September 21, 2012

Ms. Rebecca Roper
Agency for Healthcare Research and Quality
Attention: HIT-Enabled QM RFI Responses
540 Gaither Road, Room 6000
Rockville, MD 20850

Dear Ms. Roper:

The Center for Democracy & Technology ("CDT") is pleased to offer our comments in response to the Agency for Healthcare Research and Quality's (AHRQ) July 20 Request for Information: "Quality Measurement Enabled by Health IT."[1] We support a quality measurement system that enables access to clinical data for quality measurement purposes in a way that builds public trust.[2] As described in more detail below, we urge AHRQ to adopt a quality measurement regime that employs a distributed network model; uses the minimum data necessary for a particular analytic purpose; and includes robust accountability and enforcement mechanisms.

CDT is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education and litigation, as well as through the development of industry best practices and technology standards.

Recognizing that a networked health care system can lead to improved health care quality, reduced costs and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health

[1] 77 Fed. Reg. 42738-42740 (July 20, 2012).
[2] Relevant to question 10, id. at 42739.

IT) initiatives. We have testified before the U.S. Congress five times since 2008 on the privacy and security issues raised by health IT, and we chair the privacy and security policy working group of the federal Health IT Policy Committee (called the "Tiger Team").

Privacy Implications of Health IT

Health IT has a greater capacity to protect sensitive personal health information than is the case with paper records, as digital technologies such as user authentication, encryption, and detection and enforcement tools offer protection above and beyond that which is possible with paper records.

However, as your July 2010 report "An Environmental snapshot – Quality Measurement Enabled by Health IT: Overview, Possibilities, and Challenges"[3] notes, uncertainty regarding legal requirements can lead to hesitation among health care entities when it comes to sharing electronic health information. Further, the computerization of personal health information – in the absence of strong privacy and security safeguards – magnifies the risk to privacy, as tens of thousands of health records can be accessed or disclosed through a single breach. This, combined with the historic lack of enforcement of existing privacy rules by federal authorities, can deepen consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.

We are among the advocates that the AHRQ report says argue that "a comprehensive, flexible privacy and security framework is needed, which sets clear parameters for access, use, and disclosure of personal health information for all entities engaged in electronic health information."[4] An effective quality measurement system must include privacy protections that accommodate and support necessary data flows, while at the same time keeping personal health information private and secure.

Elements of an Effective Quality Measurement Regime

In order to ensure maximum analytic benefit of health information, while simultaneously protecting patient privacy, AHRQ should promote a quality measurement regime that incorporates three key privacy functionalities: (1) a federated architecture; (2) minimum necessary data use; and (3) robust accountability mechanisms.

(1) **Federated Architecture**. A well-designed and privacy-protective health IT information sharing system should consist of a series of interconnected

[3] *See* McGraw, D. et al, "Patients and Privacy," *Health Affairs* Vol. 28, No. 2 (March/April 2009).
[4] Id. at p. 14.

databases, rather than a single, centralized data repository. A federated architecture will allow analysis across data sets – such as for quality measurement purposes – without aggregating the data into a single physical location.[5]

A centralized database may present dangerous privacy risks, as it presents an attractive target for breach, with potentially disastrous consequences. The costs to the data steward are high, including notifying the individuals whose information was breached and mitigating all real or potential damages. Further, storing health information in a single database may discourage the sharing of information, as it removes control from the original owners of the data once the data is moved to the centralized system.

A federated system, on the other hand, eliminates the need to make multiple copies of the data to meet a host of analytic needs and also substantially decreases the risk of a singular, expensive breach. It also gives the owners of the connected databases ongoing control of their data, allowing them to share only the data they choose, while at the same time maintaining responsibility for the accuracy of the data they maintain.

(2) Minimum necessary use of data. When collecting and sharing health data, including for purposes of quality measurement, the principle of "minimum necessary" should govern. This minimizes data exposure to only that information necessary to support the particular analysis being performed.

Patient records contain large amounts of information – some clinical and personally identifiable, some billing-related, some involving prescription history – not all of which is necessary for or relevant to individual analyses. HIPAA requires that covered entities take reasonable steps to limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose.[6]

(3) Robust accountability mechanisms. An effective and privacy-protective quality measurement regime should employ accountability techniques, such as access or audit logs, that ensure user identification and accountability. Further, a strong oversight system is essential, in order to ensure that personal health information is being collected, used and disclosed in compliance with applicable law and policy. Any oversight

---

[5] *See* CDT's paper "Decentralizing the Analysis of Health Data," March 2012, *available at*: https://www.cdt.org/files/pdfs/Decentralizing-Analysis-Health-Data.pdf.

[6] *See* 45 CFR 164.502(b), 164.514(d).

system must also include enforcement mechanisms that result in appropriate consequences for data misuse.

Accountability and enforcement will do much to bolster consumer trust in health information technology and exchange, a necessary component of any quality measurement initiative.

Thank you for the opportunity to submit these comments. Please let us know if we can be of further assistance.

Sincerely,

Deven McGraw

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology

Alice Leiter

Alice Leiter
Policy Counsel
Center for Democracy & Technology