Managing Information Privacy & Security in Healthcare

Enhancing Patient Understanding

By Jeff Collmann, PhD and Ted Cooper, MD

Introduction

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.

Notice of Privacy Practices

The HIPAA Privacy Standard requires that this text must be used as a header or otherwise be displayed prominently in the notice:
"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

The notice must contain:
(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted for each of the following purposes: treatment, payment, and healthcare operations.
(B) A description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the individual's written authorization.
(C) If a use or disclosure for any purpose is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.
(D) For each purpose described the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by law.
(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization in writing at any time.
(F) If the covered entity intends to engage in any of the following activities, the description required must include a separate statement describing the activity:

- The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other heath-related benefits and services that may be of interest to the individual;
- The covered entity may contact the individual to raise funds for the covered entity.

- A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(G) The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights.

- The right to request restrictions on certain uses and disclosures of protected health information and that the covered entity is not required to agree to a requested restriction.
- The right to receive confidential communications of protected health information and request that these be delivered by an alternative method or at an alternative location.
- The right to inspect and copy protected health information.
- The right to amend protected health information.
- The right to receive an accounting of disclosures of protected health information made for purposes other than treatment, payment, or healthcare operations.
- The right of an individual, including an individual who has agreed to receive the notice electronically to obtain a paper copy of the notice from the covered entity upon request.

(H) The notice must contain statements of the covered entity's responsibilities including the following:

- The covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information.
- The covered entity is required to abide by the terms of the notice currently in effect.
- For the covered entity to apply a change in a privacy practice that is described in the notice of protected health information that the covered entity created or received prior to issuing a revised notice that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(I) The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(J) The notice must contain the name, or title, and telephone number of a person or office to contact for further information.

(K) The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

Revisions to the Notice

The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

Provision of Notice

A covered entity must make the notice available upon request to any person:

- No later than the compliance date for the health plan, to individuals then covered by the plan;
- Thereafter, at the time of enrollment, to individuals who are new enrollees;
- AND within 60 days of a material revision to the notice, to individuals then covered by the plan;

No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

Health plans satisfy the notice distribution requirements of this paragraph if the notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

A covered healthcare provider that has a direct treatment relationship with an individual must:

- Provide the notice no later than the date of the first service delivery, including service delivered electronically, to each patient or in an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.
- Except in an emergency treatment situation, make a good-faith effort to obtain a written acknowledgment of receipt of the notice provided and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;
- If the covered healthcare provider maintains a physical service delivery site have the notice available at the service delivery site for individuals to request to take with them and post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered healthcare provider to be able to read the notice.
- Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision.
- A covered entity that maintains a Web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the Web site.

A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity and any written acknowledgments of receipt of the notice or documentation of good-faith efforts to obtain such written acknowledgment.

The HHS recommendations signal some broad social changes; however, whose significance transcends the narrow legal and regulatory context of their development. Reforms in healthcare finance are refocusing some aspects of healthcare from the doctor-patient relationship to the organization-patient relationship, thus making healthcare organizations accountable to patients in new ways. In addition to being accountable for healthcare processes and outcomes, organizations are becoming accountable to patients for their business practices, particularly for what they do with information about their individual cases. These changes as well will increasingly require healthcare organizations to obtain authorizations for certain uses and disclosures of protected health information, provide access to information historically reserved for institutional use only, educate patients about their business practices, and extend new services to their patients using electronic media. Model examples for how some healthcare organizations are trying to meet these new obligations follow.

Examples of Online Statements of Privacy Practices

- Office of Civil Rights Model Notice of Privacy Practices
- Department of Defense Military Health System
- Department of Veterans Affairs
- Beth Israel Deaconess Medical Center
- Mayo Clinic
- Stanford University Hospitals