Reviewing the New HIPAA Rules

Save to myBoK

By Chris Dimick

At 138 fine-print pages, the final rule detailing the HITECH Act's modifications to HIPAA privacy and security requirements is not a quick or easy read. But it is an important read since the content of the *Federal Register* post drastically impacts HIM professionals and their business associates. Hoping to direct HIM professionals to the sections of the rule that specifically impact the HIM industry and provide guidance on how to respond, AHIMA staff experts have conducted a full analysis of the omnibus regulation and posted it to AHIMA's website. The following is a segment of that analysis. Those who haven't discussed the individual impact of these changes should do so soon-the new HIPAA requirements are effective March 26, 2013. The compliance date for the regulations is September 23, 2013.

Final Rule's HIM Highlights

The Department of Health and Human Services' Office for Civil Rights posted the HITECH Act's HIPAA modification final rule to the *Federal Register* in January after several years of industry anticipation. The rule covers a variety of HIPAA changes that affect many subsectors of the HIM, health IT, and general healthcare industries. AHIMA's analysis of the rule breaks it down by section. Major highlights from the rule include:

- Big changes for healthcare business associates and their subcontractors, who must now follow the HIPAA Security Rule for electronic protected health information (PHI). Business associates must handle obtaining HIPAA-compliant agreements with their subcontractors-not the business associate's covered entity. A grandfather clause for business associate agreement transition has also been instituted.
- Patients must authorize any health marketing they receive, though some exceptions-like prescription refill reminders-do apply. Business associates must now obtain authorizations prior to marketing.
- The sale of PHI by a covered entity or business associate is prohibited and defined by the rule.
- Compound authorizations for research have been authorized, with certain rules attached.
- Any individually identifiable health information of a person deceased more than 50 years is no longer considered PHI under the Privacy Rule.
- Covered entities are now permitted to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of a decedent prior to death, unless doing so is inconsistent with any known prior expressed preference of the individual.
- Covered entities can disclose proof of immunization to a school where state or other law requires it prior to admitting a student. Written authorization is no longer required, but an agreement must still be obtained, which can be oral.
- Covered entities must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications.
- The notice of privacy practices must be revised and redistributed.
- Patients can restrict health plans' access to medical records that pertain to treatment paid for by the patient out of their own pocket.
- Patient access to electronic PHI is now required. Covered entities must provide an electronic copy of protected health information that is maintained electronically and located in one or more designated record sets. The covered entity must produce a copy of the electronic record in the form and format requested by the individual.
- Fees for paper and electronic copies are defined. Providers can charge for the cost of labor and materials used to copy PHI, whether in paper or electronic form. Labor costs can include a reasonable cost-based fee for skilled technical staff time spent creating and copying the electronic file. An entity can't withhold record copies due to a failure to pay for any services above the copying costs.
- Timeliness for paper and electronic records was defined.
- The breach notification rule's "harm" threshold was removed and replaced with a more objective standard.

- Various changes were made to the Genetic Information Nondiscrimination Act. Title I of GINA required a revision of the HIPAA Privacy Rule. Genetic information is defined as health information. Also, genetic information may not be used or disclosed for underwriting purposes (excludes long-term care plans from the underwriting prohibition).

New Privacy Notice Requirements

The HIPAA privacy notice that most providers require patients to read and sign before their first visit will need to be adapted due to the final rule. The notice of privacy practices (NPP) for protected health information has several new requirements. The NPP must now include:

- A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require an authorization.
- A statement that other uses and disclosures not described in the NPP will be made only with an authorization from the individual.
- A statement about fundraising communications and an individual's right to opt out. The mechanism does not have to be included on the NPP.
- Healthcare provider's NPP must inform individuals of their new right to restrict certain disclosures of PHI to a health plan if they pay for a service in full and out of pocket. Other covered entities can retain current verbiage as required under the privacy rule.
- The NPP must include a statement of an individual's right to be notified of a breach of unsecured PHI in the event they are affected.

The final rule clarifies that providers are not required to print and hand out a revised NPP to all individuals seeking treatment. Providers are required to give a copy of the NPP to and obtain a good faith acknowledgement of receipt from new patients. The revised NPP must be posted in a clear and prominent location with copies of the NPP available for individuals to easily take one. It would not be appropriate for an individual to have to ask the receptionist for a full copy of the NPP.

More Analysis to Come

More analysis of the HITECH-HIPAA privacy and security final rule will be provided in future *Journal of AHIMA* issues. In addition, AHIMA Practice Briefs impacted by these regulations and modifications will be updated. AHIMA has created a series of webinars and in-person meetings related to the final rule. For more information, visit www.ahima.org. The full final rule is available in the *Federal Register* at www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

Chris Dimick (chris.dimick@ahima.org) is editor-in-chief of the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "Reviewing the New HIPAA Rules" *Journal of AHIMA* 84, no.2 (March 2013): 40-41.