HHS Issues Proposed Updates to HIPAA Privacy Regulations

by Harley Geiger [1]
July 9, 2010

The U.S. Department of Health and Human Services (HHS) proposed [2] a set of significant updates to health privacy rules yesterday. The proposed rule tackles how sensitive patient information is handled under Health Insurance Portability and Accountability Act (HIPAA), which is the nation's foremost health privacy law.

Although the proposed rule does not clarify some outstanding issues in the health information technology (health IT) area, CDT is encouraged that HHS' proposed rule would strengthen patient privacy, data security and enforcement of the law. One area of the rule that stands out in this regard is the new privacy and security requirements for business associates and subcontractors.

Strengthening Subcontractors' Privacy Practices

Under HIPAA, "business associates" are organizations or individuals that perform activities involving patients' personal data on behalf of health care providers and other "covered entities." Historically, business associates were not directly accountable for complying with HIPAA privacy and security requirements. Instead, the law required covered entities and business associates to enter into specialized contracts – called "business associate agreements" – that contained certain patient privacy protections. However, the protections in the business associate agreements were still generally less comprehensive than those covered entities themselves were required to follow under HIPAA.

The HITECH legislation largely eliminated that gap. HITECH required business associates to comply with most of the same privacy and security requirements as covered entities when they handle protected health data and made them directly accountable to federal and state authorities for failure to comply. However, the HHS proposed rule treats subcontractors as business associates. Under HHS' proposed rule, business associates must enter into business associate agreements with any subcontractors the business associates hire to handle patient data – and those subcontractors can also be held directly accountable for failure to comply with HIPAA rules .

This change focused on one of the more troubling problems in health privacy – that legal privacy safeguards diminish as patient data is handed off from covered entity to business associate to subcontractor. HHS' proposal takes a very positive step towards strengthening patient privacy as it flows downstream.

Partial Clarity on PHRs

However, more work needs to be done. One issue not fully addressed in the proposed rule is establishing consistent rules for personal health records (PHRs). A PHR is essentially an electronic tool that enables consumers to store, manage, use, and share their personal health information. A key characteristic of PHRs is the high degree of control the individual consumer – not the health care provider – has over how the data is used.

The privacy rules for PHRs are a gray area. PHRs can be broken into three general categories, each with somewhat different legal responsibilities:

- PHRs offered by covered entities, like health insurance companies, that are subject to HIPAA,
- PHRs offered by entities that are not covered under HIPAA, such as software manufacturers, health websites and search engines,
- and, most confusing, PHRs that are partnerships between entities covered under HIPAA and entities that are not.

The HITECH legislation partially clarified the third category. HITECH stated that organizations offering PHRs on behalf of covered entities are now considered business associates. This is a positive step, as it formally requires this class of PHRs to enter into business associate agreements and abide by the privacy protections the law compels the agreements to contain. However, the proposed rule merely formalizes the HITECH requirement without shedding light on exactly when the business associate relationship is established in these circumstances. CDT would like greater official guidance on what factors HHS believes trigger business associate requirements for PHR vendors.

The second category of PHRs – those offered by entities not covered under HIPAA – still lacks privacy and security rules tailored to their unique services. However, patients consistently report [3] high levels of concern for the privacy of their data. HITECH requires HHS and the Federal Trade Commission to undertake a study on this very issue, which the agencies are still developing. In coming days, CDT will release a paper recommending privacy protections for PHRs.

Finally, HHS' proposed rule did nothing to alter the "harm standard" for data breach notification that the agency established in an August 2009 rule [4]. Under the harm standard, a health care company does not need to notify patients when it loses their data so long as the company determines that the breach poses no "significant risk of financial, reputational or other harm" to the patient. This determination is an internal assessment on the part of the company, which has financial and reputational incentives of its own to avoid having to report the breach. CDT wrote extensively of the deep flaws in the harm standard in a blog post [5] and in its comments [6] to the 2009 rule.

All That and Then Some

This article focused on two issues related to HHS' proposed rule, but the proposal actually contains numerous changes to health privacy regulations, most of which are quite positive. The rule is open for public comment for the next 60 days, and CDT intends to file a set during this period. Although the rule is not as comprehensive as CDT would have preferred, it is refreshing to see HHS begin to take its commitment to patient privacy to another level. We hope it continues.

- PHRs
- hipaa
- HHS
- Health Privacy

Source URL:
https://cdt.org/blogs/harley-geiger/hhs-issues-proposed-updates-hipaa-privacy-regulations

Links:
[1] https://cdt.org/personnel/harley-geiger
[2] http://www.healthitlawblog.com/stats/pepper/orderedlist/downloads/download.php?file=http%3A//www.healthitlawblog.com/uploads/file/NPRM%2520July%25202010.pdf
[3] http://www.chcf.org/~/media/Files/PDF/C/ConsumersHealthInfoTechnologyNationalSurvey.pdf
[4] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html
[5] http://cdt.org/blogs/harley-geiger/hhs-new-harm-standard-breach-notification
[6] http://www.cdt.org/files/pdfs/CDT&MarkleComments.pdf