HIGHLIGHTS OF THE NEW HIPAA REGULATORY PROVISIONS

Amanda G. Fields, General Counsel for American Pharmacies (APRx)

Introduction

The U.S. Department of Health and Human Services (DHHS) has issued wide-ranging changes to HIPAA rules, in part designed to flesh out changes to the HIPAA Privacy and Security Rules made by the Heath Information Technology for Economic and Clinical Health Act (HITECH). ***Many of these new rules take effect September 23, 2013.***

The regulatory changes are both big and small. Major changes include lowering the standard for what constitutes a security breach and subjecting subcontractors to HIPAA regulations; minor changes include allowing an individual to request protected health information sent to a third party. Both the major and minor changes will affect pharmacists and should be reflected in everything from HIPAA policies to business associate agreements to notice of privacy practices.

Major Changes Affecting Pharmacists

❶ **New requirements for business associate agreements.** Older HIPAA regulations required covered entities such as pharmacists to have agreements in place with business associates receiving protected health information to ensure that the information remains safe. This rule is still in effect under the new regulations, but these agreements now must contain provisions reflecting the regulatory changes. For example, a business associate must agree to ensure that its subcontractors agree to the same restrictions and conditions on use of protected health information.

Covered entities will have one year beyond the Sept. 23, 2013 compliance date to update existing contracts with their business associates that complied with the old HIPAA regulations and were not renewed or modified between March 26, 2013 and September 23, 2013. HHS has published sample business associate agreement provisions that comport with the new regulations on its website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

❷ **Changes to the definition of marketing.** Under both old and new HIPAA regulations, covered entities such as pharmacies are forbidden from marketing to individuals—defined as encouraging an individual to buy a product or service on behalf of a third party for pay by telephone, mail, or email—unless previously authorized by the individual. Under HITECH, communication about a drug or biologic currently prescribed was specifically excluded from the definition of marketing and so did not require prior authorization, so long as any payment received for the communication was reasonably related to the cost of that communication.

The new regulations make it clear that refill reminders are not marketing. HHS states that if a pharmacy is paid by drug manufacturer to provide refill reminders, no authorization from the individual is required as long as the payment covers only the pharmacy's cost of writing, printing, and mailing the reminders. If the drug manufacturer pays more than those costs, however, the refill reminder requires prior authorization—unless it is provided in a face-to-face communication.

HHS has further clarified in the preamble to the new rule that the exception for communications about a drug currently prescribed includes communications about a generic equivalent, communications

about drug delivery systems such as an insulin pump, and "adherence communications" encouraging an individual to take prescribed medication as directed.

❸ **The right of individuals to non-disclosure of protected health information.** Under HITECH, an individual has a right to request non-disclosure of information pertaining to an item or service paid for out of pocket, and a covered entity must comply with the request if the disclosure is for carrying out payment or healthcare operations and is not otherwise required by law. For example, if an individual wishes to restrict disclosure of a prescription to his health plan, he may do so if he pays for the prescription out of pocket.

In the preamble to the new rules, HHS has clarified that the payment may be made by the individual or another person, and if the payment is dishonored —for example, a check bounces—a covered entity must first make reasonable efforts to contact the individual and obtain payment before billing his health plan.

❹ **Access of individuals to protected health information.** New regulations make it easier for individuals to access health records in electronic format and harder for a covered entity to provide it in a hard copy. Under the new rule, a pharmacist would have to provide a health record to an individual in a mutually agreeable electronic format, such as a PDF or an MS Word document. A hard copy may be provided only if the individual declines all digital formats that are readily producible or if the record is maintained only in a hard copy.

The new regulations require that a pharmacy transmit requested information to a designated person instead of the requesting individual if that individual clearly indicates in writing the designated person and where to send the requested information.

Finally, the regulations shorten the response time for providing the record when it is stored off-site. Previously, a covered entity had 60 days, plus a permissible 30-day extension in extenuating circumstances, to respond to the request; under the new regulations, a covered entity has 30 days plus the permissible 30-day extension.

❺ **New notice of privacy practice requirements.** The new regulations require that a notice of privacy practice reflect these changes. In particular, under the new regulations, a notice of privacy practice must describe the uses and disclosures of protected health information that require authorization. The notice must state that disclosures constituting the sale of protected health information, as well as most

Recommended Actions

- ***Update business associate agreements.*** *Business associate agreements must reflect these new regulatory changes, although existing and unmodified agreements need not be updated until Sept. 22, 2014.*
- ***Revise notice of privacy practice.*** *Notice of privacy practices must reflect an individual's new right to nondisclosure of certain information, the right to notification if a breach occurs, & the uses and disclosures of protected information that require authorization.*
- ***Update HIPAA policies & procedures & retrain workers on what constitutes a breach****. HIPAA regulations require pharmacists to develop & document policies & procedures & to train employees on HIPAA requirements. You should revise your policies & retrain employees to address these changes, particularly what constitutes a breach. This step is vital because:*

  (1) changes to what constitutes permissible & impermissible disclosure have in turn changed what constitutes a breach,

  (2) notification deadlines hinge on when the covered entity knew or by reasonable exercise of diligence would have known about the breach, and

  (3) documentation to prove adequate response to a potential breach must reflect the new requirements, including consideration of the four mandatory factors for assessing risk.

marketing, will be made only with authorization from the individual. It must also inform individuals of their new right to restrict disclosure of information on health-care items or services paid for out of pocket. And it must state the right of an individual to be notified following a breach of unsecured protected health information.

❻ **What constitutes a breach requiring notification.** The new regulations mandate a stricter standard for what constitutes a breach of security of protected health information. Under the new regulations, any impermissible use or disclosure of protected health information is presumed to be a breach requiring notification unless the covered entity demonstrates through a risk assessment that there is low probability that protected health information has been compromised.

The risk assessment must be conducted using objective factors, including consideration of the following four factors:

(1) the nature and extent of protected health information involved;

(2) the unauthorized person using the information or to whom the disclosure was made;

(3) whether the information was actually acquired and viewed; and

(4) the extent to which the risk to the protected health information has been mitigated.

HHS has stated, as an illustration of the new rule, that if a covered entity sends a fax with protected health information to the wrong physician practice and the receiving physician promptly destroys the fax, the covered entity may be able to show after performing a risk assessment that there is a low probability of compromise and thus no breach requiring notification.

Because a covered entity has the burden of proving notification or, alternatively, that there was no breach requiring notification, it should document that the required notifications were made or that no notification was required.

Questions? Please contact Amanda Gohlke Fields at afields@aprx.org