Comments of the Center for Democracy & Technology

Request for Information
Regarding the President's Council of Advisors on Science and Technology Report
Entitled "Realizing the Full Potential of Health Information Technology To Improve Healthcare for Americans: The Path Forward"

January 19, 2011

Dr. David Blumenthal
National Coordinator
Office of the National Coordinator for HIT
U.S. Dept. of Health and Human Services

Dear Dr. Blumenthal:

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 submits these comments in response to the December 10, 2010, Request for Information (RFI) issued by the Department of Health and Human Services (HHS) Office of the National Coordinator (ONC).[1] The RFI concerned the implications of the recent report by the President's Council of Advisors on Science and Technology (PCAST) on how to achieve the nation's health information technology (HIT) goals.[2]

PCAST issued its report at a critical juncture in our national efforts to promote the widespread adoption of HIT to improve individual and population health. There is much in the report that is positive and groundbreaking, and we applaud PCAST for its leadership and vision. We wholeheartedly agree with the need to focus national efforts on appropriate exchange of health information for health system reform, including the adoption of Internet-based standards that will enable such exchange. We also agree with the promotion of distributed network architecture for data sharing, the acknowledgement that a business model for exchange should not be driven by commercial gain, and PCAST's rejection of the notion that a unique patient identifier is necessary for effective information exchange.

However, we have some concerns about the efficacy and feasibility of PCAST's technical approach that appear not to have been fully explored by PCAST prior to the issuance of the report. We urge HHS, in implementing the PCAST recommendations, to carefully consider and address these concerns in order to realize the important goal of

[1] 75 Fed Reg. 76986-76987 (Dec. 10, 2010).

[2] President's Council of Advisors on Science and Technology, *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*, Dec. 8, 2010, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf. (Hereinafter, "PCAST Report.")

robust health information exchange while building on the progress HHS has made to date.

I. Focus on policy infrastructure to promote trust in information exchange

Building the public's trust in robust health information exchange will require a comprehensive framework of privacy and security policies, as well as technical safeguards. In building this framework, it is critical to focus first on the policies needed to achieve and maintain trust, while considering the supportive role that innovative technology and sound network design can play in realizing this goal. PCAST seems to recognize this in its report, where it cites the need for "comprehensive privacy and security protections that are based on fair information practices and set clear rules on how patient data can be accessed, used and disclosed, and that are adequately enforced."[3] However, this statement is not supported by specific policy recommendations; instead, it is muted by examples of application of PCAST's technological approach to achieving exchange, which rely heavily on patient consent.

We urge ONC to continue its efforts to build and implement a comprehensive and extensible privacy and security framework rooted in fair information practices. ONC should continue leveraging current infrastructure, policy, and existing trusted exchange relationships to build trust in nationwide health information exchange. Any technological approaches to exchange must be then evaluated with regard to their efficacy as tools to achieving this framework.

II. Avoid overreliance on consent for privacy protection

PCAST recommends affixing standardized, mandatory metadata tags to individual elements of health data. This granular metadata tagging is foundational to the other major proposals in the PCAST report. The tags would describe attributes of the health data, including data provenance (where the data was created) and the patient's privacy permissions.[4] Creating an accountability infrastructure for data use based primarily on tethering privacy permissions to data is untested in the marketplace, especially across disparate institutions and at the scale PCAST is proposing. On the contrary, other technology solutions that have attempted to protect data by rendering it unreadable to unauthorized parties, such as Digital Rights Management (DRM) technologies, have proven ineffective against piracy[5] and have presented obstacles to both legitimate use and to innovation.[6]

---

[3] PCAST Report, Pg. 46.

[4] PCAST Report, Pg. 41.

[5] Electronic Frontier Foundation et al., *Digital Rights Management: A failure in the developed world, a danger to the developing world*, Mar. 2005, http://www.eff.org/wp/digital-rights-management-failure-developed-world-danger-developing-world.

[6] Center for Democracy & Technology, *Evaluating DRM: Building a Marketplace for the Convergent World*, Pg. 21, Sep. 2006, http://www.cdt.org/files/pdfs/20060907drm.pdf.

PCAST relies on metadata tagging to apply granular patient consent directives. Although the report appropriately describes patient consent as just one important component of an effective privacy framework, the report also focuses heavily (through the text and examples) on consent as the major use of metadata tags for privacy protection.[7] CDT agrees with PCAST that consent is an important component of privacy protection, but as CDT has stated in numerous reports, overreliance on consent in practice leads to less individual privacy in health data.[8] Any privacy framework must also address the principles of transparency, purpose specification, data minimization, use limitation, and oversight. These important principles receive little attention in the report, and it is completely unclear how metadata tagging could be used to meet these policy imperatives.

PCAST rightly points out that patients cannot make informed privacy choices unless they understand how their health data is used and disclosed, as well as the pros and cons of restricting certain health data from providers. PCAST presumes "most patients will probably educate themselves on the issues… ideally when they are healthy and competent," but the history of consumer privacy does not bear out this premise. "Understanding the issues" is very challenging for medical professionals, let alone patients, because of the immense complexity of the health care system. Numerous studies on privacy and marketing, including the latest Federal Trade Commission report on consumer privacy, indicate that consumers' lack of understanding about what happens to their personal data makes consent a poor privacy protection.[9]

In addition to the complexity of health information flows, the intricate nature of PCAST's granular data tagging proposal may pose a challenge to patients seeking to protect their privacy. Facebook implemented granular privacy controls, but its privacy settings grew so complicated that the social networking site ultimately moved to simplify its settings in response to user confusion and frustration.[10] PCAST's proposal that patients set privacy permissions for discrete data elements, presumably each time data is created (such as with each visit to a care facility), seems far too burdensome to be effective for patients. It is unlikely that most patients will have enough time and expertise to provide meaningful

---

[7] PCAST Report, Pg. 46.

[8] Center for Democracy & Technology, *Rethinking the Role of Consent in Protecting Health Information Privacy*, Pg. 8, Jan. 2009, http://cdt.org/files/pdfs/20090126Consent.pdf. See also Fred H. Cate, *The Failure of Fair Information Practice Principles*, in Consumer Protection in the Age of the 'Information Economy' 341 (Jane K. Winn ed., 2006); comments of Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, at the Federal Trade Commission's Dec. 7, 2009, Privacy Roundtable, http://kantarainitiative.org/confluence/display/p3wg/FTC+Privacy+Workshop+Notes.

[9] Federal Trade Commission Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change*, Dec. 2010, Pg. 25, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[10] Miguel Helft and Jenna Wortham, *Facebook Bows to Pressure Over Privacy*, New York Times, May, 2010, http://www.nytimes.com/2010/05/27/technology/27facebook.html. Facebook CEO Mark Zuckerberg: "The settings have gotten complex and it has become hard for people to use them effectively."

consent to all future uses of all their data, especially as their preferences change over time. Consequently, implementing the PCAST proposal will likely lead to an increase in blanket consents,[11] whereby patients consent to broad information sharing simply to move beyond the paperwork and obtain treatment.

In focusing privacy more on implementing patient directives, we believe that PCAST, with all due respect to its members, significantly underestimates the complex policy issues involved in developing a framework that the public and health care stakeholders will trust to support exchange of health data. Health data holders have enormous legal and ethical data stewardship responsibilities, and the overwhelming number of them takes these responsibilities very seriously. These issues are not implicated to the same degree by most web search queries, and they are not sufficiently addressed in a technical model that is largely brokered by patient consent. The choice of this technical model will not eliminate the need for stakeholders to come to consensus and agree on terms and conditions of exchange, or to upgrade our laws and policies on health information sharing, or to address financial disincentives to share data.[12] There is no technical shortcut to grappling with the difficult issues that, if unaddressed, pose inordinate barriers to health information exchange.

As noted above, although we are concerned about an information-sharing system that is based largely on patient consent, we do support providing patients with some meaningful choices on how their health data is accessed, used and disclosed. There are several areas of the law that require patient consent to share health information, such as for marketing and categories of sensitive information protected by federal or state law. In addition, there are some institutions that will seek patient consent for certain uses as a matter of policy, beyond what the law requires. In such circumstances, patients' choices must persist as data flows through the health care system. HHS should explore ways to leverage metadata tags for this purpose, and perhaps also as a means for entities to enforce specific limitations embedded in business associate agreements.

---

[11] Consent by category of use is arguably another form of "blanket" consent. For example, if I agree to share my data for care coordination purposes, the actual uses that I have blessed depends on how care coordination is defined.

[12] We note that PCAST blames the HIPAA Privacy and Security Rules, as well as data-sharing agreements between participants in health information exchanges, for impeding the flow of health information for both medical care and research. PCAST Report, Pgs. 31 and 47. With respect to the criticism of HIPAA, the referenced articles in footnotes 59 and 60 of the report were published early in HIPAA's implementation, when confusion about HIPAA's requirements created disincentives to access, use and disclose information even for legitimate purposes. (The 2009 IOM report on research (footnote 62) does raise some important issues regarding HIPAA's impact on research that regulators should address; but this is not an indication of an overall failure of HIPAA.) Although there are significant gaps to be addressed in HIPAA, and a critical need for greater guidance from the Administration on how to comply in a digital age, most covered entities today are accustomed with HIPAA compliance as a business routine. We should build on existing frameworks that are familiar to stakeholders and the public in lieu of ripping and replacing them with a completely new, unproven model largely brokered by patient consent.

In its privacy and security recommendations to the National Coordinator, the HIT Policy Committee recommended that ONC pilot technological approaches for managing granular consent options.[13] A program piloting PCAST's proposal would provide an opportunity for metadata tagging to prove its ability – for the first time – to consistently persist meaningful patient privacy choices on a large scale. Until the metadata tagging approach demonstrates its effectiveness, however, CDT believes practical and policy challenges, in addition to the lack of experience with granular data tagging, make immediate and widespread implementation of PCAST's proposal premature.

III. DEAS and institutional accountability

The PCAST report recommends establishing an infrastructure – termed the data-element access service (DEAS) – for indexing and controlling access to health data from the exchange network.[14] The proposed service would resemble web search engines, querying information contained in metadata tags and revealing the query results only to users with proper authentication and in accordance with patient privacy directives. PCAST should be applauded for focusing on a query-response model of patient exchange, building on the "push only" models currently under consideration, without including the patient's health data in the index.[15] However, there are several areas that need clarification and likely modification in order to make the concept of a searchable patient index workable.

The PCAST report proposes that the role of a DEAS user would largely determine access to the indexed health information.[16] Individual and institutional users would be "authorized" based on their roles, and then could access data appropriate to that role if consistent with the individual's privacy permissions expressed in the metadata tag. However, the report provides no detail on which roles qualify or how those roles are assigned to DEAS users. The PCAST approach appears to leave the responsibility for determining appropriate access roles to the operator of the DEAS based on preferences issued by the patient.

Furthermore, the PCAST report appears to give DEAS users automatic access to data if the users have the appropriate role and authentication credentials, and their access is consistent with the individual's privacy permissions. Providers and institutions are unlikely to be comfortable automatically sharing data to unknown users – and this is particularly true where the access is brokered solely by authentication of role assignment

[13] Tiger Team, *Transmittal Letter*, Sep. 1, 2010, Pg. 16, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

[14] PCAST Report, Pg. 41.

[15] The PCSAT Report states that health data will not be accessible by the DEAS, but since the DEAS will index at the data element level, it is not clear how this statement can be accurate. PCAST Report, Pg. 42.

[16] PCAST Report, Pg. 50.

and patient patient consent.[17] The primary means ONC has to encourage providers to share data are the reimbursements under the HITECH financial incentive programs. However, we do not believe these time-capped and relatively limited incentives are sufficient to get providers and institutions to participate in a system in which they cede substantial control over their data, which is the model PCAST has proposed. CDT urges HHS to continue developing a trusted exchange infrastructure that does not rely on companies automatically sharing their data with entities that they do not necessarily know or trust.

We also note that the DEAS approach (based on the limited description in the report) may have the unintended result of exposing more "false positive" patient records. Based on the hearing recently held by the Tiger Team on accurately matching patients to their data, data holders play a key role in eliminating false positives. Data holders are in a strong position to know which records are the best matches to a given query, and can release just enough data to the querying party to confirm the match (and no more). Until this confirmation has occurred, health data should not be shared. However, the DEAS does not provide this role for data holders, nor would the DEAS itself have access to the additional data to confirm the match – which could mean that health data is unnecessarily exposed to querying users in false positive matches.

Today, we hold providers and institutions responsible for making decisions regarding appropriate roles for accessing data within a practice or institution, and other data-sharing partners then rely on the existence of these internal policies. Through this process, patients trust providers, and providers build trust in other providers through relationships and adherence to consistent policies and ethical norms regarding data sharing. In contrast, the PCAST model asks stakeholders to trust in software and data. ONC should continue pursuing an approach that promotes accountability at the organization level and gives organizations discretion and flexibility to structure their data sharing to fit their business needs. For this reason, CDT believes the decision of who has access to the data shared through an indexing service should remain with providers and institutions. Providers and institutions can then share data in response to queries based on the trusted relationships that patients and providers have built through consistent compliance with health privacy regulations and legal agreements.

The Markle Common Framework presents a pathway to indexing and querying patient data that is trusted by major stakeholders.[18] The Common Framework approach utilizes a decentralized network of Record Locator Services (RLS), but leaves stewardship of the data with institutions. The Common Framework advocates a two-step process in which a user's queries reveal only pointers to records authorized to be in the index by the data holder. Building on patients' customary trust in their providers, it is then the decision of the data holder whether it is appropriate to release that data to the querying user (including confirming the match of clinical health data with demographic data). While patient consent plays a role in determining whether data is accessed through the RLS

[17] As noted above, this significantly underestimates the complex issues that serve as barriers to exchange, as well as what it will take to get stakeholders to trust each other enough to exchange data

[18] Markle Foundation, *Connecting for Health Common Framework*, Apr. 2006, http://www.policyarchive.org/handle/10207/bitstreams/15506.pdf.

(just as is the case with the proposed DEAS), covered entities and health care companies are still held accountable for compliance with law and legal agreements – and it is this accountability that builds and maintains trust.

IV. Conclusion

CDT strongly agrees with PCAST that more needs to be done to promote health information exchange. However, health information exchange should be built on institutional trust, bolstered by a comprehensive privacy and security framework that details clear policies regarding how data can be used and disclosed. The work ONC is already doing to build this framework should be continued and its implementation accelerated to the extent practicable.

We thank ONC for the opportunity to issue these comments. Please do not hesitate to contact us if we can be of any assistance.

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

Harley Geiger
Policy Counsel
Center for Democracy & Technology