HIPAA Omnibus Rule - Google+ Hangout

Posted: 23 Jan 2013 08:38 PM PST

For a first look at the **HIPAA omnibus rule**, I had a Google+ Hangout on Air with **Brian Ahier** and **Deven McGraw** this afternoon. We talked through the changes made to the privacy and security rules, the breach notification rule, the enforcement rule, and the harmonization of HIPAA and GINA. The video runs about an hour, and we got some pretty good reviews live and in the hours since this ran. Check out the **HIPAA discussion on Google+** concurrent with and immediately after the hangout, too.

HIPAA Omnibus Rule Hangout (click to watch)

One viewer, Ben Watts, posted his notes almost immediately after we were through, on his blog **EMRSoap**. (Thank you, Ben!) Here's an excerpt from his post:

EMRSoap Write-up of the HIPAA Hangout by Industry Leaders

Below are our notes from the discussion – they're not specifically tied to the individual speaker.

- Most of the final rule was the same. Except for the Marketing provision – that was quite a bit different than the proposed rule.
- We're still not done. Even though this is the 'Omnibus rule', there's still 2 new rules that need to come out.
- Bus related puns abound.
- What do providers need to watch out for? One thing: Primary liability of BA's and subcontractors. You really can't sub out responsibility entirely.
- There's a community of small providers and Business Assocaites who aren't aware of the reality of HIPAA and haven't completed Risk Assessments (and more). They're just not familiar enough with their obligations and the HIPAA environment. They'll have till September 23rd to comply with this rule.
- Date by which new BAA and NPP need to be entered into is a year after that September 23rd. The agency will be issuing further guidelines throughout this timeline.

- The government is committed to more audits and fines. The fines they collect will fund the audit process. We're going to have audits of Business Associates and their subcontractors, not just Covered Entities.

- Enforcement is moving to Penalty base, and away from voluntary compliance.

- But not entirely, says Devin. Rule was pretty clear – informal resolution and voluntary compliance would still play a factor in enforcement. HHS will have discretion.

- HHS has been going after the smaller groups as well, even without the Omnibus rule.

- Environment of 'Hands off' has led to people being careless. Behavior has been beyond what's acceptable for building up trust in EMRs.

- Why should patients be excited? People most bugged by marketing – that'll be limited by HIPAA Omnibus rule. Also, breach notification provision much more clear means that institution are going to pay a lot more attention to encryption.

- Discussion on the 'conduit' exemption – very narrow exemption. Really only works for courier-like firms (ISP and postal services, for example). Only making sense in cases of random or intermittent access to ePHI. As opposed to entities that store data – would be a BA, even if the intention is to not to look at it.

- Failing to sign a BAA doesn't exempt you from BA status.

- Researchers are now permitted to give people conditional treatment if they agree to research.

- Now allowed to have authorizes for future research as long as the description is rich enough to give patient a general idea of the types of research that'll be enacted. No need for individual study approval. Requirement is somewhere in between 'all research' and 'one study'.

- Patients can request records in forms that makes sense for them. If you can't technically do it in the form (5.5 in floppy, for example?) then the provider will have to reach an agreement with the patient.

- Is it possible to segment your record, and keep some info off of your Health record? Yes. It'll probably be hard for a fair amount of providers. If a patients says 'don't send this to my payer', you can't do it.

- Patient right to get data trumps security requirement. If the patient is notified of risks of transmitting ePHI over email, then the ePHI can be transmitted to the patient. Requirement of alerting patients is fairly low. Bi-lateral communication is a different realm, however.

- Changes to enforcement rule – bottom line is there's a max of 1.5 million per violation. Likelihood of greater fines in the future? Maybe. Largest fine to date was against a bankrupt company.

- There's more breaches reported...not necessarily more breaches in total. Now, with our digital health system, we know who's seen what. We'll see more breaches in total, but that's not necessarily a bad thing.

- BA's right to use data is explicitly limited. BA's are directly liability, but they're still subordinate to Covered Entities.

- Breach Notification – we've moved away from the 'harm standard' – moved away from the subjective value of the underlying data. We've moved to an examination of 'what happened in this instance?' Presumption being if we don't know what happened, then there was a breach. Notion of 'if it's info about your big toe then it's not harmful' is gone, as is underlying subjective value judgment of data. Faxing info to Doctor X instead of Doctor Y, maybe less of a big deal. As long as that mistake is handled appropriately, it's not that big of a deal. If there's greater than a low probability that the ePHI was breached, then there needs to be a notification. There's a 4 pronged set of standards that need to be examined in that investigation to determine if there was a breach. But if you know that there was a breach, you don't need to do an investigation.

- Everybody: gotta revise your Notice of Privacy Practices. Remember that you have until September.

We enjoyed using the Google+ Hangout on Air platform, though it was a little bumpy as it was our first time. We are considering putting together future hangouts on the HIPAA omnibus rule, and would welcome your input regarding which issues warrant a closer look.

David Harlow
The Harlow Group LLC
Health Care Law and Consulting