HIPAA Omnibus Final Rule – What's in it for Patients?

Posted: 01 Feb 2013 01:34 PM PST

After years of delay, the federales ***finally*** finalized the HIPAA Privacy, Security, Breach Notification and Enforcement Rules.

Introduction

The Final Rule offers significant changes to patient rights and patient protections. (There is much more to the rule, but other aspects are not addressed in this post. Here you may find a link to the **HIPAA Omnibus Rule**, a Google+ Hangout taking a first look at the rule as a whole, and a bullet-point summary of the hangout; here you may find a piece I wrote on the **Breach Notification Rule**. Some work remains to be done on other parts of the HIPAA rules, such as the accounting of disclosures provisions.)

Before detailing the patient-focused changes, a bit of broad-brush background is in order. The original HIPAA privacy and security rules are all designed to protect the privacy and security of "protected health information" (PHI) of individual patients. PHI may be shared among health care providers and payors (and health care clearinghouses - a type of claims processor) (collectively, Covered Entities or CEs) for purposes of treatment, payment and operations (TPO) without asking patients for permission. Any other use or disclosure of PHI requires patient consent. Some CE operations require dealings with Business Associates (BAs) -- entities that are not CEs, but that end up using PHI to help CEs carry out their TPO responsibilities (e.g., medical records vendors, billing companies, etc.). Every CE is required to give patients a Notice of Privacy Practices (NPP) and to enter into a Business Associate Agreement (BAA) with each of its BAs, under which the BA agrees to maintain the privacy and security of PHI.

The amendments collected in the Final Rule are promulgated under the HITECH Act (the portion of the 2009 Recovery Act that also funded the Meaningful Use EHR incentive program) and GINA (the Genetic Information Nondiscrimination Act of 2008). The amendments under the HITECH Act added additional privacy and security protections to HIPAA in order to allay concerns that, with the promotion of more widespread use of electronic health records, there would be more opportunities for breaches of the privacy and security of PHI. Amendments under GINA harmonize HIPAA regulations with GINA regulations.

So, without further ado, here are the highlights:

Business Associates are held to the same strict standards as Covered Entities

Business Associates and their subcontractors are now directly responsible for compliance with HIPAA, not just responsible for signing a BAA. They will now be subject to **OCR HIPAA compliance audits**, just as CEs are, and should be undertaking risk assessments in order to ensure that their privacy and security compliance is up to snuff. BAs have always been responsible for compliance under their BAAs, but some BAs, particularly smaller ones, probably have not focused enough on HIPAA compliance. Now they will have to because they are fully accountable -- they can be audited and fined, just like the Covered Entities.

The definition of BA is expanded

Business Associates are now defined to include a broader array of contractors that store and touch PHI -- including, for example, document storage companies and other contractors that "maintain" PHI, even if they do not actually view the information in their possession.

Use of Protected Health Information for marketing is limited

Covered Entities may not send marketing materials to patients on behalf of third parties if the communication is paid for by a third party whose products or services are being promoted. Several exceptions to this rule that applied in the past, whether or not the communication was funded by a third party (i.e., communications about (i) treatment, (ii) a health-related product provided by, or covered by a benefit or insurance plan issued by, the CE making the communication, or (iii) case management, care coordination or treatment alternatives) now apply only if the communication is funded internally by the CE.

Sale of PHI is limited

PHI may not be sold, licensed, or accessed in exchange for giving anything of value -- with a handful of exceptions. PHI may be disclosed in exchange for remuneration (i) for public health purposes, (ii) for research, so long as payment is limited to the sending CE's costs, (iii) for treatment and payment, (iv) in connection with a sale or merger of the CE, (v) to or by a BA where the CE is just paying for the BA's services, (vi) to a patient who requests access to his or her own PHI, (vii) as required by law or (viii) as otherwise permitted under HIPAA where the remuneration covers costs only.

Use of PHI for fundraising is limited

On the one hand, nonprofit health care providers can target their fundraising efforts by using PHI that clues them in to what services were provided to which patients. On the other hand, each contact must allow a patient to opt out of all future fundraising communications.

Use of PHI for research is simplified

A single consent for release of PHI in connection with research study participation can now cover future studies done using the same data. In addition, clinical trial consents can now be combined with retrospective data review consents. (If you like being a lab rat, you won't have to sign as many data release forms.)

Use of genetic information for insurance underwriting purposes is banned

As required by GINA, genetic information may not be used for health insurance underwriting purposes. Thus, genetic information is now included in the definition of PHI. In addition, the underwriting ban is carried forward into regulation. However, genetic information *may* be used in long term care insurance underwriting decisions.

Patients may access PHI electronically

Upon request, a CE must provide a patient or an authorized representative a copy of a requested medical record, in the format requested, within 30 days. If, or some reason, the 30-day timeframe is unworkable, the regs give CEs an additional 30 days. If the CE cannot produce the records in the format requested by the patient, the parties need to get together and agree on a workable compromise solution. Previously, the patient had to make do with whatever format the CE produced (often a paper printout), and had to allow 60 days plus 30 days for tough situations. So there is some progress here. Of course, a CE that is in compliance with the Meaningful Use regulations for EHR implementation is required, in Stage 2, to provide records to patients electronically within just a few days (though **the Society for Participatory Medicine called for immediate patient access to EHR information** - as soon as a clinician who did not author the entry can see it, the patient should be able to see it).

Patients may restrict disclosure of some information

If a patient pays for a particular service out of pocket, he or she may require that the provider not disclose any information about the service to the patient's health plan. Providers are required to advise patients about potential inferences that payors can make based on other services provided (e.g., "If you pay for lab test A out of pocket, but have us bill your health plan for tests B, C, D and E, your health plan will be able to figure out that you had test A done as well.") If a visit that a patient pays for out of pocket will generate a prescription, the patient would be well-advised to ask that prescriptions be written by hand, so that no electronic notice of the prescription will get to the health plan. In a perfect world, sharing of treatment information with one's health plan would not be problematic, but some patients have legitimate concerns about the use and misuse of such information by employers, health insurers, life insurers and others.

The **HIPAA Omnibus Rule** was published on January 25, 2013. It is effective 60 days later, and (with certain exceptions) regulated parties must come into compliance within 180 days after that, or September 23.

What do you think?

What do you think? Was this rule worth the wait? Are your pet peeves addressed by the final rule? Let us know in the comments.

David Harlow
The Harlow Group LLC
Health Care Law and Consulting

This post first appeared on ***e-patients.net****, the blog of the* ***Society for Participatory Medicine****. David Harlow chairs the Society's Public Policy Committee.*