FierceHealthIT

Uncertainties surround new HIPAA breach notification rule

January 29, 2013 | By David Harlow

- **Comment**
- **Print**
- **Contact Author**
- **Reprint**

The federal government finally published the HIPAA Omnibus Rule, including, in final form, revisions to the Privacy and Security Rules (including GINA-related amendments), the Enforcement Rule and the Breach Notification Rule. The rule will be effective in 60 days (late March), and the compliance date is 180 days out (late September). We have six months to get used to the new rules, and the Office of Civil Rights at the U.S. Department of Health & Human Services will not begin enforcing the new rule until then (with an additional year grace period for revisions to be made to Business Associate Agreements and Notices of Privacy Practices that are already in the wild). You may find an introduction to the HIPAA final rule on my home blog, *HealthBlawg*, complete with a video of a Google+ hangout on air.

While there is much to say about the broadening of the definition of business associate, the new obligations of business associates and their subcontractors, increased protections provided to patients (in terms of being able to opt out from marketing communications and being able to request records in formats most convenient for the patient), enforcement changes (fines of as much as $1.5 million per violation may be imposed in some cases) and more, in this post I will focus on the breach notification rule.

Some of you will recall that the Breach Notification Rule was published as an Interim Final Rule in 2009, with a "harm" standard, and was pulled by the agency after some negative comments came in (including several from members of Congress, who noted that they had considered, but rejected, the idea of a harm standard in the law). The harm standard proposed would have required notice of a breach of privacy or security--i.e., an unauthorized release of protected health information--to be given to the data subject (the patient) if the breach posed a significant risk of financial, reputational or other harm to the individual. The thinking behind the harm standard was that individuals might otherwise be flooded with breach notifications about inconsequential breaches, and that anxiety and, eventually, apathy would ensue.

The IFR required a risk assessment to be done in order to determine whether the risk of harm was present. The feds observe in the commentary to the final rule that some folks "may have interpreted the risk of harm standard in the [IFR] as setting a much higher threshold for breach notification than we intended to set." Hence the "clarification" in the final rule that:

> "an ***acquisition, access, use, or disclosure*** of protected health information in a manner not [otherwise] permitted ***is presumed to be a breach unless*** the covered entity or business associate, as applicable, ***demonstrates*** that there is a ***low probability that the protected health information has been compromised based on a risk assessment*** of at least the following factors:
>
> > (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
> >
> > (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
> >
> > (iii) Whether the protected health information was actually acquired or viewed; and
> >
> > (iv) The extent to which the risk to the protected health information has been mitigated.
>
> 45 CFR 164.402 (emphasis added)."

This revision is intended to provide a more objective standard, in response to comments filed in connection with the IFR. (See comments filed by the Markle Foundation and the Center for Democracy and Technology.) Thus, the default assumption is that any irregular release of PHI is a breach, with no subjective standard of harm getting in the way. The covered entity or business associate unfortunate enough to have suffered this breach may either (a) immediately acknowledge that it is, in fact, a breach, and rev up the notification machinery (notice to data subjects, the federales--possibly for posting on the Wall of Shame--and the press, as appropriate, based on the size of the breach) or (b) decide that a risk assessment is necessary, and begin its assessment of at least the four factors highlighted in the regulation.

The factors to be examined are commonsensical ones. A release of PHI that consists of a list of discharge dates and diagnoses would probably not be a breach (unless we're talking about a community hospital in a very small town, where just that information would be enough for someone in the community to tie individuals to diagnoses). A release to another covered entity, though the release is inappropriate, is probably not a breach, since the second covered entity is bound to keep such information private and secure, and in most cases may be trusted to do so.

A lost unencrypted recovered hard drive that is recovered and shown by forensic analysis to have remain unexamined (so the PHI was not compromised) while on holiday would not be considered the source of a breach. If a confidentiality agreement could be executed with the third party who improperly received PHI, then perhaps that release would not be considered a breach either. All of these examples are presented

in the final rule as examples of situations where there is a low probability that PHI has been compromised, based on a risk assessment.

Given the uncertainties surrounding the new rule, and how close the new and improved objective standard comes to the subjective "harm" standard of the IFR, covered entities and business associates may be inclined to forego the risk assessment and report any breach, despite the attendant publicity, rather than risk a double whammy in enforcement for failure to report a breach, in addition to failing to maintain the privacy and security of the PHI in the first place.

Of course, the best approach to this situation would be to avoid it entirely: by encrypting data and by limiting the use of removable media.

Have you experienced a breach within your organization? Has one of your business associates had a breach that affected you? Do you think the final rule will make life easier on the breach notification front? Let us know what you think in the comments.

David Harlow, a member of the FierceHealthIT Editorial Advisory Board, a healthcare attorney and consultant at The Harlow Group LLC in Boston, MA. He writes the award-winning HealthBlawg. Follow him on Twitter.