FREQUENTLY ASKED QUESTIONS

May a physician use a sign-in sheet? Call out names in the waiting area? Place charts outside a patient's room while the patient is waiting to see the physician?
Yes. To the extent these activities result in other people learning a patient's name or other information, the disclosure would be considered "incidental" to the physician's treatment of the patient, and therefore acceptable under HIPAA.

Physicians should take appropriate precautions to limit the amount of information that might be incidentally disclosed in this manner. For example, physicians should not ask patients to list "reason for visit" on a sign-in sheet. With respect to placing charts outside of an examination room or the patient's hospital room while the patient is waiting to see the physician, the physician should take precautions such as turning the front of the chart towards the wall so others do not have the opportunity to read the front page while walking past the room.

May a physician or hospital "fax" a patient's medical information to other physicians or to an insurer?
Yes. The Privacy Rules do not prohibit a "covered entity" from faxing protected health information.

A physician should be sure, however, to comply with the Privacy Rules' requirements for disclosures generally. For example, the physician should check whether the "minimum necessary" rule applies and, if it does, limit the information in the fax to the minimum necessary information.

Also, a physician should be sure to have appropriate security safeguards in place that are administrative, technical, and physical in nature. For example, the physician should use policies and procedures that require office staff to verify the recipient's fax number and use a cover sheet that does not include protected health information.

What is the "minimum necessary" standard?
The Privacy Rules require a physician to make reasonable efforts to limit the amount of protected health information that the physician uses or discloses to the minimum amount that is necessary to accomplish the purpose of the use or disclosure.

Importantly, this requirement does **not** apply when a physician discloses information to another provider for treatment purposes or when a physician requests information from another provider for treatment purposes. Accordingly, the minimum necessary standard should not interfere with a physician's ability to provide appropriate treatment to patients.

The minimum necessary standard also does **not** apply when the physician releases information: (a) directly to the patient, (b) pursuant to a patient's authorization, or (c) for disclosures that are required by law or are necessary to comply with the Privacy Rules.

What can a physician say to another covered entity if the covered entity will not fax information on the belief that the "fax" would not be allowed under the Privacy Rules?
The Privacy Rules do not prohibit a covered entity from faxing protected health information to a physician.

If a covered entity refers to the Privacy Rules as the reason the covered entity will not fax information to a physician, the physician may direct the covered entity to the Department of Health and Human Services' Frequently Asked Questions at: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html . The physician may also find it helpful to assure the covered entity that appropriate safeguards are in place to receive the fax securely.

May a physician discuss information about a patient's treatment with other physicians using e-mail?
Yes. Physicians may use any method of communication – including e-mail, oral conversations, written letters, or other methods (including sending facsimiles) – so long as the physician uses "reasonable and appropriate safeguards" to protect the communication.

What steps should a physician take to protect oral communications with or about patients?
The Privacy Rules require physicians to use appropriate administrative, technical, and security safeguards to protect the privacy of protected health information – including oral communications. This means that physicians must use reasonable efforts to have protections in place, but they do not need to make expensive structural changes to "soundproof" their offices. The Department of Health and Human Services addresses this topic in one of its Frequently Asked Questions at http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html .

Physicians who would like to learn more about protecting oral communications through use of "sound masking" or "acoustic engineering" tools can review a paper entitled "Oral Communications: Myths and Facts White Paper," one of the "SNIP Work Products" posted on the Web site of the Workgroup for Electronic Data Interchange (WEDI)/Strategic National Implementation Process (SNIP) at http://www.wedi.org .

If a patient's family members call to ask how their loved one is doing, what can the treating physician disclose?
This depends on whether the person calling has a role in taking care of the patient and whether the physician believes, in his/her professional judgment, release of the patient's information is in the patient's interest and relates to the person's involvement in the patient's care.

The Privacy Rules allow a physician to share a patient's information with the patient's family member or friend so long as the information is limited to information directly relevant to that person's involvement in the patient's care. For example, a physician may tell a person living with the patient that the patient needs plenty of rest and lots of fluids or that the patient needs to take a prescribed medication twice daily with food. The physician should not share more information than the person needs to assist with the patient's care.

A physician should not share a patient's information with the patient's family or friends if the patient has asked the physician not to or if the physician believes, in his/her professional judgment, a disclosure would be inappropriate.

Question regarding physicians' difficulty with gathering patient information
"Some physicians are complaining that the Privacy Rules are making it hard for them to get information about their patients. For example, there have been reports of physicians unable to check on a patient who has been transferred to another hospital or unable to get information from a specialist who is seeing one of the physician's patients. How does a physician keep these problems from interfering with his/her practice?"

The Privacy Rules do not place any restrictions on the ability of a covered entity to share a patient's protected health information with a physician for treatment purposes.

The best way for a physician to respond to this problem is to be armed with knowledge about what the Privacy Rules actually do and do not prohibit. The physician should be ready to explain that the Privacy Rules permit a covered entity to share unlimited protected health information with a physician for the physician to use for treatment purposes. The Privacy Rules state that "A covered entity may disclose protected health information for treatment activities of a health care provider" (45 C.F.R. § 164.506(c)(2)) and that the minimum necessary requirement "does not apply to....Disclosures to or requests by a health care provider for treatment" (45 C.F.R. § 164.502(b)(2)(i)).

Department of Health and Human Services - Frequently asked questions

Physicians report a concern the Privacy Rules may create a barrier to effective communication about patients. How should a physician evaluate whether a particular communication is acceptable or is restricted by the Privacy Rules?
A physician may always disclose protected health information to another physician or other health care provider for treatment. The physician does not need to limit or otherwise restrict the amount of information disclosed for purposes of treatment.

The only exception applies to a mental health professional's personal psychotherapy notes, which may be disclosed only with the patient's authorization.

May a physician send out appointment-reminder postcards? Leave messages on answering machines? Verify appointment times with the patient's spouse or other living companion?
Yes. The Privacy Rules allow a physician to communicate with patients, including communications to the patient's home. When making these types of communications, however, the physician should take precautions to safeguard the patient's privacy. For example, when leaving a message on the patient's answering machine, the physician should limit the amount of information left in the message to just the information necessary to confirm the appointment time or to request that the patient call the physician's office.

The Privacy Rules also permit a physician to leave a message directly with the patient's family member or companion. Physicians are allowed to disclose information about the patient's care to the patient's family members and friends, even if the patient is not present or has not affirmatively given the physician permission to do so, so long as the

physician believes, in his/her professional judgment, that the disclosure is in the patient's best interest. However, if the patient has expressly directed that there be no disclosure to specific family members or friends, the patient's wishes must be respected.

Also, if a patient has requested that the physician communicate in a confidential manner, the physician must accommodate the request if it is reasonable. For example, it would be reasonable for a patient to request that all mailings be sent to a specific address (e.g., to the patient's office instead of home, or vice versa), or be sent in a closed envelope instead of on a postcard.

May a hospital provide information, including a patient's room number, to a patient's family or friends or to the clergy?
Yes. The Privacy Rules allow hospitals to disclose patients' names and other directory information to anyone asking for the patient by name or to the clergy. Patients do not need to sign up to be included in the directory, but must be allowed to "opt out" and choose not to be listed.

May a physician send protected health information overseas for transcription?
Yes. The Privacy Rules limit the types of disclosures that are acceptable, but do not limit the ability of a physician to make a disclosure to any particular type of recipient, including a non-U.S. recipient.

A physician must enter into a Business Associate Agreement with its transcription company, regardless of where the company is located, so that safeguards to protect privacy are in place at the transcription service. The Privacy Rules require physicians to use appropriate safeguards when storing or transmitting information (within or outside of the U.S.), and the physician is responsible for ensuring that a subcontractor (such as a transcription service), wherever located, uses appropriate safeguards too.

Depending on where the physician is sending the patient information, local laws may also apply and the physician should consider consulting with legal counsel there as well.

May a physician or hospital release information to the police to assist with an investigation?
Yes. The Privacy Rules explicitly allow a physician to disclose protected health information for law enforcement purposes, although the physician must comply with certain requirements. For example, the type of information that may be disclosed may be limited and the physician may need to verify the identity and authority of the officer making the request. To learn more about the requirements for disclosing protected health information to the police, check the Department of Health and Human Services' Frequently Asked Questions at:
http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html .

The family of a deceased patient is requesting the patient's original medical records. Can my office refuse?
Yes, in some instances. The Privacy Rule protects the identifiable health information of the deceased individual for a period of 50 years to the same extent the Rule protects the health information of a living individual. However, the Rule provides three 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, the Privacy Rule allows disclosure of certain protected health information about a decedent to family members of the decedent, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity. The information that may be disclosed is that which is relevant to the person's involvement in the decedent's care or payment for care.

Third, 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. Therefore, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.

Are there any physicians or groups exempted from the HIPAA privacy requirements?
Yes—in limited circumstances. A provider (or provider group) would be exempt from the HIPAA privacy requirements where (a) the provider 1) has less than 10 full time employees and 2) all claims transactions to all payers are made

solely on paper (regardless of whether the provider participates in Medicare or not); OR (b) the provider 1) has a practice of any size and 2) all claims transactions to all payers are made solely on paper and 3) the practice does not participate in Medicare.

Under the HIPAA privacy regulations, "a health care provider who transmits any health information in electronic form" is a "covered entity." Thus, a practice that accepts or uses any electronic transactions (or uses a business associate to do so) must comply with the privacy regulations--whether the practice has more or less then 10 full time employees.

Providers with 10 or more full time employees, which might otherwise wish to conduct all claims transactions solely on paper, will—if claims are submitted to Medicare—be required to comply with the HIPAA privacy requirements. This is because the HIPAA Transactions and Code Set (TCS) regulations that became effective in October, 2003 require practices with 10 or more full time employees to conduct all Medicare transactions electronically. While at the present time (January 2004), a contingency plan enables Medicare to accept legacy (paper) claims, the contingency plan does not exempt covered entities from compliance with applicable privacy regulations. A reminder: the present contingency arrangement for compliance with the TCS regulations will not continue forever. Any practice with 10 or more full time employees that accepts Medicare must convert to electronic claims as soon as possible.

What is a Notice of Privacy Practices?
A Notice of Privacy Practices is a document required by the Privacy Rules that explains how a physician may use and disclose a patient's information and what rights a patient has with respect to the medical information about him/her that is maintained by the physician. The Privacy Rules impose specific requirements for the Notice of Privacy Practices regarding what must be included and how the information should be presented.

The AMA has posted a sample Notice of Privacy Practices (Word, 56KB) as well as links to other samples.

What are the requirements for a physician to distribute a Notice of Privacy Practices to patients and seek an acknowledgement that each patient has received a copy?
A "direct treatment provider" (e.g., a primary care physician) must provide the Notice of Privacy Practices to each patient at the time of first service delivery. The direct treatment provider must make a good faith effort to obtain the patient's written acknowledgement of receipt. A physician is temporarily relieved of the provision and acknowledgement requirements in emergency circumstances, but must provide the Notice as soon as reasonably practicable after the emergency situation.

A physician is not required to obtain the patient's written acknowledgement of receipt so long as the physician documents that he/she attempted to obtain such acknowledgement and why the acknowledgement was not obtained.

If there is a physical service delivery site, the Notice must be posted in a clear and prominent location and copies of the Notice must be available for patients to take with them upon request.

An "indirect treatment provider" (e.g., a pathologist or radiologist) is not required to distribute a Notice of Privacy Practices except to provide a copy to a patient upon request.

Do the Privacy Rules require physicians to have pharmaceutical sales representatives sign any type of confidentiality agreement, even one that is not a Business Associate Agreement?
No. The Privacy Rules require physicians to adopt reasonable safeguards to protect the security of protected health information and to protect against inadvertent disclosures. The reasonable safeguard requirement does not mean that a physician must obtain a confidentiality agreement from visitors who might have access to patient information.

Physicians should take other measures, however, such as not allowing visitors to roam freely through the office or examination areas and keeping medical records and other notes away from plain view of office visitors.

Although the Privacy Rules do not require physicians to have pharmaceutical sales representatives sign any type of confidentiality agreement, may a physician ask sales representatives to sign them anyway?
Yes. The Privacy Rules do not require physicians to have sales representatives sign any type of confidentiality agreement—neither a Business Associate Agreement nor a more general confidentiality agreement. A physician may, however, ask a sales representative to sign a confidentiality agreement if the physician believes it would be useful to protect the confidentiality and security of information maintained by the physician.

May a physician continue to make adverse event reports to pharmaceutical manufacturers and/or the FDA?

Yes. The Privacy Rules expressly permit a physician to make adverse event reports to a person or entity subject to the FDA's jurisdiction, such as a pharmaceutical manufacturer. As an added precaution to protect patient privacy, and to be sure a report is directed appropriately, physicians should make adverse event reports directly to the drug safety (or other appropriate department) of the manufacturer rather than to the sales representative.

As with the majority of disclosures that are not for treatment purposes, physicians should disclose only the minimum amount of information that is necessary to make the report.

May a sales representative sit in on a patient's exam or treatment?
No – unless the physician has obtained a valid authorization from the patient to share the information for these purposes. A sales representative may sit in on a patient's exam or treatment only if the patient has signed a valid authorization expressly allowing the sales representative to do so. The physician should provide the patient with sufficient opportunity to read the authorization form and ask questions before the patient decides whether to provide permission.

May a physician share protected health information with a sales representative as part of a discussion about the physician's experiences with the manufacturer's product?
No – unless the physician has obtained a valid authorization from the patient to share the information for these purposes.

Physicians may continue to engage in discussions with sales representatives about a particular drug's side effects, benefits, or other qualities. Physicians should ensure, however, that they do not use identifiable information when having these discussions. If the physician wants to discuss a specific patient in a manner that might reveal the patient's identity, the physicians should obtain a valid authorization from the patient prior to engaging in the discussion.

May a physician disclose protected health information to a pharmaceutical sales representative or directly to a pharmaceutical manufacturer for purposes of enrolling a patient in a patient assistance program?
No – unless the physician has obtained a valid authorization from the patient to share the information for these purposes.

There may be an argument that this type of disclosure can be categorized as a disclosure for treatment purposes as the "coordination or management of health care by a health care provider with a third party," and therefore an authorization would not be necessary. Until clarification of the Privacy Rules becomes available, physicians should obtain a valid authorization prior to making such a disclosure.

May a physician provide a sales representative with patients' names and addresses so the sales representative can send follow-up mailings?
No. This would require the physician to obtain a valid authorization from each patient giving the physician permission to disclose the patient's protected health information to the pharmaceutical manufacturer for this purpose.

What tools and resources does the AMA have available to assist physicians to understand and implement the Privacy Rules?
The AMA has many helpful resources available to assist physicians with HIPAA Privacy compliance, including sample forms, and explanations of important requirements at the AMA Compliance Resources Web page.

Does the AMA recommend other resources that a physician might find helpful to learn more about the Privacy Rules?
Yes. The Department of Health and Human Services, Office of Civil Rights, maintains a Web site (This link will take you off the AMA Web site.) that provides a variety of helpful information, including forms and many educational materials about the Privacy Rules.

View links from the AMA's Web site to other resources.

Where can a physician learn more about the HIPAA Transaction and Code Set Rules and the Security Rules?
The AMA has many helpful resources to assist physicians with all of HIPAA's requirements.

Learn more about the Transaction and Code Set Rules, including information about the AMA's Click and Complain HIPAA Complaint Form, which allows physicians and their office staff to register complaints with the AMA about health plans,

clearinghouses, and other entities that are not acting in compliance with the Transaction and Code Set Rules which became effective October 16, 2003.

Learn more about the Security Rules for which compliance will be required in April, 2005.

Is HIPAA ever preempted by state law?
Yes. Although HIPAA usually preempts contrary state law, there are four situations in which state law preempts HIPAA. The exceptions are for: 1) state reporting laws; 2) health plan reporting and information; 3) specific exemptions determined by the HHS secretary; and 4) when state health privacy provisions are more stringent.

State law, state constitutions, regulations, rules, common law, and other state actions that have the force and effect of law may all give rise to these exceptions.