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

Before the
National Committee on Vital and Health Statistics
Subcommittee on Privacy, Confidentiality & Security

Hearing on Personal Health Records

June 9, 2009

Thank you for holding this hearing on personal health records and for the opportunity to testify. CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works to keep the Internet open, innovative and free by developing practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation. The Health Privacy Project, which has more than a decade of experience in advocating for the privacy and security of health information, was merged into CDT last year to take advantage of CDT's long history of expertise on Internet and information privacy issues. Our mission is to develop policies and practices that will better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

Surveys consistently demonstrate the support of the American public for health IT. At the same time, however, the public is very concerned about the risks health IT poses to health privacy. A system that makes greater volumes of information available more efficiently to improve care will be an attractive target for those who seek personal health information for commercial gain or inappropriate purposes. Building public trust in health IT systems is critical to realizing the technology's potential benefits. While some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT can bring, it is clear that the opposite is true: enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits.

This is particular true in the case of personal health records. Personal health records (PHRs) hold significant potential for consumers and patients to become

key, informed decision-makers in their own health care. PHRs can be drivers of needed change in our health care system by providing individuals with options for storing and sharing copies of their health records, as well as options for recording, storing, and sharing other information that is relevant to health care but is often absent from official medical records (such as pain thresholds in performing various activities of daily living, details on side effects of medication, and daily nutrition and exercise logs). However, in order to feel comfortable using PHRs, consumers need assurance that their information will be protected by reasonable privacy and security safeguards.

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 adoption of PHRs, is the critical window for addressing privacy.

Our testimony below discusses the need for a comprehensive privacy and security framework to protect consumers using personal health records and pave the way for the more widespread adoption of these potentially transformative tools; a model for such a framework; the need for (and lack of) consistent policies governing PHRs; and why the HIPAA Privacy Rule – in its current form – is not appropriate vehicle for protecting the privacy of consumers using PHRs.

Why Privacy and Security Protections are Critical

Recent survey data from the Markle Foundation shows that consumers see the enormous potential of PHRs – but that privacy and security concerns are a major factor impeding their adoption. According to this survey, released in June 2008, four in five U.S. adults believe that electronic personal health records (PHRs) would help people:

- Check for errors in their medical records (87 percent).
- Track health-related expenses (87 percent).
- Avoid duplicated tests and procedures (86 percent).
- Keep their doctors informed of their health status (86 percent).
- Move more easily from doctor to doctor (86 percent).
- Manage the health of loved ones (82 percent).
- Get treatments tailored to health needs. (81 percent).

- Manage their own health and lifestyle (79 percent).[1]

Only a small percentage of survey respondents – 2.7% – reported having a PHR, although among this group, four in five described their PHR as "valuable."[2] Of those who said they were not interested in having a PHR, more than half (57%) cited privacy concerns as a reason. Specifically, 24% reported their privacy concerns as high; 49-56% characterized them as moderate; and only 20-27% reported their privacy concerns as low.[3] According to Alan Westin, who designed the survey, "[t]his pattern of health privacy intensity suggests that [73-80%] of the public will want to be assured of robust privacy and security practices by online PHR services, if they are to join those offerings."[4] It is clear that privacy and security protections are needed to spark greater interest in and use of PHRs.

We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust in PHRs

To build public trust in PHRs and similar consumer-based health tools, we need a comprehensive privacy and security framework that targets the risks to consumers using them and is flexible enough to allow for innovation to meet a wide array of consumer needs. Policymakers need not start from scratch in developing this framework. In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information, [5] outlining consensus privacy and security policies for PHRs and other "consumer access" services. This framework — which was developed and supported by a diverse and broad group including technology companies, consumer organizations like CDT, and HIPAA-covered entities[6] — was designed to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices. It includes four overviews and 14 specific technology and policy approaches for consumers to access health services, to obtain and control

[1] http://www.connectingforhealth.org/news/pressrelease_062508.html.

[2] Id.

[3] Id.

[4] Id.

[5] See www.connectingforhealth.org/phti.

[6] See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at the following URL: http://www.connectingforhealth.org/resources/CCEndorser.pdf.

copies of health information about them, to authorize the sharing of that information with others, and sound privacy and security practices.[7]

The American Recovery and Reinvestment Act of 2009 (ARRA or the economic stimulus legislation) requires HHS (in consultation with the FTC) to report to Congress no later than February 18, 2010, with recommendations for privacy and security requirements for PHR vendors and related entities that are not covered by HIPAA as either covered entities or business associates.[8] In recent public comments, we urged HHS to rely on the Markle Connecting for Health framework in developing its recommendations.[9] CDT also recently held an all-day workshop on PHRs, bringing together major vendors, patients, consumer organizations, other health care stakeholders and "health 2.0" innovators to begin addressing the question of which elements of the framework should be incorporated into regulations and which should be enforced through other mechanisms like chain-of-trust agreements and business best practices. We will issue a paper with more specific recommendations for regulating PHRs this summer.

PHRs should be Governed by Consistent Policies; Current Federal Policies are Insufficient or Inadequate

Among the policies endorsed in the Markle framework is that individuals should have the choice of whether or not to open a PHR account, and they should choose what entities may access or exchange information into or out of that account.[10] This foundational policy is reflected in the definition of a PHR in the economic stimulus legislation: "an electronic record of information on an individual "that is managed, shared, *and controlled by or primarily for the individual.*"[11]

At the core of the framework is the belief that PHRs should be governed by a consistent and meaningful set of privacy and security policies, regardless of the type of entity offering them. It will be confusing and potentially harmful to consumers to have different protections and rules for PHRs depending on the legal status or business model of the offering entity, and even more so if the

[7] For a short summary of the overview and principles, please see http://www.connectingforhealth.org/resources/CCPolicyBrief.pdf.

[8] Section 13424(b) of ARRA.

[9] http://www.cdt.org/healthprivacy/20090521_RFI_coments.pdf

[10] See http://www.connectingforhealth.org/phti/reports/cp3.html.

[11] Section 13400 of ARRA.

policies do not consistently support meaningful consumer participation in and control of these emerging and powerful tools.

There is no such consistent regulatory framework in place today. PHRs are regulated by HIPAA only if they are offered by covered entities or business associates acting on their behalf. If they are not regulated by HIPAA, as is the case for most PHRs offered by Internet companies and employers,[12] consumer privacy may be protected only by the PHR provider's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the Federal Trade Commission (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.[13] In some cases, other federal laws that govern storage and transmission of electronic communications or that regulate Internet sites may apply, but none provide comprehensive privacy and security protections for health information, and none were enacted specifically to protect consumers using PHRs.

The economic stimulus legislation provides opportunities to advance a consistent approach to regulating PHRs regardless of the source, but further action from the Administration is needed to make this a reality. The study to be conducted by HHS and FTC with respect to privacy and security for PHRs is only required to consider those not already covered by HIPAA. HHS should extend this study to look at creating a consistent set of regulations for PHRs across the board. Consistent with this view, CDT and the Markle Foundation jointly urged HHS, in implementing the new breach notification rules applicable to PHRs, to define a breach as the "acquisition, use or disclosure" of information in a PHR without the authorization of the individual.[14] We posited that this approach is required to appropriately implement the PHR definition in the stimulus legislation as being an electronic record of information on an individual "that is managed, shared, *and controlled by or primarily for the individual.*"[15] It is also consistent with the FTC's proposed breach notification standard, which requires notification when information in a PHR is acquired

---

[12] We note that HIPAA requires these entities to enter into business associate agreements with covered entities under some circumstances. See Section 13408 of ARRA.

[13] 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.

[14] http://www.cdt.org/healthprivacy/20090521_RFI_coments.pdf. We noted in our comments that our suggestions with respect to regulation of PHRs should not be interpreted to suggest any changes in the rules governing a covered entity's operational record (e.g., their legal medical record) and its permitted uses of data captured in such operational records of the covered entity.

[15] Id. (emphasis added).

without individual authorization.[16] We urge this Subcommittee and NCVHS to develop recommendations that support a consistent policy environment for consumers using PHRs.

Application of the HIPAA Privacy Rule – in Its Current Form - is Not the Answer

Although some PHRs are currently covered by HIPAA, the need for consistent policies does not make it appropriate to automatically extend HIPAA coverage in its current form to all PHRs. The HIPAA rules were based on fair information practices, and with respect to the sharing of health information among physicians, hospitals and health plans, HIPAA represents the foundation upon which a comprehensive framework of protections for e-health should be built. But HIPAA was specifically designed to regulate only the sharing of information among traditional health care system entities. As a result:

- personal health information is permitted to flow without patient authorization for treatment, payment, and health care operations;
- other uses are permitted without consent pursuant to certain procedures and safeguards (i.e., disclosure to researchers, law enforcement); and
- a number of uses—such as to employers or for marketing and any uses not expressly mentioned in the Privacy Rule— require express, uncoerced patient authorization, but the marketing provisions in particular have historically provided weak privacy protections.

These aspects of the Privacy Rule (among others) render it ineffective at protecting PHRs. As a result, application of the Privacy Rule in its current scope may do more harm than good.[17] In particular, the Privacy Rule's reliance on individual authorization for marketing and commercial uses places people in an unfair and potentially dangerous situation, shifting the burden of protecting privacy solely to the individual and putting the bulk of the bargaining power on the side of the entity offering the PHR. A few of the most troubling problems are:

- Research on consent on the Internet shows that most people do not read the details of consent forms before signing them, and those that do often do not understand the terms. Many wrongly assume that the existence of a privacy

[16] Section 13407(f)(1) of ARRA.

[17] Because of our concerns about relying on the HIPAA Privacy Rule to protect consumers using PHRs, we recently blogged about the need to narrowly interpret the provision in ARRA requiring vendors of PHRs to enter into business associate agreements and therefore be covered by HIPAA. See http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis/.

policy means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite. And for free web-based products like PHRs, consent to the statement of uses and disclosures (a.k.a. the "privacy policy") will likely be required in order to use the service. [18]

- A major business model to support third-party PHRs is advertising revenue and partnerships with third-party suppliers of health-related products and services. As a result, people using these tools will be more likely to be marketed to on the basis of health information in their PHI. They will likely be subjected to the tools that Internet companies typically use to gather information about consumer preferences (such as cookies), so that the companies can target them with specific ads or product offers. Their data may be more likely to be sold to third parties (such as pharmaceutical companies and health insurers). They also will likely be solicited by the PHR's formal and informal business partners (for example, diabetes management programs sponsored by the diabetes meter companies, weight loss and fitness programs, etc.), who also will likely solicit individuals to share their data and may use that data for multiple business purposes (including selling it).

For PHRs to flourish, we believe clear rules are needed regarding marketing and commercial uses of information that will better protect consumers by restricting PHR vendors from engaging in certain practices, or by providing individuals with certain rights—in other words, a much stronger and more comprehensive package of privacy and security safeguards than merely affording people the right to check a box acknowledging the uses and disclosures of their information. This may mean the application of certain provisions in HIPAA (for example, HHS should consider whether the HIPAA Security Rule provides adequate security protections for PHRs), but for the most part will require a different set of requirements.

If the Privacy Rule is nevertheless viewed as the appropriate vehicle for strengthening or expanding privacy protections for consumers who use PHRs, CDT believes the HHS Secretary should promulgate HIPAA rules specific to PHRs that respond to the unique issues they raise. (For just one example, the rules permitting covered entities to use personal health information without express authorization for treatment, purposes, and health care operations should not be applied to PHRs.) CDT further recommends that Secretary consult with the FTC, which has experience in issues related to online privacy and consumer protection, in developing these rules.

---

[18] For additional details on CDT's view of the role of individual consent in protecting health information, please see http://www.cdt.org/healthprivacy/20090126Consent.pdf.

Establishing Privacy Protections for PHRs

The economic stimulus legislation – which tasks HHS and FTC with jointly coming up with recommendations for privacy and security requirements for PHRs – is the right approach for ultimately establishing comprehensive privacy and security protections for consumers using these new health tools. As noted above, we hope HHS will consider establishing consistent rules regarding PHRs that are based on the Markle framework regardless of the type or legal status of the entities offering them. For PHRs offered by entities that are not part of the traditional health care system, it is critical that regulators understand the business model behind these products, which will largely rely on advertising revenue and partnerships with third-party suppliers of health-related products and services. Even for PHRs offered by HIPAA covered entities, consumer trust in these products will be built through a consistent set of rules regarding access to and disclosure of information.

As noted above, patients should have the right to control information in their PHRs, but relying solely or disproportionately on consumer authorization for use of information shifts the burden of protecting privacy solely to the consumer and puts the bulk of the bargaining power on the side of the entity offering the PHR. For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – such consumer consent should be situated within a clear framework of rules regarding marketing and commercial uses that will better protect consumers.

For example, in order to ensure that consumers do not inadvertently grant blanket authorization for use of their data, regulators may have to address the form and content of the terms of service and the privacy policies for systems offering PHR services. The foundation of PHRs should be opt-in (i.e., affirmative as opposed to implied consent), but even opt-in consent can be too general. Therefore, baseline regulatory standards might specify particular uses or disclosures for which independent consent must be obtained. For example, it might be required that consent to disclose data for marketing or commercial purposes must be obtained independently of other consent. Special consent might also be required for research uses of data, even if the data is de-identified or aggregated.

Policymakers may find it necessary to go further and prohibit certain uses or disclosures of data in PHRs, regardless of consent. Compelled disclosures pose a particular problem in the contexts of employment, credit or insurance, where individuals are often compelled to sign authorizations granting employers, banks, insurers, and others access to their health records for non-medical

purposes. While the problem of these disclosures, which are nominally voluntary but in fact compelled, applies to traditional health records, it is exacerbated with PHRs, which may contain not only copies of provider records but also user-generated data not revealed even to a doctor. If PHRs are to be encouraged, the best course may be to prohibit their use in the context of employment, credit or insurance. Congress has already moved in this direction with the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits employers from using genetic information to make employment decisions and prohibits health insurers from using such information to make coverage and underwriting determinations. Under GINA, individuals cannot be asked for permission to use their genetic information for these purposes.[19]

A comprehensive privacy framework would also include limits on downstream recipients of data from PHRs. As noted above, the revenue model to support many Internet-based PHRs will be partnerships with third parties who will offer services or "applications" to PHR account holders, which means a consumer's PHR data may pass to many organizations. Contractual agreements will be necessary to bind business partners to particular privacy and security policies, such as a commitment not to re-disclose the data or to use it for purposes other than those for which consent was granted. However, such contractual commitments will be insufficient to build consumer trust in PHRs. Even if such contracts were required to contain certain elements, consumers could not be assured of consistent enforcement.

Conclusion

To establish greater public trust in PHRs and pave the way for their adoption, we need a comprehensive and consistent privacy and security framework that is vigorously enforced. The Markle Common Framework for Networked Personal Health Information, developed through a multi-stakeholder process and endorsed by a broad group of stakeholders, provides a consistent policy framework for PHRs. HHS and FTC should consider which elements of the framework should be imposed by regulation and which should be adopted through other mechanisms. From traditional health entities to new PHR developers to policymakers, all have an important role to play in protecting consumers using PHRs.

[19] The Johns Hopkins University, Genetics and Public Policy Center, Summaries of GINA Title I (Health Insurance) and GINA Title II (Employment), http://www.dnapolicy.org/resources/GINATitle1summary.pdf and http://www.dnapolicy.org/resources/GINATitleIIsummary.pdf (accessed November 20, 2008).

Thank you for the opportunity to present this testimony. 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