KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

CENTER FOR DEMOCRACY & TECHNOLOGY

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

President's Council of Advisors on Science & Technology
Health Information Planning Meeting

December 18, 2009

The Center for Democracy and Technology ("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.

Introduction

We appreciate the opportunity to present on health privacy issues. By way of background, you received the paper we published in *Health Affairs* in March 2009. I plan to use the bulk of my time to address the specific questions you posed in your invitation, but I first want to summarize some of the main points made in the article.

- The public supports health IT – but is also very concerned about the risks health IT poses to health privacy. Thus, privacy is not the obstacle to

health IT – in fact, appropriately addressing privacy and security is key to realizing the technology's potential benefits.

- To build public trust in health IT, we need the second generation of health privacy — specifically, a comprehensive, flexible privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. Such a framework should be based on three pillars:
  - Implementation of core privacy principles;
  - Adoption of trusted network design characteristics; and
  - Strong oversight and accountability mechanisms.

This requires building on – and in some cases modifying – the HIPAA privacy and security regulations so that they address the challenges posed by the new e-health environment, as well as enacting additional rules to cover access, use and disclosure of health data by entities outside of the traditional health care system. The privacy provisions enacted in the stimulus legislation – HITECH or ARRA – are an important first step to addressing the gaps in privacy protection, but more work is needed to assure effective implementation and address issues not covered by (or inadequately covered by) the changes in ARRA.

In a digital environment, robust privacy and security policies should be bolstered by innovative technological solutions that can enhance our ability to protect data. This includes requiring that electronic record systems adopt adequate security protections (like encryption; audit trails; access controls); but it also extends to decisions about infrastructure and how health information exchange will occur. For example, health information exchange is decentralized or part of a federated system, data remains at the source (where there is a trusted relationship with a provider) and then shared with others for appropriate purposes.

Giving patients some choice over how their health data is used and disclosed is important to building patient trust – but consent is not the panacea, particularly for protecting privacy within the health care system. As appealing as it may appear to be in concept, in practice reliance on consent would provide weak protection for consumer's health information. All too frequently consumers do not read privacy policies or consent forms, and even when they do, they rarely do so with a full understanding of the uses of information covered by the consent. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is <u>less</u> protective of privacy and confidentiality.

In contrast, a comprehensive approach – which allows health information to flow for core purposes with consent but also establishes clear rules about who can access, use and disclose a patient's personal health information and for what purposes – puts the principal burden on the entities holding this information.

We have published a number of papers on critical health privacy issues, and I invite you to visit our website for more details: www.cdt.org/healthprivacy.

Below we address the specific questions posed in the invitation.

Questions

1. **Electronic medicine requires trust and reliable authentication, as well as standardized computable health data.[1] How can the healthcare system create trust in the area of electronic records when the consumer is frequently made aware of security weaknesses in other segments of the market? There are no guarantees; are we demanding an impossible solution?**

If you are seeking guarantees, then yes, you are demanding an impossible solution. Fortunately, consumers are not seeking perfection; most people recognize that even the most secure data systems have experienced data breaches (for example, the recent inadvertent internal breach by the Transportation Security Administration). But consumers do deserve – and have the right to expect – vast improvement over where we are today with respect to data security, particularly as we increasingly move health information on-line. According to a recent survey of large health care organizations conducted by the Health Information Management Systems Society (HIMSS):

- Fewer than half (47%) conduct annual risk assessments (required under HIPAA)
- 58% have no security personnel
- 50% reported spending 3% or less of organizational resources on security.

The prospect of storing and moving personal health data electronically in such an environment should give us all pause. We need – through certified electronic

[1] We should seek to facilitate the exchange of "standardized computable health data" for the types of data where standards already exist and have been embraced by early adopters. For types of data where standards either don't exist or exist but are not widely used, exchange in human readable format is better than no exchange at all. See http://www.markle.org/downloadable_assets/20090430_meaningful_use.pdf (pp 10-15).

health record requirements and enhancements to the HIPAA Security Rule – stronger requirements with respect to data security. Providers with fewer resources (such as small physician practices) may need to have security requirements scaled up over time; we should, however, consider imposing greater obligations on the connecting infrastructure to better address gaps or potential weak links as these systems develop. The Privacy and Security Workgroup of the Health IT Policy Committee, which I co-chair, will be making some security policy recommendations in 2010 on this issue.

2. **Patients and health plan members may wish for some, but not all of their record to be accessible. They may wish for some data to be shared, but only for a specific period of time. Is existing technology sufficiently robust and malleable to support these requirements and expectations?**

As noted above, providing patients with additional consent rights with respect to exchange of data is not as important as establishing and enforcing a clear framework of rules to govern the electronic exchange of health information. Having said that, health IT systems will at least need to be able to honor the consent requirements that exist in current law (for example, special consent requirements for federally funded substance abuse treatment facilities and state law requirements that typically govern certain categories of sensitive data).

The capability of existing electronic health record systems to segment data subject to special consent requirements is an important question. Honoring more granular consent appears to be more technologically feasible with respect data availability through decentralized networks. For example, in the Massachusetts eHealth Collaborative, which is testing community-wide implementation of EHRs in three communities in that state, individuals were required to opt in at the provider level to having their data accessible from the network (which allowed individuals to keep their mental health providers, for example, from exchanging data through the network). New York State is pursuing a similar policy, where individuals must opt-in for any individual provider or hospital to be able to access data in, or share data through, the state's health information exchange. This level of granularity – at the provider level – appears to be technologically feasible in federated exchange models. I note that this is another topic the Health IT Policy Committee Privacy and Security Workgroup will be exploring in more detail.

3. **Will EHR's or PHR's be trusted, or valued, if the records are patient-mediated, and if the provider has no way to ensure that the records are comprehensive, accurate and reliably documented? Will patients withhold information if they do not trust the privacy of the system?**

Will providers withhold information if they know the record will be viewed by the patient and family?

There are a few patient-mediated models of exchange that are beginning to be deployed – for example, the State of Oregon is contemplating employing the health record banking model for exchange (health record banks are a form of PHR). This presents us with an opportunity to truly test whether the oft-expressed provider concerns about not trusting "patient-mediated" data hold up in actual implementation. I have also seen models of PHRs where the source of the data in the record is clear (i.e., was it directly downloaded from an EHR; did it come from a portable device; or was the patient the sole source of the data). A number of these models also do not permit individual account holders to alter or modify data that has been directly downloaded into the PHR by a provider or from a medical device.

As for the second part of the question, we know from survey data that patients do withhold data if they don't trust the privacy of the system. Without appropriate protections for privacy and security in the healthcare system, patients will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[2] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[3] Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.[4] Thus, the need to comprehensively address privacy and security to build public trust is critical.

With respect the last question, providers have long been required to share copies of medical data with patients (or their families) upon their request – with exceptions for certain types of data, such as psychotherapy notes. Any policy initiatives aimed at getting patients with more prompt access to their medical information so they can be more engaged in their own care involve access to this same type of data (albeit more efficiently), so there does not seem to be any legitimate basis to these concerns.

---

[2] Id.

[3] Harris Interactive Poll #27, March 2007. Such behaviors including withholding information, asking providers to store sensitive data in separate files, switching providers to avoid having one's records all in one place (a strategy likely to be less successful in a linked, e-health environment), or lying to providers.

[4] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

4. Ultimately, a distributed heath data network will be most useful and adoption most successful, if opting out is not an option. Is a commitment to an "opting out" option inevitable, and likely to be permanent? Or might a tipping point be achieved if incentives are aligned, and trust is achieved?

I understand the concerns about giving patients some level of choice with respect to having their data shared through data networks, but individuals are likely to rebel against being forced to have their data be part of a system they do not trust. Notwithstanding that consent is arguably one of the weakest inks in a framework of privacy protection, it can still be critical to building public trust in e-health. Before adopting any policy (state or national) that forecloses any choice options, we should look at the experience that regional, state and local health exchanges have had in implementing opt-in or opt-out policies. My understanding (largely from discussions with persons who helped establish the networks in Tennessee, Massachusetts and New York is that only a small percentage of persons opt-out (or decline to opt-in) when given the choice. If we build privacy into the design of these systems, and establish clear rules regarding who can access this data and for what purpose –that are then adequately enforced – with few exceptions, people's comfort level will increase and trust will be achieved. If we are not careful in stewarding the resource we are developing, we will squander this unprecedented opportunity.

5. Is a national patient identifier ever likely to be a reality? Would this likely build trust or erode it?

I don't think it is a reality – and it is likely to erode trust. I also think it's the wrong question to ask. If we have any hope of using this infrastructure of electronic records to improve individual as well as population based care, we will need to have a patient identification system – but that is quite different from saying that a national patient identifier is the only or even the most ideal way to resolve this. For whatever benefits a national patient identifier purports to offer, there are a number of factors that make it unappealing as a policy solution that can quickly be deployed to resolve this problem.

- The political sensitivity of this topic should not be underestimated. Congress – regardless of which party is in power – has zero funded this effort every year since XXXX. [Any idea where I can get a source for this?]
- The privacy concerns associated with establishing a national identification system are significant. We have one national identifying number in this country – the social security number – which was originally established for a very limited purpose; since that time it has

been nearly impossible to prevent its use for a range of other purposes, and thereby multiplying the potential for misuse. There is no reason to expect the same would not happen to a national health identifier. Such an initiative is also likely to be opposed by a far broader stakeholder community than just those interested in health privacy. (Anyone opposed to a national identification card, for example.) Efforts to build consensus on this will take years and in my view have a very low probability of success.

- My understanding is that imposing a national identifier onto existing systems will be very expensive to deploy and will take years to have any beneficial impact.

Technology exists today that can rapidly match and link data across state lines and disparate systems, without the use of a national patient identifier.[5]n contrast to building on solutions that are being utilized today.

Conclusion

To establish greater public trust in HIT and health information exchange systems, and thereby facilitate adoption of these new technologies, a comprehensive privacy and security framework must be in place. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. Thank you for the opportunity to present this testimony, and I would be pleased to answer any questions you may have.

FOR MORE INFORMATION

Please contact: Deven McGraw, (202) 637-9800 x 119, deven@cdt.org

[5] http://www.gcn.com/Articles/2006/09/19/Scott-Schumacher---Another-View-Identifying-patients-vs-patient-identifiers.aspx. This opinion piece, written by Scott Schumacher, the Chief Scientist at Initiate Systems, Inc., offers examples where patient data across multiple settings has been successfully lined.