Codify
BY AAPC

Health Information Compliance Alert

Privacy AND OCR SHALL GUIDE THEM

Many covered entities feel discombobulated by the delivery of the final privacy rule; for some, it's akin to being given a shiny new car, but without the keys. Fortunately, the OCR has taken steps to get your HIPAA engines pumping.

The HHS Office for Civil Rights Dec. 3 issued its first significant guidance on the Health Insurance Portability and Accountability Act's privacy rule since the Bush administration reworked the reg in August.

"The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented with minimum necessary standard, as appropriate, with respect to the primary use or disclosure," OCR reminds providers.

The 123-page guidance includes scores of frequently asked questions and other explanatory information addressing various sticking points in the HIPAA privacy framework.

Generally speaking, the HIPAA privacy rule requires covered entities to notify patients of their privacy rights, train employees on the privacy rule, adopt and implement privacy policies and procedures, designate a privacy officer who will ensure that employees follow these policies and procedures, and ensure that patient records containing individually identifiable health information are kept confidential, OCR instructs.

The guidance lists a host of routine health care practices that some observers feared would run afoul of the privacy rule such as using patient sign-in sheets and leaving answering machine messages at patients' homes (both of which OCR says are A-OK) and elaborates how the rule affects such practices.

As in past guidance from OCR, the agency seems to be taking pains to ensure that complying with the privacy rule won't overly disrupt the way covered entities do business. The guidance specifically points out that the rule is "scalable," so the feds don't expect a small physician practice to go to the same lengths to ensure privacy that a hospital or other large provider would.

OCR addresses some concerns specifically tailored to certain entities. Take physicians' practices, for example. "The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan my be a full-time position, and may have the regular support and advice of a privacy staff or board," OCR notes.

Similarly, "the training requirement may be satisfied by a small physician practice providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs."

While one industry expert approves of OCR's guidance on a practical level, there are still some concerns that weren't addressed, according to Kristen Rosati, an attorney with Phoenixbased Coppersmith Gordon Schermer Owens & Nelson. Rosati says she was disturbed that the guidance required business associates to follow covered entity's minimum necessary policies.

"This is the first we've ever heard of this requirement" as it applies to BAs, Rosati notes, adding that the requirement for BAs "isn't supported by the regulatory language" of the privacy rule.

Rosati says scores of BAs do business with many different CEs. "Whose policies are [the BAs] supposed to follow?" she asks. "This is one area in the guidance I think will cause a lot of problems, and [the OCR] needs to reconsider it immediately," Rosati tells Eli.

Despite its limitations, the document includes much-sought guidance on a variety of compliance quandaries, including the intersection of the HIPAA privacy rule with medical research and public health endeavors.

The guidance, for example, makes it clear that HIPAA-covered entities' disclosure of protected health information to researchers doesn't require a business associate contract.

Other topics contained in the guidance include the minimum necessary standard, workers' compensation issues, marketing and government access. And while the guidance is certainly plenty long, not much of the information contained in the tome is new, notes attorney Michael Roach with Michael Best & Friedrich in Chicago.

The OCR does, however, provide useful clarification on the one-year extension for business associate contracts, points out Jill Callahan Dennis, principal at Health Risk Advantage in Parker, CO. Covered entities that established contracts with business associates before Oct. 15, 2002 are allowed to continue operating under those contracts "for up to one additional year beyond the April 14, 2003 compliance date, provide that the contract is not renewed or modified prior to April 14, 2003," OCR explains.

Some contracts contain an automatic renewal provision, Dennis notes, and the guidance makes clear that such a renewal won't invalidate the one-year extension, "even if that renewal occurs before the extended compliance date" of April 14, 2004.

Finally, OCR notes that the guidance "does not address all of the relevant provisions in the Rule," and it plans to add to the guidance as more issues arise in the future.

Further, the HHS reserves the right to amend the privacy rule as the Secretary sees fit. That's an important caveat to consider for entities still struggling to reach compliance, a sentiment echoed by Rosati: "This guidance doesn't function as law it's just guidance."

Editor's Note: To see the guidance, go to www.hhs.gov/ocr/hipaa/privacy.html