HealthBlawg :: David Harlow's Health Care Law Blog

OCR HIPAA Audits Finally Kick Off - Do They Matter?

Posted: 09 Nov 2011 05:07 AM PST

The HITECH Act called for stepped-up **HIPAA privacy and security and breach notification rule enforcement** with respect to covered entities and business associates, to be accomplished by spot-check audits. This month, the first 20 of a planned 150 audit subjects will be getting notices from the U.S. Department of Health and Human Services Office of Civil Rights' contractor, KPMG, saying that their numbers are up. These early test cases will be a proving ground for the auditors and the audit process, as much as for the covered entities to be audited (no business associates in the first 20, or even in the whole batch of 150, apparently). The first round of 20 audits -- and a review of the audit protocols -- is slated to take about five months. Up to 130 other audits will follow, in the final eight months of this pilot. Each audit is supposed to take about 30 business days, and will include on-site interviews and investigations. Document requests are to be turned around in ten days, and KPMG will give 30-90 days advance notice of site visits. In theory, audits may bring to light issues that do not surface in the course of complaint investigations, and are expected to yield OCR guidance and highlighting of best practices.

Will this audit program change behavior of covered entities and business associates?

In general, the regulated community seems to get a free pass for about a year after a new regulatory schema is rolled out, before real enforcement kicks in. It's been longer that for HIPAA (well, most of HIPAA, anyway), and there have been enforcement actions initiated by the federales (and by **state attorneys general under the HITECH Act**). Many of these enforcement actions -- largely initiated by complaints filed by the public -- have generated more heat than light. (Consider the **Harvard teaching hospital and its paper records left on the subway, or T**; consider the judgment-proof, bankrupt incompetence of a **company that couldn't, or wouldn't, provide requested information to patients**, led by someone who perhaps whould not have been allowed to hold such a position. Is either a relevant example that will cow an otherwise recalcitrant covered entity or business associate into compliance?) The "**Wall of Shame**" reports of significant data breaches, as a whole, do not seem to have motivated behavior change -- behavior change like encrypting a laptop or portable hard drive containing protected health information, for example, which encryption would mean its loss would not have to be reported on the Wall of Shame. In sum, since the reputational and operational dislocations caused by reportable breaches to date have not yielded a significant change in behavior by covered entities and business associates, generally, it is unclear whether a small-scale -- or even a large-scale -- audit program will yield meaningful increases in HIPAA compliance. Living through a reportable data breach, and fixing privacy and security policies and their implementation after the fact, is probably at least as

painful as going through an OCR audit, yet many covered entities have yet to adopt and implement data encryption and other policies and procedures that would eliminate the possibility of that happening to them.

Here's hoping we don't have to wait until after December 2012 to get some guidance and best practices from the auditors based on their work. Will we see an army of HIPAA auditors in 2013? And when will OCR start auditing business associates?

The $64,000 question is: Will all this have an impact on the privacy and security of protected health information (PHI)?

I am skeptical, at best. ONC is rolling out an educational message to let individuals know more about privacy and security and that, together with hiring bands of auditors, may build towards having some effect. But we need to consider the range of data whose release would be considered a data breach, and perhaps revisit the general approach. It may be that the default setting for some information should be public, or that some easy sharing options should be built in. Consider the "**green button**" and "**rainbow button**" initiatives (riffing on the VA's **Blue Button**). Rolling out these initiatives could have the effect of lessening the amount of data that must be kept 100% private and secure, and could have some beneficial effects, as well. Finally, consider the **radical proposal to reverse the presumption of privacy** entirely.

While we are not yet in a utopian society where release of health information will have no negative effects on an individual (think: employment, insurance, to name two key domains where this is an issue), perhaps we could devote more resources to reaching that ideal, and fewer to the ultimately futile attempt to assure 100% compliance with the privacy and security requirements applicable to an ever-increasing universe of PHI -- because not only is the volume of data out there ever-increasing, but information that may be considered de-identified (and therefore beyond the reach of the regs) today, may become easily re-identifiable tomorrow as more and more data, from diverse sources, is shared on line.

Meanwhile, metaphorically speaking, be sure the doors and windows are locked before KPMG and OCR come knocking.

David Harlow
The Harlow Group LLC
Health Care Law and Consulting