KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

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

Before the House Committee on Science and Technology
Subcommittee on Technology and Innovation

STANDARDS FOR HEALTH IT: MEANINGFUL USE AND BEYOND

September 30, 2010

Chairman Wu and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today.

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.

You have asked me to address, in particular, the main challenges for personal privacy and information security presented by health information technology (health IT), as well as the privacy and security gaps and priorities that remain to be addressed for future health IT activities. Not surprisingly, the main privacy and security challenges in health IT result from gaps in current law and a lax approach to enforcement, accountability and oversight. My testimony below focuses on those gaps. However, since the broad topic of the hearing deals with health IT "standards," I have referenced some comments endorsed by CDT urging a measured role for government in setting and enforcing standards for health IT.

Introduction

Survey data consistently show the public supports health IT but is very concerned about the risks health IT poses to individual privacy.[1] Contrary to the views expressed by

[1] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005); study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006); Consumer Engagement in Developing Electronic Health Information Systems, AHRQ Publication No. 09-0081EF (July 2009).

some, privacy is not the obstacle to health IT. In fact, appropriately addressing privacy and security is key to realizing the technology's potential benefits. Simply stated, the effort to promote widespread adoption and use of health IT to improve individual and population health will fail if the public does not trust it.

To build and maintain this trust, 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, or fair information practices;[2]
- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.[3]

This requires building on – and in some cases modifying – the privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA) so that they address the challenges posed by the new e-health environment. It also requires enacting new rules to cover access, use and disclosure of health data by entities outside of the traditional health care system and stimulating and rewarding industry implementation of best practices in privacy and security.

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, when health information exchange is decentralized (or "federated"), data remains at the source (where there is a trusted relationship with a provider) and then shared with others for appropriate purposes. These distributed models show promise not just for exchange of information to support direct patient care but also for discovering what works at a population level to support health improvement. We will achieve our goals much more effectively and with the trust of the public if we invest in models that build on the systems we have in place today without the need to create new large centralized databases that expose data to greater risk of misuse or inappropriate access.

We are in a much better place today in building that critical foundation of trust than we were two years ago. The privacy provisions enacted in the stimulus legislation – commonly referred to as HITECH or ARRA – are an important first step to addressing the gaps in privacy protection. However, more work is needed to assure effective implementation and address issues not covered by (or inadequately covered by) the changes in ARRA.

---

[2] Although there is no single formulation of the fair information practices or FIPs, CDT has urged policymakers to look to the Markle Foundation's Common Framework, which was developed and endorsed by the multi-stakeholder Connecting for Health Initiative. See http://www.connectingforhealth.org/commonframework/index.html.

[3] See "Policy Framework for Protecting the Privacy and Security of Health Information," http://www.cdt.org/paper/policy-framework-protecting-privacy-and-security-electronic-health-information (May 2008); "Beyond Consumer Consent: Why We Need a Comprehensive Approach to Privacy in a Networked World," http://www.connectingforhealth.org/resources/20080221_consent_brief.pdf (February 2008).

In my testimony below, I call for:

- Establishing baseline privacy and security legal protections for personal health records (PHRs);
- Ensuring appropriate limits on downstream uses of health information;
- Strengthening protections against re-identification of HIPAA de-identified data;
- Encouraging the use of less identifiable data through the HIPAA minimum necessary standard;
- Tightening restrictions on use of personal health information for marketing purposes;
- Strengthening accountability for implementing privacy and security protections; and
- Strengthening accountability for implementing strong security safeguards.

Health IT: Key Privacy and Security Concerns

Establish Baseline Protections for PHRs

To keep pace with changes in technology and business models, additional legal protections are needed to reach new actors in the e-health environment and address the increased migration of personal health information out of the traditional medical system. Personal health records (PHRs) and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers, are not covered by the HIPAA regulations unless they are being offered to consumers by covered entities.[4] In the absence of regulation, consumer privacy is protected only by the PHR offeror's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information). If these policies are violated, the FTC may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.[5]

The absence of any clear limits on how these entities can access, use and disclose information is alarming – and has motivated some to suggest extending HIPAA to cover PHRs. However, CDT cautions against applying a one-size-fits-all approach. The HIPAA regulations set the parameters for use of information by traditional health care entities and therefore permit access to and disclosure of personal health information without patient consent in a wide range of circumstances. As a result, it would not provide adequate protection for PHRs, where consumers should be in more control of their records, and may do more harm than good. Further, it may not be appropriate for the Department of Health and Human Services (HHS), which has no experience

[4] HIPAA applies only to covered entities – providers, health plans, and health care clearinghouses. Section 1172 of the Social Security Act; 45 CFR 164.104. As explained in more detail below, ARRA extended the reach of some of HIPAA's regulations to business associates, which receive health information from covered entities in order to perform functions or services on their behalf.

[5] The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

CDT applauds Congress for not extending HIPAA to cover all PHRs.[6] Instead, Congress directed HHS to work with the Federal Trade Commission (FTC) to come up with recommendations for privacy and security protections for PHRs. This PHR "study" was due February 2010 but has not yet been released.

The agencies need not start from scratch in developing their recommendations. In June 2008, the Markle Foundation released the Common Framework for Networked Personal Health Information outlining a uniform and comprehensive set of meaningful privacy and security policies for PHRs. This framework was developed and supported by a diverse and broad group of more than 55 organizations, including technology companies, consumer organizations (including CDT) and entities covered by HIPAA.[7] In addition, CDT in 2010 issued a report with further guidance to regulators on how the provisions of the Markle Common Framework could be implemented in law.[8] Establishing these protections will likely require Congress to extend additional authority to HHS and/or the FTC.

Ensure Appropriate Limits on Downstream Uses of Data

As noted above, HIPAA applies only to "covered entities." However, under the HIPAA Privacy Rule, entities that contract with HIPAA covered entities to perform particular services or functions on their behalf using protected, identifiable health information (or PHI) are required to enter into "business associate" agreements.[9] Such agreements may not authorize the business associate to access, use or disclose information for activities that the covered entity itself could not do under HIPAA.[10] The agreements also are required to establish both the permitted and required uses and disclosures of health information by the business associate[11] and specify that the business associate "will not use or further disclose the information other than as permitted or required by the contract or as required by law."[12]

This combination of provisions demonstrates that HHS intended to place limits on what a business associate can do with health information received from a covered entity. However, one large national business associate has been accused of using data they receive from covered entities to support other business objectives,[13] and some privacy advocates have long suspected that such practices are more widespread.

---

[6] Under ARRA, PHRs that are offered to the public on behalf of covered entities like health plans or hospitals would be covered as business associates. Section 13408.
[7] See http://connectingforhealth.org/phti/#guide. A list of endorsers can be found at http://www.connectingforhealth.org/resources/CCEndorser.pdf.
[8] "Building a Strong Privacy and Security Framework for PHRs," http://www.cdt.org/paper/building-strong-privacy-and-security-policy-framework-personal-health-records (July 2010).
[9] 45 CFR 164.502(e)(1) & (2).
[10] 45 CFR 164.504(e)(2)(i).
[11] Id.
[12] 45 CFR 164.504(e)(2)(ii)(A)
[13] See http://www.alarmedaboutcvscaremark.org/fileadmin/files/pdf/an-alarming-merger.pdf, pages 14-16.

In ARRA Congress took a significant step toward strengthening accountability for business associates by making them directly accountable to federal and state regulators for failure to comply with HIPAA or the provisions of their business associate agreements.[14] HHS recently issued a proposed rule making it clear that accountability also extends to subcontractors of business associates, taking positive steps toward maintaining a consistent level of accountability for privacy and security protections as personal health data moves downstream.[15] CDT strongly applauds these actions.

However, CDT remains concerned that the HIPAA Privacy Rule is not sufficiently clear with respect to the important role of business associate agreements in placing clear limits on how business associates and their subcontractors can use and disclose patient data received from covered entities. The reports of business associates using health information to develop additional lines of business not directly related to the services they have been asked to perform by their covered entity business partners are either: (1) an indication that HIPAA is not being adequately enforced or (2) evidence that some business associate agreements are too permissive with respect to additional uses of information. In this testimony below CDT calls for stronger enforcement of HIPAA. Further, in comments to HHS CDT has urged revising the Privacy Rule to require business associate agreements to expressly limit the business associate's access, use and disclosure of data to only what is reasonably necessary to perform the contracted services.[16] Failure to appropriately account for and control downstream uses of data will jeopardize building trust in health IT.

Strengthen Protections Against Re-identification of HIPAA De-Identified Data

HIPAA's protections do not extend to health information that qualifies as "de-identified" under the Privacy Rule. As a result, covered entities may provide de-identified data to third parties for uses such as research and business intelligence without regard to HIPAA requirements regarding access, use and disclosure. In turn, these entities may use this data as they wish, subject only to the terms of any applicable contractual provisions (or state laws that might apply). If a third party then re-identifies this data – for example, by using information in its possession or available in a public database – the re-identified personal health information would not be subject to HIPAA.[17] It could be used for any purpose unless the entity holding the re-identified data was a covered entity (or had voluntarily committed to restrictions on use of the data).

There is value to making data that has a very low risk of re-identification available for a broad range of purposes, as long as the standards for de-identification are rigorous, and there are sufficient prohibitions against re-identification. Neither condition is present today. A number of researchers have documented how easy it is to re-identify some data that qualifies as de-identified under HIPAA.[18]

---

[14] ARRA, section 13404.
[15] 75 Fed. Reg. 40867-40924, at 40885 (July 14, 2010).
[16] http://www.cdt.org/comments/cdt-comments-hhs-proposed-rule (hereinafter, CDT Comments).
[17] If a covered entity has a reasonable basis for knowing that the recipient of "de-identified" data will be able to re-identify it, the data does not qualify as de-identified. See 45 C.F.R. 164.514(b)(2)(ii).
[18] See, for example, Salvador Ocha, Jamie Rasmussen, Christine Robson, and Michael Salib, Re-identification of Individuals in Chicago's Homicide Database, A Technical and Legal Study (November 2008), http://web.mit.edu/sem083/www/assignments/reidentification.html (accessed November 20, 2008).

Congress recognized this, and ARRA requires HHS to do a study of the HIPAA de-identification standard; that study, due in February 2010, is delayed. CDT has urged HHS to revisit the current de-identification standard in the Privacy Rule (in particular, the so-called "safe harbor" that deems data to be de-identified if it is stripped of particular data points) to ensure that it continues to present *de minimis* risk of re-identification.[19] However, Congress need not wait for the issuance of the study. To ensure consumers are protected, Congress should enact provisions to ensure data recipients can be held accountable for re-identifying data.

Encourage Use of Less Identifiable Data

Although the HIPAA provisions for de-identifying data need to be revisited and strengthened, CDT also believes that privacy risks are lessened when data has been anonymized to the greatest extent possible. In particular, many non-treatment uses of health data – including quality, research and public health – can be effectively done with data where sufficient patient identifiers have been removed to make it anonymous to the recipient. Unfortunately, federal and state privacy laws do not sufficiently promote the use of less identifiable data. Instead, they permit (in the case of HIPAA) or require (in the case of many state reporting laws) the use of fully identifiable data (including patient names, addresses, phone numbers, etc.), providing little incentive to remove identifiers from data before its use.

Under the collection and use limitations of fair information practices, data holders and recipients must collect, use and disclose only the minimum amount of information necessary to fulfill the intended purpose of obtaining or disclosing the data. The HIPAA Privacy Rule incorporates these principles in the "minimum necessary" standard, which requires covered entities to use only the minimum necessary amount of data for most uses and disclosures other than treatment. This standard is intended to be flexible, but HHS has not issued any meaningful guidance on this standard. As a result, covered entities and their business associates frequently express concerns about how to implement it, and CDT suspects that few covered entities or business associates take affirmative steps to minimize the identifiability of data.

The Privacy Rule does provide for two anonymized data options – de-identification (as discussed above) and the limited data set, which can be used for research, public health and health care operations). These data sets provide greater privacy protection for individuals, but are not useful for all purposes due to the number of identifiers that must be removed before the data can qualify for either option.

ARRA attempts to strengthen the Privacy Rule's collection and use limitations by strongly encouraging covered entities to use a limited data set to comply with the minimum necessary standard, as long as limited data is sufficient to serve the purposes for the data access or disclosure.[20] This section of ARRA also requires the HHS Secretary to issue guidance on how to comply with the minimum necessary standard. In comments to HHS, CDT has asked HHS to be clear in its guidance that covered entities

[19] See http://www.cdt.org/healthprivacy/20090625_deidentify.pdf for a more comprehensive discussion of CDT's views on the HIPAA de-identification standard.
[20] ARRA, Section 13405.

must address the identifiability of data in order to be in compliance with the minimum necessary standard.[21]

Tighten Rules Regarding Use of Patient Data for Marketing

The use of sensitive medical information for marketing purposes is one of the most controversial practices affecting health privacy. In health privacy surveys, use of data for marketing ranks as a top concern among respondents.[22] Consequently, protections against the unauthorized use of personal health information for marketing purposes are critical to building trust in new e-health systems.

The HIPAA Privacy Rule has provisions intended to limit the use of health data in marketing, but it historically was subject to a number of exceptions. There also has been little regulatory or legislative investigation of health marketing practices.

In ARRA, Congress took some steps to tighten the definition of "marketing" in the Privacy Rule. Under the new provisions, communications that are paid for or "subsidized" by third parties are marketing, and therefore require prior patient authorization – even if those communications would otherwise not be construed as marketing because they qualify for one of the existing exceptions. But even this new provision includes exceptions that could swallow the rule. For example, HHS has initially interpreted subsidized treatment communications to be outside the new ARRA rules requiring prior patient authorization. As a result, a covered entity can use a patient's data without consent to send her a letter urging her to switch to a different brand medication, even if that communication was paid for by the manufacturer of the medication.[23] Patients will experience these communications as marketing and mistrust any system that allowed this to happen without their authorization.

Strengthen Accountability/Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but those rules have never been adequately enforced.[24] The Office for Civil Rights (OCR) within HHS, charged with enforcing the HIPAA privacy regulations, had not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office found numerous violations of the rules.[25] The Justice Department had levied some penalties under the criminal provisions of the statute, but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limited the application of the criminal provisions to covered entities, forcing

---

[21] See CDT Comments, supra note 16.

[22] In the 2006 Markle Foundation survey referenced in footnote 1, 89% of respondents said they were concerned about marketing firms getting access to their personal health information online, and 77% described themselves as "very concerned." http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

[23] HHS did give patients the right to opt-out of receiving subsidized treatment communications, but an opt-out is not as protective of patient privacy as requiring prior consent.

[24] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008), http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

[25] Id. Although this story is two years old, to the best of our knowledge no civil monetary penalties have been assessed since that time. Over the last couple of years HHS has extracted monetary settlements (most recently from large chain pharmacies) for what were largely violations of the HIPAA Security Rule. In materials connected with these settlements, HHS made it clear that the amounts being paid in settlement of the alleged violations were not civil monetary penalties.

prosecutors to turn to other laws in order to criminally prosecute certain employees of covered entities who have criminally accessed, used or disclosed a patient's protected health information.[26]

A lax enforcement environment sends a message to entities that access, use and disclose protected health information that they need not devote significant resources to compliance with the rules. Without strong enforcement, even the strongest privacy and security protections are but an empty promise for consumers. Further, HIPAA has never included a private right of action, leaving individuals dependent on government authorities to vindicate their rights.

In ARRA, Congress took a number of important steps to strengthen HIPAA enforcement:[27]

- State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA, which puts more hands on the enforcement deck.
- As mentioned above, business associates are now directly responsible for complying with key HIPAA privacy and security provisions and can be held directly accountable for any failure to comply.
- Civil penalties for HIPAA violations have been significantly increased. Under ARRA, fines of up to $50,000 per violation (with a maximum of $1.5 million annually for repeated violations of the same requirement) can now be imposed.[28]
- HHS is required to impose civil monetary penalties in circumstances where the HIPAA violation constitutes willful neglect of the law.
- The U.S. Department of Justice can now prosecute individuals for violations of HIPAA's criminal provisions.
- The HHS Secretary is required to conduct periodic audits for compliance with the HIPAA Privacy and Security Rules. (The HIPAA regulations provide the Secretary with audit authority, but this authority has rarely if ever been used.)

The ARRA provisions are a major advancement in enforcement of federal health privacy laws, but enforcement is still lax. To strengthen accountability and further build public trust in health IT, CDT has two recommendations: (1) deem providers who are found to be in significant violation (either criminally responsible or found to be in willful neglect of the law) ineligible to receive subsidies under the federal health IT incentive program, and (2) provide individuals with a limited private right of action to enforce their HIPAA privacy rights.

With respect to the former (declaring a significant HIPAA violation to be a disqualification

---

[26] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences.
[27] See Sections 13409-13411 of ARRA.
[28] Of note, the increased penalties went into effect on the day of enactment – February 17, 2009. State Attorneys General are limited to the previous statutory limits - $100 per violation, with a $25,000 annual maximum for repeat violations.

for health IT subsidies), it is hard to justify providing tax dollars as a reward for meaningful use of health IT to an entity in significant violation of our nation's privacy laws.

With respect to a private right of action for privacy and security violations, CDT recognizes that providing such a right for every HIPAA complaint – no matter how trivial – would be inappropriate and disruptive. However, Congress should give consumers some right to privately pursue recourse in specific circumstances. For example, policymakers could create compliance safe harbors that would relieve covered entities and their business associates of liability for violations if they meet the privacy and security standards but would allow individuals to sue if they could prove the standards had not been met. Another suggestion is to limit the private right of action to only the most egregious HIPAA offenses, such as those involving intentional violations or willful neglect.

Strengthen Accountability for Strong Security Safeguards

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 (which are required under the HIPAA Security Rule),
- 58% have no security personnel, and
- 50% reported spending 3% or less of organizational resources on security.[29]

The prospect of storing and moving personal health data electronically in an environment where security is a low institutional priority should give us all pause. We need – through certified electronic health record requirements and enhancements to the HIPAA Security Rule – stronger requirements with respect to data security, as well as more proactive education and guidance from regulators. Under the meaningful use incentive program, the certification requirements include a number of important security functionalities, including the ability to encrypt data in motion and at rest, the ability to generate an audit trail, and authentication and access controls.[30] However, there is no clear requirement, either in the meaningful use criteria or in the HIPAA Security Rule, to actually implement and routinely use these functionalities. Providers are required under meaningful use to perform a security risk assessment and respond to any deficiencies discovered, but this falls short of a clear requirement to implement or have a plan for implementing the functionalities required for EHR certification. CDT is continuing to advocate with regulators for strengthened security requirements. Providers with fewer resources (such as small physician practices) may need to have security requirements scaled up over time; policymakers should, however, consider imposing greater obligations on the

[29] See testimony of Lisa Gallagher, Senior Director of Privacy & Security, HIMSS, http://healthit.hhs.gov/portal/server.pt?open=512&objID=1817&parentname=CommunityPage&parentid=28&mode=2&in_hi_userid=11673&cached=true (November 19, 2009).

[30] http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf.

connecting infrastructure to better address gaps or potential weak links as these systems develop.

Promote a Measured Role for Government in Health IT Standards

Although most of this testimony concerns health IT privacy and security, CDT would like to take this opportunity to reference a set of collaborative comments drafted by the Markle Foundation and endorsed by a broad range of stakeholders, including CDT. The comments concern the role of standards in health IT and urge a limited role for government in certifying health IT.[31] CDT asks that these comments also be included in the Subcommittee hearing record.

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.

[31] http://www.markle.org/downloadable_assets/20090430_meaningful_use.pdf (see in particular, section 4) and http://www.markle.org/downloadable_assets/20100510_collabcmts.pdf.