HHS Releases Rules for Electronic Health Records

by Deven McGraw [1]
July 14, 2010

The health IT and privacy communities have their heads buried in text! Three branches of the U.S. Dept. of Health and Human Services (HHS) have released more than a thousand pages of rules on health IT in less than a week.

HHS released two rules on Tuesday. The Office of the National Coordinator for Health IT (ONC) released [2] the final rule setting the criteria for certification of electronic health records (EHRs). At the same time, the Centers for Medicare and Medicaid Services (CMS) issued the final requirements [3] that health care providers (chiefly physicians and hospitals) must meet to be "meaningfully using" EHRs and therefore qualify for federal Medicare and/or Medicaid subsidies beginning in 2011. This is on top of the proposed privacy rule [4] issued by the Office of Civil Rights last Thursday (see our blog post [5] on that rule).

We are still wading through the meaningful use and certification final rules but, naturally, flipped first to the criteria related to privacy and security.

HHS Kept Some Good Stuff In

EHRs must be certified in order to qualify for the meaningful use program to which the subsidies apply, and the certification criteria includes data security functionalities and standards. We were pleased to see that the final rule on certification left the security criteria largely intact from the proposed rule [6]. The criterion for "accounting for disclosures" – an accounting of all the disclosures made of a patient's record – was determined to be voluntary, to provide HHS time to issue details on the requirements, and we look forward to seeing those details.

On the meaningful use final rule, we are glad that "meaningful users" will still required to do a security risk assessment. To achieve "meaningful use" and qualify for government subsidies, health care providers are required to meet numerous objectives. Under the proposed rule [7], one of these objectives was a requirement that health care providers conduct the assessment to identify security gaps in their EHR systems. One change from the proposed rule to the final rule was to make some of the objectives mandatory and others voluntary. We think it was a good decision for CMS to preserve the security risk assessment as a mandatory requirement, although we still believe it would be useful for HHS to issue more guidance for providers – many of whom will be very new to using EHRs – on how to complete the assessment effectively.

Tepid Treatment of Privacy

Unfortunately, using the meaningful use objectives to achieve significant advances in privacy and security appears to be off the table. Maintaining patient privacy and data security remain stated goals of meaningful use, but nothing is required to achieve this goal beyond the mandatory security risk assessment and response. CMS rejected recommendations [8] from the Health IT Policy Committee to make compliance with state and federal privacy and security laws a meaningful use requirement, and also to disqualify providers fined for willful neglect of the HIPAA privacy and security regulations from eligibility for the federal health IT subsidies. CMS did not provide justification for its rejection of the latter recommendation. I guess providers fined for willful neglect of federal privacy and security rules can ease their pain with their meaningful use subsidy.
Privacy and security may still be a goal of meaningful use – and compliance with privacy and security mandatory – but the impact of those statements feel hollow in the absence of a set of clear and "meaningful" expectations for strong privacy and security practices.

Unfortunately, this tepid treatment of privacy may not be limited to just the first stage of meaningful use objectives. There are two more stages of meaningful use to go before the program is completed.

In commentary to the final rule provisions, CMS states "we do not see meaningful use as an appropriate regulatory tool to impose different, ***additional***, and/or inconsistent privacy and security policy requirements from those policies already required by HIPAA" (emphasis added). We agree that meaningful use should not contradict or conflict with HIPAA requirements. We also agree it makes little sense to use meaningful use as the primary mechanism for implementing a comprehensive privacy and security framework (which just creates one more incentive for providers to opt out of the incentive program). But to foreclose the use of meaningful use criteria to make any advances in health privacy and security is to surrender a significant policy lever for encouraging industry adoption of privacy and security best practices for using EHR technology.

Different perspectives?

The HIT Policy Committee endorsed the HIT Strategic Framework [9] for use by ONC in developing its HIT strategic plan. In the HIT Strategic Framework, the Policy Committee recommends using meaningful use criteria as a tool for accomplishing the enforcement of privacy and security laws and policies. Perhaps this highlights a difference of opinion between ONC and CMS about the role that meaningful use plays in building a foundation of trust for health IT. If privacy and security are the foundation for health IT, meaningful use criteria should “meaningfully” support that goal.

Links:
[1] https://www.cdt.org/personnel/deven-mcgraw
[2] http://www.ofr.gov/OFRUpload/OFRData/2010-17210_PI.pdf
[3] http://www.ofr.gov/OFRUpload/OFRData/2010-17207_PI.pdf
[4] http://frwebgate1.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=Z4O0H6/0/2/0&WAISaction=retrieve
[5] http://cdt.org/blogs/harley-geiger/hhs-issues-proposed-updates-hipaa-privacy-regulations
[6] http://edocket.access.gpo.gov/2010/pdf/2010-4991.pdf
[7] http://edocket.access.gpo.gov/2010/pdf/E9-31217.pdf
[8] http://healthit.hhs.gov/portal/server.pt?open=512&objID=1269&parentname=CommunityPage&parentid=5&mode=2
[9] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_911024_0_0_18/HITStrategicFramework030910.pdf