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 Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

YOUR HEALTH AND YOUR PRIVACY: PROTECTING HEALTH INFORMATION IN A DIGITAL WORLD

November 9, 2011

Chairman Franken 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.

We are at an important juncture in the effort to build a health care ecosystem powered by information technology. The nation is at the beginning of a five-year commitment to achieve widespread adoption and use of electronic medical records by health care providers. The health care system suffers from unsustainable costs and uneven or poor quality, and increased digitization and more robust sharing of health information is widely seen as key to reversing these trends. At the same time, the public consistently expresses concern about the privacy and confidentiality of digital health records. Changes to federal health privacy laws enacted by Congress in 2009 have not been implemented due to regulatory delays, and breaches of electronic health data are far too common.

Failure to build and maintain public trust in the collection and sharing of electronic health information will doom efforts to leverage health information technology (health IT) to promote innovation in the health care sector. In this testimony we discuss some of the key privacy and security challenges that will need to be addressed in

order to provide a firm foundation for realizing the benefits of 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] In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information.[2]

Health IT has a greater capacity to protect sensitive personal health information than is the case with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing among health care system entities for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption and similar technologies can reduce the risk to sensitive data when a system is breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, the perpetrators will be detected and punished.

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. Tens of thousands of health records can be accessed or disclosed through a single breach. In early October of this year, private medical data for nearly 20,000 emergency room patients at Stanford University Hospital were breached by a billing

---

[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). In the most recent survey conducted by the Markle Foundation, more than 80% of both the public and doctors surveyed said that requiring protections and safeguards for patient privacy was important. http://www.markle.org/publications/1443-public-and-doctors-agree-importance-specific-privacy-protections-health-it (January 2011).

[2] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006).

contractor.[3] Just the month before, Science Applications International Corporation (SAIC) reported a breach of personal medical information from 4.9 million military clinic and hospital patients due to a theft of back-up tapes from an SAIC employee's car.[4] Sadly, such incidents are all too common, with 364 breaches of greater than 500 patient records having been reported to HHS since implementation of federal breach notification rules covering health care entities in 2009.[5] The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[6]

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[7] Without appropriate protections for privacy and security in the healthcare system, people will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[8] Such privacy-protective behaviors include failing to seek care for sensitive medical conditions, asking health care providers to leave sensitive information out of the medical record, and traveling outside of the area to seek care.[9] According to a 2007 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.[10] A September 2011 study by the New London Consulting commissioned by FairWarning®, a vendor of breach detection software, found that:

- 27.1% of respondents stated they would withhold information from their care provider based on privacy concerns.

---

[3] http://www.nytimes.com/2011/10/06/us/stanford-hospital-patient-data-breach-is-detailed.html?src=twrhp.

[4] Id.

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[6] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[7] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[8] Id.

[9] Id.

[10] Harris Interactive Poll #27, March 2007. 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. National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

- 27.6% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.

- Greater than 1 out of 2 persons said they would seek care outside of their community due to privacy concerns, and 35% said they would drive more than 50 miles to seek care.[11]

The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;

- Their health care providers' ability to diagnose and treat them accurately may be impaired;

- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and

- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[12]

Contrary to the views expressed by some, privacy is not the obstacle to great adoption of 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**.

It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult —and more expensive—than building it at the start. Now, in the early stages of health IT adoption, is the critical window for addressing privacy.

We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

To build and maintain the public's 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:

- Policies to implement core privacy principles, or fair information practices;[13]

---

[11] http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-US-PATIENT-SURVEY.pdf

[12] Protecting Privacy, supra note 7.

- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.[14]

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 three years ago. The privacy provisions enacted in the stimulus legislation – commonly referred to as HITECH (Health Information Technology for Economic and Clinical Health Act) or ARRA (American Recovery and Reinvestment Act) – are an important first step to addressing the gaps in privacy protection. However, more work is needed to assure effective implementation of those privacy provisions and address issues not covered by (or inadequately covered by) the changes in HITECH.

In the testimony below, we call for:

- Prompt release by the Administration of final regulations to implement the HIPAA Privacy and Security Rule changes mandated by HITECH;
- Strengthened accountability through greater transparency about enforcement of privacy and security rules;

---

[13] 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.

[14] 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).

- Baseline privacy and security legal protections for personal health information not covered by HIPAA;
- Appropriate limits on downstream uses of health information by contractors or "business associates;"
- Strengthened accountability for implementing strong security safeguards, like encryption; and
- Protections against re-identification of HIPAA de-identified data.

Addressing Health IT Key Privacy and Security Concerns

Issuance of final regulations to implement the HIPAA Privacy and Security Rule changes mandated by HITECH

Congress enacted a number of important modifications to the HIPAA Privacy and Security Rules to strengthen their protections as the nation moves rapidly to the widespread adoption of electronic health records. Such modifications included:

- Extension of accountability for complying with the HIPAA Privacy and Security rules to contractors (business associates and their subcontractors);
- Requirements to notify individuals and HHS in the event of a breach of health information;
- Strengthening prohibitions on using a patient's personal health information for marketing purposes without the patient's express authorization;
- Clarifying that patients have the right to an electronic copy of any medical information about them that is stored electronically;
- Prohibitions on the sale of personal health information;
- A new right for patients to prohibit the sharing of personal health information with insurers when the patient pays out-of-pocket for care; and
- Stronger enforcement provisions, including higher civil monetary penalties; mandates on HHS to audit entities covered by HIPAA and to pursue violations indicating willful neglect of the law; clarity that individuals can be prosecuted for criminal violations of HIPAA; and express authorization of state attorneys general to enforce HIPAA.

A proposed rule to implement most of the above provisions was issued in July 2010; the comment period closed September 13, 2010. (The exception is the rule requiring notification of individuals in the event of a breach, which was required by Congress to be promulgated in interim final form no later than 180 days after enactment of

HITECH.[15] That interim final rule was made effective as of September 23, 2009, although HHS is expected to respond in the main HITECH rulemaking to comments submitted to that interim final rule.) More than a year later, the final, "omnibus" rule to implement most of these HITECH changes has not yet been issued by HHS, and the latest prediction of release is not until early 2012. In the meantime, providers are actively adopting electronic health records with federal tax dollars authorized by Congress without the benefit of the privacy protections that Congress recognized were important to build public and stakeholder trust in health IT. Congress established an effective date for most of the HIPAA changes mandated by HITECH of 12 months post enactment, or February 2010.[16]

We have seen that it is possible to have regulations released when the Department of Health and Human Services (HHS) believes them to be high priority. The Centers for Medicare and Medicaid Services moved quickly in adopting the rules governing the new Medicare Shared Savings Program under the Affordable Care Act. The comment period for that proposed rule closed on June 6, 2011 – and just over four months later, the final rules were issued. HHS and the Administration should prioritize the release of these rules and ensure that they are issued without further delay.

Strengthen Accountability/Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but until recently, those rules have never been adequately enforced.[17] From 2003 (the date when HIPAA regulations went into effect for most entities) through 2010, the Office for Civil Rights (OCR) within HHS, charged with enforcing the HIPAA privacy regulations, did not levy a single civil monetary penalty against a HIPAA-covered entity, even though that office found numerous violations of the rules.[18] 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 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.[19]

A lax enforcement environment sends a message to entities that access, use and

[15] Section 13402(j) of HITECH.

[16] Section 13423 of HITECH.

[17] "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.

[18] Id. 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.

[19] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences.

disclose personal 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 and patients.

In HITECH, Congress took a number of important steps to strengthen HIPAA enforcement:[20]

- State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA, which puts more hands on the enforcement deck.

- Contractors or business associates to entities covered by HIPAA 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 HITECH, 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.[21]

- 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 (DOJ) 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 HITECH provisions are a major advancement in enforcement of federal health privacy law, and there was an uptick in enforcement activity in early 2011. OCR issued its first civil monetary penalty of $4.3 million on February 21, 2011, against Cignet Health of Maryland for failing to provide patients with requested copies of their medical records and not cooperating with OCR's investigation.[22] In the same week, they reached a $1 million monetary settlement and executed a corrective action plan with Massachusetts General Hospital for failing to secure health data (paper copies of HIV patient records were left on the subway).[23] In 2011, OCR also began training

[20] See Sections 13409-13411 of ARRA.

[21] 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.

[22] http://cdt.org/blogs/harley-geiger/first-hipaa-civil-monetary-penalty.

[23] http://www.fiercehealthcare.com/story/patient-info-lost-subway-earns-mgh-1-million-hipaa-fine/2011-02-25.

state attorneys general on HIPAA enforcement;[24] OCR also requested a $5.6 million increase for its FY2012 budget in order to more effectively comply with enforcement mandates.[25] It is unclear whether this increased recent activity will translate into a sustained, consistent pattern of enforcement activity from OCR.

In addition, OCR rarely provides routine guidance, such as answers to frequently asked questions, to clarify how the rules apply to new circumstances or new technologies. Building public trust in health IT will require a greater understanding on the part of patients and industry stakeholders about health privacy law and policy. HHS should provide regular and proactive communication to both industry and consumers about rights under the law, compliance, best practices, and frequently asked questions. Where uncertainty or misinformation about the law is an obstacle to facilitating the exchange of data that needs to occur to improve our health care system, it should be HHS' job to resolve that.[26]

To strengthen accountability and further build public trust in health IT, CDT has three recommendations: (1) as noted above, increase the amount of informal guidance on compliance with Privacy and Security Rules; (2) increase transparency about HIPAA violations and enforcement activity by OCR and DOJ; and (3) deem providers found to be in *significant* violation of HIPAA (either criminally responsible or found to be in willful neglect of the law) ineligible to receive subsidies under the federal health IT incentive program.

With respect to the second recommendation, OCR issues reports on an annual basis that contain summary statistics such as the number of HIPAA complaints received that year, the general category of the complaint, the number of complaints that were dismissed, the number that were resolved through voluntary corrective action, and the number that were further investigated and pursued. These statistics are helpful but tell us very little about the areas of HIPAA noncompliance that need further attention; they also tell us very little about whether the agency with oversight over HIPAA is doing a good job. Congress should consider requiring greater transparency about enforcement activity from both HHS and DOJ. Such transparency could include more details about the types of violations being reported, more detail about complaints that are handled through seeking voluntary corrective action (which could be done with a random sample if reporting on all such dispositions would be overly burdensome), more detail about the size and type of entities that are the subject of complaints, and more information about the disposition of complaints that are referred by OCR to DOJ for criminal prosecution – all of which could be accomplished without revealing the name of the provider or institution who is the subject of an investigation that may not result in fines or charges.

---

[24] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/sagmoreinfo.html.

[25] http://healthcare.cmtc.com/2011/03/office-for-civil-rights-seeks-additional-funding-for-data-breach-policing/.

[26] http://www.ihealthbeat.org/Perspectives/2009/HHS-Holds-Keys-to-Next-Generation-of-Health-Privacy.aspx%5D

With respect to the third recommendation (declaring a significant HIPAA violation to be a disqualification for health IT subsidies), the Health IT Policy Committee recommended that HHS institute such a policy before the health IT financial incentive program went into affect in 2011.[27] If the purpose of seeking greater enforcement of HIPAA is to build public trust in the use of health IT, it is hard to justify providing taxpayer funds for use of health IT to an entity in significant violation of our nation's privacy laws.

Ensure Appropriate Limits on Downstream Uses of Data by Contractors/Business Associates

HIPAA is not a health data privacy law; instead, the privacy and security regulations under HIPAA cover only certain entities in the health care system – health care providers, insurers, and healthcare clearinghouses – reflecting a limit to the statutory reach of HIPAA.[28] However, HHS also understood that HIPAA covered entities would need to be able to share data with contractors to support routine operations. 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.[29] The agreements are required to establish both the permitted and required uses and disclosures of health information by the business associate[30] 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."[31]

This combination of provisions suggests that HHS intended to place limits on what a business associate can do with health information received from a covered entity. However, other provisions of the business associate rules are less clear that business associates must be restricted in how they can use and disclose information received from a covered entity. For example, the Privacy Rule provides that covered entities may not authorize the business associate to access, use or disclose information for activities that the covered entity itself could not do under HIPAA, *except* that the contract may permit the business associate to use and disclose protected health information for the "proper management and administration of the business associate" and for "data aggregation" services related to the covered entities' operations.[32] Thus, if an activity to "manage" a business associate would be prohibited by HIPAA, the business associate agreement is still permitted to authorize

---

[27] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911073_0_0_18/PSWG%20Recommendation%20Letter_Regs_final.pdf; see also https://www.cdt.org/blogs/deven-mcgraw/hhs-releases-rules-electronic-health-records.

[28] Section 1172 of the Social Security Act; 45 CFR 164.104.

[29] 45 CFR 164.502(e)(1) & (2).

[30] Id.

[31] 45 CFR 164.504(e)(2)(ii)(A)

[32] 45 CFR 164.504(e)(2)(i).

the business associate to perform this activity. In addition, business associate agreements may permit the business associate to use protected health information to "carry out its legal responsibilities."[33]

Privacy advocates have long suspected that some business associate agreements do not tightly restrict a business associate's use of personal health information. One large national business associate has been accused of using data they receive from covered entities to support other business objectives.[34] Recently CDT has reviewed an electronic health record vendor agreement that authorizes the vendor/business associate to use information from the EHR for any purpose not prohibited by HIPAA (e.g., not just acting on behalf of the provider). We also have heard anecdotal reports of a business associate agreement with a medical device manufacturer also authorizing the manufacturing to use information from the device for its own business purposes. The extent of this problem is not known, because, to the best of our knowledge, OCR does not audit business associate agreements – and if such audits are occurring, the results have not been publicly shared.

In HITECH Congress took a significant step toward strengthening oversight 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.[35] In the proposed rule to implement the HITECH changes, HHS proposed extending this accountability 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.[36] CDT strongly applauds these actions.

However, CDT remains concerned that the HIPAA Privacy Rule is still 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: (1) an indication that HIPAA is not being adequately enforced, and/or (2) evidence that some business associate agreements are too permissive with respect to additional uses of information. In this testimony CDT calls for stronger enforcement of HIPAA, and this should include stronger oversight of business associates and business associate agreements. 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

[33] 45 CFR 164.504(e)(4)(i).

[34] See http://www.alarmedaboutcvscaremark.org/fileadmin/files/pdf/an-alarming-merger.pdf, pages 14-16.

[35] ARRA, section 13404.

[36] 75 Fed. Reg. 40867-40924, at 40885 (July 14, 2010).

data to only what is reasonably necessary to perform the contracted services.[37] Failure to appropriately account for and control downstream uses of data will jeopardize trust in health IT.

Establish protections for health data not covered by HIPAA

As noted above, HIPAA covers only covered entities and the contractors/business associates who provide services on their behalf. But health information is being increasingly shared on the Internet and stored in mobile devices, largely due to an explosion of health and wellness products and services that are aimed at, and largely used by, consumers. 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.

According to the Pew Research Center's Internet & American Life Project, a whopping 80% of Internet users look for health information on-line.[38] This represents 59% of total U.S. population, since not everyone is on-line. Searching for health information is the third most popular on-line pursuit (behind e-mail and use of a search engine), with searches for symptoms and treatments the most common. About 50% of those searching for health information on-line say they are looking "on behalf of someone else."[39] Individuals are increasingly participating in social networking sites dedicated to sharing health concerns.[40] Today there are 9,000 consumer health apps available in the Apple store, and research2guidance estimates that about 500 million people will be using mobile health apps by 2015.[41] Consequently, Internet search providers, app developers, and mobile service providers have access to, and/or are storing and sharing, sensitive health information – and none of them are covered by federal health privacy and security rules.[42]

Personal health records (PHRs) provide opportunities for consumers to store and share electronic copies of their health information and are being offered by Internet companies like Microsoft,[43] No More Clipboard,[44] or by employers, such as through

---

[37] http://www.cdt.org/comments/cdt-comments-hhs-proposed-rule (hereinafter, CDT Comments).

[38] http://www.pewinternet.org/Reports/2011/HealthTopics.aspx.

[39] Id.

[40] http://cdt.org/blogs/harley-geiger/social-networking-sites-—-they're-not-just-revolutions-anymore. A list of some of these sites, also called "e-patient communities," can be found at http://epatientdave.com/communities/.

[41] http://www.research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/.

[42] Some may be covered as "business associates" if they are providing a service on behalf of an entity covered by HIPAA – but most of these entities provide services directly to consumers.

[43] http://www.microsoft.com/en-us/healthvault/.

the Dossia Consortium.[45] Only seven percent of individuals report using a PHR -– but that number has doubled since 2008.[46] PHRs also are not covered by the HIPAA regulations unless they are being offered to consumers by HIPAA covered entities or business associates acting on the covered entity's behalf. (Kaiser offers a PHR to its enrollees, and this PHR is covered by HIPAA because it is offered to individuals by a covered entity (Kaiser).) In HITECH, Congress mandated breach notification for PHR vendors – but beyond that law, 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.[47]

HHS recently released a model privacy notice, intended to help consumers compare the privacy policies of entities offering PHRs.[48] HHS describes it as a "nutrition label" for privacy policies. We applaud this effort and the willingness of the PHR vendors mentioned above to volunteer to be part of this initiative. Although it may help consumers navigate an often-confusing PHR marketplace, it is no substitute for a comprehensive set of privacy and security policy protections that apply to health data stored and shared on the Internet.

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 and other consumer health tools. 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 or other health applications, where consumers should be in more control of their records, and may do more harm than good. Further, it may not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to

---

[44] http://www.nomoreclipboard.com/.

[45] http://www.dossia.org//.

[46] http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.

[47] 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.

[48] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_4108_1176_15440_43/http%3B/wci-pubcontent/publish/onc/public_communities/p_t/privacy_and_security/model_phr_privacy_notice_home_portlet/files/phr_model_privacy_notice_backgrounder___final.pdf.

take the lead in enforcing consumer rights and protections with respect to Internet and mobile health tools.

CDT applauds Congress for not extending HIPAA to cover all PHRs.[49] In HITECH, Congress did enact provisions requiring PHR vendors to notify individuals and the FTC in the event of a breach of personal information, and this was a positive step forward. Congress also 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.[50] 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.[51] Establishing these protections will likely require Congress to extend additional authority to HHS and/or the FTC.

Congress also should ensure that bills to protect consumer privacy on the Internet include protections for health data. At present, most privacy legislation pending in Congress does not offer specific protections to health data. The Commercial Privacy Bill of Rights Act, sponsored by Senators Kerry and McCain, does apply privacy protections to "information related to a particular medical condition or health record."[52] Likewise, Senator Blumenthal's Personal Data Protection and Breach Accountability Act of 2011 would ensure that companies not covered by HIPAA would notify individuals in the event of a breach their sensitive health information.[53] These bills take an important step forward in safeguarding health information outside of HIPAA, and CDT hopes that other commercial privacy and data breach bills do the same. The sensitivity of medical data is too great to leave out the privacy protections needed for the evolving marketplace for commercial health information.

---

[49] 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.

[50] See http://connectingforhealth.org/phti/#guide. A list of endorsers can be found at http://www.connectingforhealth.org/resources/CCEndorser.pdf.

[51] "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).

[52] S.799, The Commercial Privacy Bill of Rights Act of 2011, Sec. 3(6)(B)(i).

[53] S.1535, Personal Data Protection and Breach Accountability Act of 2011, Sec. 3(15)(F)(iv).

Strengthen Accountability for Strong Security Safeguards

The Health Information Management Systems Society (HIMSS) releases an annual study of data security initiatives adopted by hospitals and outpatient care centers. The data from the 2011 survey was released just last week:

- Nearly one-quarter of respondents say their organization does not conduct annual risk assessments (which are required under the HIPAA Security Rule);
- Only about half say their organization has a chief security officer, chief information security officer, or another full-time staff member to handle data security responsibilities;
- 53% reported spending 3% or less of organizational resources on security; and
- 14% said at least one patient had reported a case of medical identity theft during the last year.[54]

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 HITECH EHR incentive program, the certification requirements for EHRs 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.[55] However, there is no clear requirement, either in the criteria for eligibility for a stimulus payment or in the HIPAA Security Rule, to actually implement and routinely use these functionalities. OCR should provide guidance to providers with certified EHR systems with respect to implementing the security functionalities built into those systems; to date, no such guidance has been issued.

The new breach notification provisions of HITECH provide an incentive for health care providers to encrypt health information using standards approved by the National Institute of Standards and Technology (NIST). Specifically, entities are not required to notify individuals or HHS of a breach if the information that is breached is encrypted, and the encryption key has not been stolen or compromised. This safe harbor for encryption was enacted to provide a strong incentive for health care providers to encrypt. But we know from the statistics on breaches that have occurred since the notification provisions went into effect in 2009 that the health care industry appears to be rarely encrypting data. To the best of our knowledge, no one has done a comprehensive study of the reasons why the health care industry has not embraced the use of encryption.

---

[54] http://www.ihealthbeat.org/articles/2011/11/4/data-security-makes-up-small-portion-of-health-organization-it-budgets.aspx.

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

We note that at least two-thirds of the breaches that have been reported to HHS have been due to lost or stolen media (laptops, computers and thumb drives), none of which was encrypted at the time of the theft.[56] Because this represents the highest risk of exposure for PHI, CDT urges policymakers to focus on strengthening incentives for encryption – or requiring it – for media that are at high risk for theft or loss. For example, HIPAA rules could be strengthened to require encryption in these cases. As an alternative, encryption could continue to be "addressable" under the Security Rule (not required but strongly encouraged), and OCR could issue guidance on the factors OCR will use in evaluating decisions not to encrypt health data on media at risk of theft or loss. The cost of encryption varies depending on the amount of data to be protected and the encryption tool chosen – but most solutions for media at risk of theft or loss appear to be cheaper than the cost of a breach. Ponemon Institute has estimated the cost of a healthcare breach to be $294 per individual affected by the breach.[57] The mean breach size reported to HHS is about 38,000 individuals – at a cost of $294 per individual, that's a cost of over $11 million.[58]

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 voluntary 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.[59] 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 suggested it may be

---

[56] http://www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml.

[57] http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.

[58] From a webinar conducted by Dixie Baker, SAIC, Encryption: Making the Business Case, http://www.healthcareinfosecurity.com/webinarsDetails.php?webinarID=233.

[59] 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).

relatively easy it is to re-identify some data that qualifies as de-identified under HIPAA.[60]

Congress recognized this, and ARRA requires HHS to do a study of the HIPAA de-identification standard; that study, due in February 2010, is significantly 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 categories) to ensure that it continues to present *de minimis* risk of re-identification.[61] CDT recently held a workshop on HIPAA de-identification attended by industry stakeholders and consumer groups, and we will be releasing a set of specific policy recommendations in the coming months. We will share these with the subcommittee when they are ready.

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.

---

[60] 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).

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