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:

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

- How the covered entity may use and disclose protected health information about an individual.

- 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.

- 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.

- 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.

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

- 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.

- *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.

- *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.

- 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.

- 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.

- 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.