services at http://cms.hhs.gov/hipaa/.

Q: HIPAA allows "small health plans," defined as health plans having annual receipts of $5 million or less, an additional year (in the case of the Privacy Rule, until April 14, 2004) to come into compliance. How should a health plan determine what receipts to use to decide whether it qualifies as a "small health plan?"

A: Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 CFR 121.104 to calculate annual receipts. Health plans that do not report receipts to the IRS - for example, ERISA group health plans that are exempt from filing income tax returns - should use proxy measures to determine their annual receipts. Further information about the relevant provisions of 13 CFR 121.104 and these proxy measures, and additional information related to "small health plans," may be found at http://cms.hhs.gov/hipaa/hipaa2/default.asp.

Q: Does the HIPAA Privacy Rule require that covered entities provide patients with access to oral information?

A: No. The Privacy Rule requires covered entities to provide individuals with access to protected health information 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 maintained only for customer service review and not to make decisions about the member.

Q: Does the HIPAA Privacy Rule require that covered entities 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.

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 at 45 CFR 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.