

# A First Peek at the Privacy Regulations

Save to myBoK

The office for Civil Rights got a late start on the HITECH privacy regulations (due last February), and it's clear from the draft rule it released in July that the office still has almost as many questions as answers on how to enact the HITECH provisions. However, the release does offer a good indication of OCR's direction, as well as some surprises for HIM professionals.

OCR published the rule as a notice of proposed rulemaking on July 14, a format intended to solicit industry feedback before proceeding to binding regulation. Comments are due by September 13.

The NPRM addresses the modifications to the HIPAA privacy rule mandated within ARRA's HITECH Act. There are also required modifications to the security and enforcement rules. Further, OCR is using the NPRM to update HIPAA with a list of corrections, clarifications, and modifications that it has been compiling since the rule's publication in 2002.

Many changes are of a technical or conforming nature; for example, updating definitions and moving sections. At a high level, the NPRM addresses the following HITECH provisions.

## Business Associates and Subcontractors

HITECH extends to business associates the same requirements and penalties as covered entities; further, it conveys business associate status to emerging entities such as health information exchanges and personal health record operators. Within the NPRM, OCR has added patient safety organizations to this list.

The proposal defines when a covered entity's subcontractor becomes a business associate, including agents, and it discusses subcontractors of business associates.

## Fund Raising and Sale of PHI

HITECH increases requirements and restrictions related to marketing and fund raising, such as prohibiting certain written communications. The NPRM describes proposed changes related to the opt-out notice and process, and it emphasizes that a covered entity may not condition treatment or payment on an individual's choice. OCR requests comments on what information should be allowed to be shared for fund-raising purposes.

HITECH also prohibits the sale of protected health information (PHI) without authorization, which the NPRM addresses.

## Access and Request for Restriction

HITECH requires covered entities that maintain EHRs to provide individuals with copies of their PHI in electronic format upon request or transmit the copy to an entity or person as directed. It also extends a consumer's right to request restrictions on disclosure to health plans of items or services that the consumer pays in full.

OCR describes these provisions and requests significant comments on meeting such requests as well as recouping costs. It expects costs attributable to labor to be "negligible" and requests comment on the types of activities that should be compensable aspects of labor.

## Investigations

OCR describes how it will investigate privacy complaints and determine willful neglect and harm. It proposes to allow HHS to share PHI with law enforcement agencies and state attorneys general during investigations.

## Minimum Necessary

HITECH required HHS to issue guidance on what constitutes "minimum necessary" under HIPAA. The NPRM offers little direction, instead requesting comments on what information would be helpful.

## (Not So) Miscellaneous and Next Steps

The "miscellaneous" items unrelated to HITECH are by no means incidental; several will have a significant impact on HIM operations. For example, within the NPRM OCR proposes to amend HIPAA to permit covered entities to disclose the records of a deceased patient to family members and others involved in care or payment.

OCR also is proposing changes to the notice of privacy practices that would further detail uses and disclosures of PHI that require patient authorization. OCR requests comments on the impact to operations and puts forward options to lessen that impact.

More information is available at <http://journal.ahima.org>. The NPRM is available at <http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf>.

Once OCR has reviewed comments it will proceed to either an interim final rule (if it seeks further comment) or a final rule. In most instances, covered entities will have 180 days from publication of the final rule to comply. However, OCR is already proposing an extension for business associate agreements.

---

**Article citation:**

AHIMA. "A First Peek at the Privacy Regulations" *Journal of AHIMA* 81, no.8 (August 2010): 46.

---

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.