Health Information Compliance Alert

The Third Degree: READER QUESTIONS ANSWERED

Thanks, HICA readers! We've received several great HIPAA questions this month. Now, thanks to a bevy of brainy experts, you'll get your answers. Take a look at what some of your colleagues have asked about, and see how HIPAA experts interpret the regulation.

Security: Hire Another Officer?

Question: We're a small health care provider, with only a privacy officer and no security officer. Do we need to hire a security officer to begin our compliance efforts with the security rule, or can our privacy officer do double duty?

Answer: That depends on the individual and the size of the organization, says **Robert Markette**, an attorney with **Gilliland & Caudill** in Indianapolis. With a large entity, the privacy officer's going to have a lot of work to do, and it may be asking too much to also put them in charge of security rule compliance when they're also going to be managing day-to-day privacy issues. For larger entities that may have a risk management department, Markette says such organizations "may find that that's where you pick the security officer from."

And though some entities may simply want to give the privacy officer a break and hire someone new, others may be small enough with so small a staff that they can't help but to appoint the privacy officer as the security officer too.

Essentially, this all depends on the size and technical infrastructure of your organization, but Markette feels that privacy officers will play a role with security no matter what. "There are a lot of privacy officers out there that are about to become a security officer, just because you're stuck there, everyone knows your name now, and they associate you with HIPAA. You're kind of trapped." Whatever you decide, you're going to have to have somebody who understands what HIPAA requires on the regulatory side of things to guide the IT people, he advises.

User Identification and Sharing PHI

Question: Regarding the security rule's user identification requirements: If one wanted to have a limited read-only report containing PHI on a PC screen, and all that was displayed on the PC screen was the report - the PC was in a secured area, was logged on with an ID and password only for that PC, PC use was logged and was only used by certain staff, et cetera - would this be a definite violation of the requirements?

In this case, the information would be read-only and only accessed by key staff, but you would not know which staff specifically accessed it and when. What does HIPAA have to say about this?

Answer: "This is the one place the guidance for the final [security] rule differs from the proposed rule," says **Fred Langston**, CISSP, senior principal consultant with **Guardent** in Seattle. With respect to the proposed rule, this would have been a violation, but due to input from nursing groups that work in hospital environments like ERs and CCUs, the user identification rule has been relaxed to allow for group accounts shared in this environment.

This kind of arrangement can't be just for convenience, warns Langston; it should be driven by a business' functional need and would require all the elements the reader described.

Lab-to-Lab Services and HIPAA

Question: We have an in-house lab and we can handle most specimen tests ourselves. However, some tests must be sent to larger outside labs with more sophisticated equipment. This other lab has said that we don't need a business associate agreement. The lab may very well be a covered entity. Our position is that they are a CE once the specimen is in their possession. What do you recommend?"

Answer: Labs are considered indirect providers under HIPAA, says **Robert Markette**, an attorney with **Gilliland & Caudill** in Indianapolis. "As a treating provider, you're providing health care. Covered entities are allowed to share PHI with health care providers whether or not they're covered by HIPAA if it's for the purpose of treating the patient. If one lab receives a sample but can't analyze it and refers the sample to another lab, it's no different than a doctor - let's say a primary care physician - referring a patient to an oncologist or whatever. It's all treatment. The second lab is right - they're not a business associate, they're a health care provider, and there's no need for a BA agreement" in that situation.

HIPAA Not Child's Play For Pediatric Offices

Question: Can we fax absentee notes and forms authorizing the administration of medications directly to schools or camps?

Answer: No, except in the event of an emergency, say Drs. **Charles Scott** and **Benjamin Rosenblum** with **Children's Health Associates** in Trenton, NJ. These forms would be faxed to a central administrative office where many people may have access to them, and that could easily create a violation of confidentiality.

"We prefer that you give these forms to the patient or parent either in the office or by mail. They can forward the forms to the school," they advise. Scott and Rosenblum say the least preferable choice would be to fax the forms to the parent because of the possibility of faxing to a wrong number. "We feel that it is permissible to fax such forms to a school if the child is at school and the school needs immediate permission to administer a medicine or to let the child back into classes. If you fax an absentee note to the school, we suggest that you note only that the child may return to school and not give a specific diagnosis," they tell **Eli.** For example, write that "Johnny is medically cleared to return to school," and disclose only the minimum necessary information on any of these notes, they recommend.