Codify
BY AAPC

Health Information Compliance Alert

THE THIRD DEGREE: Reader Questions Answered

From the HHS Office for Civil Rights' most recent interim final rule outlining the agency's HIPAA enforcement role in the upcoming months to concerns over notices of privacy practices documents, you've been up to your ears in HIPAA this month. The good news is that we're listening. Take a look below at some of your colleagues' questions and concerns; they should help save you some time and effort.

OCR CLAIMS TO WORK WITH - N**OT AGAINST - ENTITIES**

Question: "The OCR's [interim final rule] on enforcement didn't give our practice a clearer picture of the likely direction enforcement will take. We're a small physician practice without many resources at our disposal for HIPAA compliance. How can we develop a plan of action to avoid civil money penalties?"

Answer: In its guidance published in the Federal Register April 17, the OCR said it would not proactively seek out violators of the privacy rule. However, if they do receive a complaint, "they're going to investigate it to determine whether or not there's been a violation and what's been done to correct it, as well as if there needs to be a corrective action plan - then they will get one of those in place," informs **Brian Gradle** with the Washington office of **Epstein Becker & Green.**

Gradle tells **Eli** there are affirmative defenses against civil money penalties. For example, "if one has taken steps to address the problem within 30 days, that's an affirmative defense. If one wasn't aware there was a violation and wouldn't reasonably have known that it was a violation, that's an affirmative defense as well." Gradle says the best defense against CMPs is simply to avoid breaking the law, but if you do break the rules and you do your best to fix it, it's likely the OCR will work with you and not against you.

U**SE COMMON SENSE WITH NPPS**

Question: "Required notices sent by financial institutions - such as the Gramm-Leach-Bliley notices concerning information-collection and data-sharing - were often printed in very small fonts. Does HIPAA have a minimum font size for NPPs?"

Answer: According to **Robyn Meinhardt** in the Denver office of **Foley & Lardner**, HIPAA doesn't regulate the font size for your notice of privacy practices. However, she cautions covered entities to consult local and state laws to see if there is a minimal font requirement for such notices. States like California have recently passed legislation that would require documents such as NPPs to be printed in a 12-point font, she reports.

"I've seen people that - in order to make their NPP shorter - have put it in a microscopic type, like 8-point font," she remarks. You might not get cited with a HIPAA violation for doing this, she states, but you do run the risk that patients will nonetheless complain to the OCR, which may in turn order you make your NPP more legible.

T**WO QUESTIONS HELP CREATE A BA AGREEMENT**

Question: "We're a small hospital and we have several business associate agreements contracts in place, but we're not always sure whom to contract with and what would constitute a business associate. Is there an efficient and easy way to determine the necessity of a BA agreement?"

Answer: Yes, there is. **Martha Baxter**, an attorney in the Columbus office of **Bricker & Eckler** says there are a couple of threshold questions you should ask yourself when wishing to determine what qualifies as a BA: **(A)** does the business

perform or assist in the performance of an activity or function involving the use or disclosure of protected health information? or **(B)** Does the business provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services that require the disclosure of PHI from the physician? If you answered "yes" to either of these questions, then a business associate agreement may be needed.

Baxter tells **Eli** clients often ask her about service people who come into a covered entity to work on, say, an MRI or the CE's laser equipment, and those technicians might stumble across some PHI in the process. "Well, that's incidental to the agreement," she emphasizes, and a BA agreement wouldn't be required. "But if you're contacting a software vendor and that vendor will need to look at PHI in order to undertake their audits or develop the software, then they will be a BA."

Caveat: Baxter says some CEs are sending BA agreements that aren't needed. "Nursing homes often send BA contracts to hospitals when it's really just for treatment purposes," and BA contracts aren't required in that situation. She advises CEs to thoroughly examine their own circumstances before creating a BA agreement.

Editor's Note: If you have questions of your own you'd like to have answered, submit a post on our discussion group! Be sure to include "HICA reader question" in the subject line.