CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

October 16, 2009

Office of the National Coordinator for Health Information Technology
Attention: Requirements Document Team
Mary Switzer Building
330 C Street, S.W. Suite 1100
Washington, DC 20201

Dear Dr. Bean:

On behalf of the Center for Democracy & Technology (CDT), I respectfully submit these brief comments in response to the Consumer Preferences Draft Requirements Document dated October 5, 2009. CDT, through its Health Privacy Project, promotes comprehensive privacy and security policies to protect health data as information technology is increasingly used to support the exchange of health information. As Director of the Health Privacy Project, I also sit on the Health Information Technology Policy Committee, a federal advisory committee chartered in the American Recovery and Reinvestment Act of 2009 to provide recommendations to the Office of the National Coordinator for Health Information Technology (ONC) regarding implementation of the legislation.

As a threshold matter, I believe the release of this document is premature and could significantly undermine ongoing efforts to establish critical privacy and security policies regarding consumers' rights to make choices regarding the electronic exchange of their health data. The document acknowledges that "policies surrounding consumer preferences are expected to evolve over time," and that the document will accommodate both the present state of consumer consent as well as "future policy decision" outcomes (p.3). Such language suggests that the drafters intended for the document to be policy neutral – but unfortunately, it is not. As set forth in more detail below, the recommendations do not necessarily accurately implement consent requirements in current law and assume that there will be, at a minimum, a consumer right to opt-in or opt-out of any electronic exchange of their data, at a fairly granular level. In fact, the issue of whether consumers will have a national right to opt-in or out-out of exchange has not been definitively addressed.

This document purports to focus only on technical standards, but to put it simply, standards are never policy neutral. In the absence of clear policies, technical standards will set policy by default. If, for example, we have a technical standard for consumers to have their preferences regarding data exchange both expressed and transmitted across provider settings, and this standard is either required or strongly encouraged to be part of health IT systems, we have de facto set consumer consent policy – and the parameters of such policy are established by the specifications of the standard. It is then difficult – if not impossible – to go back and set policy. The issue of the appropriate role of consumer consent in protecting privacy is too important to resolve by default via the standards development and implementation pipeline.

Consequently, where standards are needed, they should be developed before or arm-and-arm with policy and technological requirements (which are distinct from specific standards). ONC is well aware of the need to address policies on consumer choice in a thoughtful, comprehensive way, and I believe the office is continuing to seek input on this issue. (The document itself raises some issues that need to be resolved on pages 12-14.) The issue came up repeatedly in the most recent Policy Committee hearing on privacy and security issues, and the Committee will be doing further work on this issue. No further action should be taken on this document until we have established policy on consumer choice, as well as requirements for how technology will advance those policies. At that point, the document should be revisited and refocused on what standards, *if any*, are needed to implement those policies and requirements.

Although I believe further work on this document should cease until consumer preference policies and technology requirements are specified, I offer the following more specific comments to take full advantage of this opportunity:

- **Not reflective of current law.** As noted earlier, the document does not necessarily reflect current law. The document states clearly that "consumers, at the highest level, *require the capability* to opt-in or opt out of exchange of their health information." (pp. 10, 40) In fact, consumers do not have the right under the HIPAA Privacy Rule to either consent to, or opt out of, the disclosure of their health information whether in paper or electronic format, for treatment, payment, health care operations and other purposes. Some state laws do require that consumer consent be obtained in order for health data to be shared, with most of these laws applying to specific types of health information. Further, federal law covering federally funded substance abuse treatment programs also requires patient authorization for the exchange of data. But this does not constitute an overarching *requirement* for opt-in or opt-out of any exchange of health data. In fact, to allow patients to opt-out of having any of their health data electronically exchanged between two providers even for treatment

purposes would significantly change the legal landscape for sharing of patient data in most states. This is most certainly a policy decision that requires further discussion before proceeding with the development of specific technical standards.

I also note that policy discussions with respect to giving consumers the right to opt-in or opt-out of exchange of their data have largely occurred in the context of shaping policies for participation in formally organized state and regional health information exchanges and the "National Health Information Network" (NHIN). For example, the National Committee on Vital and Health Statistics (NCVHS) recommended that patients have the right to at least opt-out of having their information shared through the NHIN, and patients should have enhanced rights regarding exchange through the NHIN of certain categories of sensitive data.[1] In addition, a number of state and regional health information exchanges already sharing patient data have implemented opt-in or opt-out policies (either voluntarily, or because they have interpreted their state laws to require it) – but opt-in/opt-out typically applies only to information shared through the network and not data sharing that occurs independently between two health care organizations.[2] In contrast, this document appears to use the term "health information exchange" to refer to both formally organized networks as well as point-to-point exchanges between two entities.[3] However, even with respect to exchange through formalized networks, the discussion about policy and technology requirements must take place before we move to determine whether we need a particular technical standard to implement it.

Any such policy and technology discussions must acknowledge the appropriate role for patient consent in protecting health data. For individuals to meaningfully consent to certain uses and disclosures of their data, they need to understand precisely what they are consenting to – i.e.,

---

[1] http://www.ncvhs.hhs.gov/060622lt.htm.

[2] See, for example, recommendations regarding health information exchange network consent policy in the State of New York - http://www.nyehealth.org/files/File_Repository16/pdf/Consent_White_Paper_Public_Comment100808.pdf.

[3] The definition of "health information exchange" appears to be describing a noun – "an entity…that supports *health information exchange* and enables the movement of health-related data within state, local, territorial, tribal or jurisdictional participant groups," but it uses the verb form of the phrase within the definition (see italics). (p.40) Figure 7.0 (p.31) describes "information exchange" as occurring through an "HIE Intermediary" (which is not defined in the document) or "point to point."

for what purposes can health data be exchanged, and who is authorized to access and disclose it, and how are those information practices effectively enforced. Consent is only one part of a framework of protections for data that are critical to building public trust in health IT,[4] and overrelying on consent to protect data results in weak privacy protections for patients.[5]

Finally, there already are federal and state requirements to obtain patient consent for the exchange of certain types of health data, and federal laws that prohibit certain uses of health data (for example, the Genetic Information Nondiscrimination Act). Health information technology systems must have the capability to honor those consents and prohibitions where they already apply.[6] However, I do not think this document advances that objective, as it presumes an "opt-in/opt-out" framing that may not fit the actual consent standard or prohibition in the law, and it does not include any assurances that a consent could be honored by the recipient organization (which would seem to be a necessary prerequisite to implementing laws regarding patient consent).

- **Are specific technical standards even needed?** The document identifies specific standards that address certain events or actions required to address consumer preferences, and suggests that in areas where no current standard exist, standards will need to be developed. But specific technical standards to implement consent policy may not be needed. Achieving "inoperability" for consent policy implementation does not require a one-size-fits-all approach that could slow adoption and serve as a barrier to innovation.[7] Instead, ONC's focus should be on requiring that health IT systems have the technical capacity to implement consent policy, and that the systems demonstrate an ability to perform these functions with a relatively high level of confidence.

- **Document focuses largely on how "preferences" are collected and shared; doesn't specify how preference data is protected.** In the various scenarios – from creation of a preference, to management and exchange of a preference – the document is fairly specific on how

[4] http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.
[5] http://www.cdt.org/healthprivacy/20090126Consent.pdf.
[6] As a final note on the document not reflecting current law, we call your attention to the statement that data entered into a consumer's PHR "by default…remains private and requires authorization for disclosure." (p.13) This is not a federal legal requirement; data in PHRs is subject to consumer control only in cases where the PHR policies provide consumers with this right.
[7] http://www.markle.org/downloadable_assets/20090430_meaningful_use.pdf (in particular, pages 12-16).

consumer preferences are gathered and sent. But it is not always clear that these transactions occur only when there is a legitimate need to share health data to which the preference refers. For example, in 6.16.1, the document calls for an audit trail where the primary organization identifies all secondary receiving organizations to which the consumer's preference was transmitted, suggesting there may be instances where preferences are shared without data (why not just audit the data flow). 6.25.1 notes that once a preference is received by a secondary organization, an acknowledgement must be sent back to the primary organization – why is this not phrased in terms of whether the actual data was received with the preference attached? In addition, 6.13 notes that any amendments to preferences need to be electronically sent to any secondary organization that had received the original preference; such an action should only take place if the secondary organization has a legitimate need to receive health data to which that amended preference refers.

It seems highly inappropriate for an entity to independently send consumer preference information unless it applies to actual health data being exchanged and the preference should be exchanged with the data. The independent exchange of a preference without data creates an added potential for a privacy violation, as this preference also likely qualifies as protected health information. The document potentially compounds this error by requiring such preferences to be stored by both the primary and receiving organization, without making clear that such preferences may constitute protected health information and that they should be stored attached to the data to which they refer (merely reciting that such preferences should be stored in accordance with federal, state and local policies and procedures is not sufficient).

- **List of sensitive data categories – what is the source?** Section 9.2 of the document includes a list of possible sensitive health data categories with no indication of how this list was developed. For example, it does not match the list of sensitive categories recommended by NCVHS after they had gathered testimony and spent months in deliberation.[8] The question of whether consumers should have a right to opt-in or opt-out of having certain categories of sensitive data exchanged (beyond what may already be required in current law) is a complicated policy question that needs to be resolved through a transparent process that also includes a realistic discussion of what is technologically possible before we can proceed to developing standards. The lack of an evidentiary basis for this list makes it inappropriate to include in a document intended to foster further standards development. It was likely difficult for the Requirements team to

[8] http://www.ncvhs.hhs.gov/080220lt.pdf

come up with such a list in a short time period – which starkly illustrates the inherent contradiction involved in attempting to set forth technical standards before appropriate policies have been developed.

A number of provisions in this document may prove to be highly valuable – but only once we have worked through the significant policy and technology considerations that surround the question of consumer preferences.

Thank you for the opportunity to submit these comments.

Respectfully,

Deven McGraw
Director, Health Privacy Project