Health Information Compliance Alert

HIPAA Compliance: Are You Complying With New Health Record Access Rules?

Indecent disclosure: Why access report requirements are nothing to sneeze at.

New HIPAA rules and HITECH Act provisions are giving patients more and more ownership over health records. Don't let these new provisions for disclosures and individual access land your organization in hot water.

You always need to have a process for people to ask for copies of the information in their designated record set (DRS), says **Jim Sheldon-Dean,** director of compliance services for Charlotte, VT-based **Lewis Creek Systems, LLC.** And you must have a reasonable cost-based fee for furnishing the copies.

For instance, if a patient wants to get a copy of his records, you would give him a copy of whatever is in his DRS, Sheldon-Dean says. And if the patient wants to amend his records, you would amend whatever records exist in the DRS.

Heed New Rules for Electronic Copies But Tread Carefully

These "new rules" include interim and proposed rules that were finalized in the big HIPAA Omnibus Update, published on Jan. 25, 2013; effective on March 26, 2013; and enforceable as of Sept. 23, 2013. The Omnibus Update included new rules under both the HIPAA Rules and the HITECH Act. The Update is published in the Jan. 25 Federal Register at www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

But now, if you keep DRS information electronically, you must honor requests for copies of that information in an electronic format. If the patient asks, you need to have some way of giving the information to him electronically, "whether it's on a CD or as an email attachment or a memory stick or through a portal or however," Sheldon-Dean explains.

"You can't just say, 'Oh no, we only give out paper copies,'" Sheldon-Dean cautions. If you're keeping electronic information, you must give patients a copy electronically when requested.

Problem: You know there's no excuse for not encrypting professional-to-professional emails, but what if a patient asks for a copy of their protected health information (PHI) via an unencrypted email? What if the individual says, "I want you to just email this information to me, and I really don't care whether it's encrypted because I don't think it's really sensitive information."

Solution: You can't just outright deny or agree to a request like this. You need to have a discussion with that individual, Sheldon-Dean says. You need to discuss with the patient what kind of information you're emailing regular medical records, a test result, HIV information, or reproductive health information, etc. and explain the risks.

And you need to talk through and perform a risk analysis with the patient (see Health Information Compliance Alert Vol. 13, No. 1, page 1 for more information on risk analyses). The patient can't just say, "I don't care about this just email it to me anyway," according to Sheldon-Dean. The individual needs to tell you, "Okay, I understand what my risks are and I think that's acceptable." The person must give you an informed risk decision.

Define the Scope of Your DRS

Another problem is understanding what's on the DRS and where all that information resides. And this is not just your formal electronic health record (EHR) — "also you may have Excel files or access databases or Word documents," Sheldon-Dean notes. Any information — no matter if it resides in the EHR or elsewhere — that you're using to make decisions about the individual is part of the DRS.

Crucial: "So you need to understand where is your [DRS], how big is it, what are the limits of it," Sheldon-Dean urges. "Because the more you can define that information, the easier it is to be able to provide individual access."

Remember: Also, because the electronic access provision is new, you'll need to update your Notice of Privacy Practices (NPP) accordingly.

What You Must Include in an Access Report

If somebody wants an accounting of disclosures (also called an access report) — what information might have been disclosed to some other organization — that applies to the information in the DRS, Sheldon-Dean explains. You could have other information that is PHI associated with the individual "but maybe it's for purposes of internal audits or internal reviews or quality improvement" — that's not in the DRS.

"The new access report does not distinguish between a use (think internal use by a health care provider) and disclosure (providing the information to a third party)," attorney **Bob Coffield** of **Flaherty Sensabaugh Bonasso PLLC** wrote in his Health Care Law Blog. "Instead the new right to an access report focuses on whether someone 'accessed' the information in the EHR."

"Previously under HIPAA, uses and disclosures for treatment, payment, and health care operations (commonly referred to as 'TPO') were exempt from the accounting of disclosures requirements," Coffield said. "The requirement for accounting for some limited uses and disclosures has always been part of the HIPAA Privacy Rule."

Bottom line: Under the new rules, you must widen your scope when providing an access report/accounting of disclosures to patients. If you haven't already, you should evaluate the capabilities of your systems to ensure that you can properly produce this type of report.