Feds Boost Privacy Protections for Medical Records

by Deven McGraw [1]
January 25, 2013

The privacy protections guarding the care and handling of your medical records just got stronger… a lot stronger.

The new rules bolster prohibitions against use of a patient's medical records without consent for marketing communications; extend federal privacy and security protections to contractors (and subcontractors) of doctors, hospitals and insurers; improved your right to be notified when your medical records are lost, stolen or otherwise compromised; and clarifies your right to receive a copy of your medical records when you ask for it.

The new protections stem from the long-awaited final regulations to implement most of the improvements [2] to federal health privacy protections enacted by Congress in the HITECH provisions of the 2009 economic stimulus legislation.

CDT is elated with the release of the regulations, despite a two and half year delay [3]. We submitted comments [4] on the proposed regulations, which were issued in July 2010. The final regulations adopt many of the approaches we've recommended.

New Rule Highlights

Over the coming weeks, CDT will be publishing in-depth analyses of selected topics in the regulations, but here are highlights of the more noteworthy changes:

- Under the old rules, if your medical records were lost or stolen or somehow compromised, those responsible for the security of your records didn't have to notify you unless there was a “significant risk” you would be “harmed” by the incident. Under the new rule, individuals will have the right to be notified of security breaches of unencrypted health information unless there is a low probability that the information was “compromised.” Subjective judgments are no longer part of the calculation when deciding whether or not to notify patients.

- Under existing HIPAA regulations, health data can be used without patient consent for marketing communications urging them to use a particular product or service. Under the new regulations, patients must first approve the use of their data for marketing communications if the maker of the product or service pays for that sales pitch. This is an important privacy protection, aimed specifically at addressing patient concerns about their personal health information being used for marketing without their consent.1 However, information gleaned from health records about any medication a patient is using can be used for subsidized marketing purposes as long as the payment for the communication is reasonable and does not generate a profit for the sender. In addition, face-to-face communications to patients about products and services are not considered marketing under long-standing HIPAA provisions.

- HIPAA doesn’t protect all health data, but its scope of coverage was expanded by HITECH – and the final rules put that expansion into effect. Individuals or persons who handle patient health information in order to perform services for an entity covered by HIPAA (doctors, hospitals, health plans) are also now accountable for complying with the HIPAA Privacy and Security Rules – and this accountability extends to any subcontractors that access data to help perform those services.

- The final rule clarified patients’ rights to receive an electronic copy of their health data, and to have that copy sent, at their request, somewhere else, for example, to a doctor, a

caregiver, or a personal health record or mobile health app. The rule also clarified that patients have the right to receive electronic copies by insecure e-mail. Unfortunately, the final rule still allows entities covered by HIPAA to take up to 60 days to provide patients with requested records; however, the rule does encourage faster response when feasible.

The final rules are effective March 26, 2013; entities covered by the rule have another 180 days to comply with most provisions.

This final rule implements most of the HITECH provisions related to privacy and security; however, there are further rulemakings on the horizon. The final rule to implement changes to rules giving patients greater transparency [5] about disclosures from electronic medical records is still in process. In addition, HHS has yet to propose rules to implement the HITECH requirement that patients have the ability to receive a percentage of penalties or monetary settlements due to violations of HIPAA rules.

HHS has two other important privacy reports in the pipeline. One looks at the privacy protections for personal health records not covered by HIPAA. The second report mandates guidance on how medical record holders can ensure they are collecting, using, and disclosing only the minimum necessary amount of health data appropriate to the task at hand.

But today, we celebrate this milestone and the substantial improvements to health privacy and security contained in these rules.

1. 1. A 2006 survey [6]conducted for the Markle Foundation found that 77% of people were very concerned about use of their medical information for marketing purposes.

The content through CDT is for Site that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Copyright © 2013 by Center for Democracy & Technology.

Source URL:
https://www.cdt.org/blogs/deven-mcgraw/2501feds-boost-privacy-protections-medical-records

Links:
[1] https://www.cdt.org/personnel/deven-mcgraw
[2] https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules
[3] https://www.cdt.org/blogs/kate-black/2706omb-announcement-furthers-health-privacy-frustration
[4] https://www.cdt.org/files/pdfs/CDT_Comments_to_HHS_Proposed_Rulemaking_09-13-10.pdf
[5] https://www.cdt.org/blogs/harley-geiger/128cdt-files-comments-proposed-accounting-disclosures-rule
[6] http://www.markle.org/publications/1214-survey-finds-americans-want-electronic-personal-health-information-improve-own-hea