September 23, 2011

Steven Posnack
Director, Federal Policy Division
Office of Policy & Planning
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Re: RIN 0991-AB78 Metadata Standards To Support Nationwide Health Information Exchange

Dear Mr. Posnack:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive, workable privacy and security policies to protect health data as it is exchanged using information technology. CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. We have testified before Congress four times on the privacy and security issues raised by health IT, and we chair the privacy and security working group of the federal Health IT Policy Committee (called the "Tiger Team").

We submit these brief comments in response to the Advance Notice of Proposed Rulemaking on Metadata Standards to Support Nationwide Health Information Exchange.[1] Of relevance to that topic, CDT submitted comments on the recommendations proposed by the President's Council of Advisors on Science and Technology in its report of December 2010, http://www.cdt.org/comments/comments-cdt-hhs-pcast. We also served on the PCAST Workgroup of the Health IT Policy Committee.

We support the efforts of the Office of the National Coordinator for Health IT (ONC) to propose and pilot test metadata standards that will allow for the communication of privacy policy information, including any applicable patient consents, with electronic health information as it is shared more extensively. We believe this work should move forward, and we heartily agree that any such standards will need to be thoroughly tested in real-world settings before they can be adopted as industry requirements.

[1] 76 Fed. Reg. No. 153 (August 9, 2011).

However, we want to raise a few notes of caution:

Some have framed the PCAST as specifically recommending that, as a policy matter, patients should be provided with granular choices with respect to their health data. Although the ANPRM does not expressly deal with consent policy issues, unfortunately some of the text in this ANPRM further perpetuates this framing. For example, in summarizing comments to the PCAST report, the ANPRM states "several commenters supported the concept of giving patients granular consent as envisioned in the PCAST report." (48771) As expressed in some detail in CDT's comments to the PCAST report (see reference above), we disagree with this interpretation. We believe that PCAST set forth technical recommendations intended to provide a mechanism to honor existing or future consent policy; PCAST did not call upon ONC (or other agencies within HHS) to adopt specific policy with respect to consent.

Whether patients should be granted more granular choices with respect to their data is a policy decision that should be determined through a robust policymaking process; policy on consent should not be set merely through the adoption of a particular technical standard. This effort to establish metadata privacy standards should focus on supporting policies already in existence that provide patients with granular consent rights, such as the laws governing the disclosure of certain identifiable substance abuse treatment records, the state laws that require consent for the sharing of certain categories of sensitive health data, and the right established in HITECH that allows patients to restrict the sharing of their data with health plans when they pay out-of-pocket for their care.

It is also critical that providers and patients understand that a metadata tag indicating a patient preference does not necessarily translate into a legal obligation for that preference to be honored. Consent preferences are only required to be enforced in circumstances where there exists a legal requirement to obtain the patient's consent. The presence of a metadata tag with a consent preference allows a data discloser (such as a health care provider) to indicate that the required consent to share the data has been obtained; the tag also puts a recipient of a patient's data on notice that the patient has expressed a preference with respect to the sharing of that data. However, if the recipient is not bound by a legal obligation to obtain consent before further utilizing or sharing that data, the presence of the metadata tag will not create a legal obligation to honor the preference. For example, if a patient sends health information to her physician, and the information includes a metadata tag that indicates that the data cannot be disclosed to others, that physician is only legally bound to honor the metadata tag if they are subject to a binding legal requirement to obtain the patient's consent prior to further access, use and disclosure of the data.

The language of the ANPRM suggests that a metadata tag will govern further disclosures of information[2] – but as noted above, we believe this is only the case if the entity

[2] "HL7 vocabulary for sensitivity would be used to indicate at a more granular level the type of underlying data to which this metadata pertains in order for the potential for automated privacy

receiving the information has a binding legal obligation to obtain the patient's consent before further disclosing it. In other words, the presence of a metadata tag with a consent preference does not by itself create consent policy – and this needs to be better understood by all who will be impacted by this initiative.

The comments we make above should not be construed to negate the importance of creating standards that will enable granular consent policy to be honored. If electronic health records are unable to honor existing granular consent policy, they will be far less useful to providers who are already required to comply with such policies. But we urge HHS to be more careful about not overstating the legal significance of a consent metadata tag.

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

Sincerely,

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

filters to apply more stringent protections to the data *in the event it is selected for a future disclosure.*" (emphasis added) (48774)