

1634 Eye Street, NW  
Suite 1100  
Washington, DC 20006

August 8, 2011

Donald M. Berwick, M.D.  
Administrator  
Centers for Medicare and Medicaid Services  
Department of Health and Human Services  
P.O. Box 8012  
Baltimore, MD 21244-1850

Re: CMS-5059-P

Dear Dr. Berwick:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive, workable privacy and security policies to protect health data as policies and information technologies spur the exchange of health information. CDT is frequently relied on for sound policy advice regarding these challenges; we have testified before Congress four times in relation to these issues, and we chair the privacy and security working group of the federal Health IT Policy Committee (called the “Tiger Team”). CDT submits these comments in response to the Center for Medicare and Medicaid Service’s (CMS’) June 8, 2011, Notice of Proposed Rulemaking (NPRM) regarding the *Availability of Medicare Data for Performance Measurement* required by Section 10332 of the Patient Protection and Affordable Care Act (ACA).<sup>1</sup>

Reform of the U.S. health care system depends on robust, accurate measurement and public reporting of system performance, both in terms of cost and quality. CDT supports CMS’ effort to release Medicare claims data to systematically measure the performance of providers and suppliers. However, it is vital that this information only be accessed, used and disclosed in a responsible manner that is protective of patient privacy and security.

**We applaud and enthusiastically support all of the strong privacy and security provisions in this NPRM (both in the preamble and regulatory text), and we urge that they be retained in the final rule.** Our comments below address a few areas where CDT believes the rule could be strengthened.

#### Requirements to be a qualified entity (QE)

Under the Affordable Care Act and the provisions of the NPRM, CMS may share Medicare claims data for performance measurement only with “qualified entities” (QEs). Among the requirements to be qualified is that the entity must establish, maintain and

---

<sup>1</sup> 76 Fed. Reg. 33566 (June 8, 1991).

monitor a rigorous data privacy and security program and must disclose to CMS any “HIPAA violations for the precedent 10-year period, and any corrective actions taken to address” violations or inappropriate disclosures of beneficiary identifiable information.<sup>2</sup> The HHS Office of Civil Rights issued its first civil monetary penalty for HIPAA violations only this year and has entered into monetary settlements for HIPAA violations with only a handful of entities. In order to be certain that entities with poor histories of compliance with health privacy laws are not permitted to participate in this program, CDT recommends that CMS also require QE applicants to disclose any confirmed violations (or settlements due to allegations of) of state health privacy laws and to identify any corrective actions taken in response.

#### Circumstances under which beneficiary identifiers can be released

CDT strongly supports CMS’ decision to provide QEs with beneficiary information that is encrypted so that it is possible for QEs to link beneficiary claims across data sources without knowing the beneficiary’s identity.<sup>3</sup> We recognize, however, that providers and suppliers may need to receive identifiable information in order to check the accuracy of information included in a particular performance report. CMS contemplated three options for providing identifiable data to providers and suppliers, and opted to propose providing QEs with identifiers only on a transactional basis in order to respond to provider or supplier inquiries. QEs are required to destroy the identifiable data after responding to a provider or supplier’s request.<sup>4</sup>

Although we would prefer that QEs not have access to identifiable patient information under any circumstances, we believe the proposed option strikes the most workable balance given the interests and issues at stake. However, we also suggest that the DUAs include strong prohibitions against re-identification of beneficiary information, either by using identifiers provided by CMS or by using other data available to the QE from private or public sources. We also suggest that CMS require QEs to commit in the DUA to limiting the number of staff members who have access to identifiable information. QEs should also be required to strictly bind any contractors to these provisions.

#### Data retention limits

Under the proposed rule, QEs are required to return to CMS or destroy Medicare claims files if their agreement with CMS is terminated. We support this provision but note that there are no provisions regarding how long QEs can retain Medicare claims data if they remain participants in this program. At some point these data files will no longer be useful for measuring performance – and yet there are no provisions to either return or destroy this data after some reasonable period of time. Responsible data stewardship includes setting and being held accountable for limits on retention of personal information. We urge CMS to establish an outer limit for retention of any Medicare

---

<sup>2</sup> 401.703(a)(1)(vii).

<sup>3</sup> 33573.

<sup>4</sup> 33575-76. (“CMS would only provide beneficiary names to qualified entities on a transactional basis for the purposes of responding to specific requests for data by providers of services and suppliers. . . . The qualified entity . . . would be expected to destroy the identifiable data after responding to the providers’ request for this data.”)

claims files – such as three years – and require QEs to return or destroy Medicare claims files after the data retention period has passed (such a requirement should be included in the final rule and in the DUA). In the event that there are legitimate reasons for QEs to retain the data for longer, such reasons should be listed as exceptions in the proposed rule, or CMS can provide a process for QEs to request an extension.

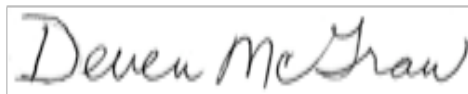
#### Providers & supplier not covered by HIPAA

CDT believes that non-HIPAA covered providers and suppliers that request Medicare beneficiary identifiable information should be required to adhere to a DUA that binds them to the terms of the HIPAA privacy and security rules.

CMS notes that 0.1% of institutional providers and 1.8% of non-institutional providers are not covered under HIPAA.<sup>5</sup> It is possible that one of these providers could request Medicare beneficiary identifiable data in order to dispute a particular QE report.<sup>6</sup> Currently CMS is proposing that applicants to the QE program include a plan on how to protect information given to non-HIPAA covered providers.<sup>7</sup> To illustrate, CMS gives the example of a plan where the QE would require the non-HIPAA covered provider to sign an agreement that would hold the provider to the terms of the DUA between the QE and CMS.<sup>8</sup>

CDT believes that the suggestion to bind non-HIPAA covered entity to the terms of the DUA should be elevated to the level of a requirement. When these providers request Medicare beneficiary identifiable information, they will necessarily have to interact with the QE under the current proposed rulemaking.<sup>9</sup> This would provide an excellent opportunity to require these providers to sign a specifically tailored DUA that would require them to abide by the HIPAA privacy rules with respect to the data being provided.

We thank CMS for including strong privacy and security protections this NPRM and for the opportunity to submit comments.



Deven McGraw  
Director, Health Privacy Project

---

<sup>5</sup> 33576

<sup>6</sup> 33577 (“However, qualified entities may generate performance reports for providers of services and suppliers not subject to HIPAA.”)

<sup>7</sup> 33577 (“For those few providers that are not subject to HIPAA . . . we propose to require that qualified entities include a plan in their application materials for assuring protection of the data . . .”)

<sup>8</sup> 33577 (“ . . . such as requiring a signed privacy and security agreement between the qualified entity and the provider of services or supplier that includes the same privacy and security protections as the qualified entity is subject to under the DUA it enters into with CMS.”)

<sup>9</sup> 33575