Health Information Privacy: Current Trends, Future Opportunities

March 17, 2010

CDT is a non-profit public interest organization founded in 1994 and dedicated to keeping the Internet open, innovative and free. With offices in Washington, DC and San Francisco, CDT works with all interested stakeholders to develop and advance public policies, corporate practices and technology designs that enhance free expression, privacy, and democratic participation. Through research, dialogue, and advocacy, CDT's Health Privacy Project is promoting pragmatic, effective actions to better protect the privacy and security of electronic health information and build consumer trust in a wired health care system, so that the benefits of health information technology can be realized. CDT's work on consumer privacy on the Internet focuses on protecting the privacy of consumer's health information on-line, as consumers increasingly use the Internet to access and share health information on-line. This FTC roundtable touches on CDT's work in these areas.

Thank you for the opportunity to submit these comments to the Third Roundtable on Privacy. Those expressed here focus on protections for health information as part of electronic medical records kept by traditional participants in the health care system (such as physicians and other care providers, hospitals, and health plans), and personal health records, which are commonly offered by Internet companies and allow consumers to store and share copies of their health information with their health care providers and others as they see fit. We also briefly address FTC's specific question for this Roundtable on different standards for minors. CDT also is separately submitting comments for this Roundtable on identity management and submitted comments for previous Roundtables on on-line privacy with respect to sensitive personal information, including health.

Privacy and Security Protections Are Critical to Achieving the Benefits of Health IT

Health information technology (health IT) and electronic health information exchange have the potential to improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. Survey data shows that Americans are well aware of and eager to reap the benefits of health IT. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers – because they believe such access is likely to increase their quality of care.

At the same time, however, people have significant concerns about the privacy of their medical records, posing the risk that people will not trust, and therefore will not use, electronic health records systems if they do not protect privacy and security. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[1] In a 2006 survey, when Americans were asked about online health information:

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

- 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]

These concerns are well founded. As the repeated reports of both small-scale browsing and large-scale breaches demonstrate, serious vulnerabilities exist now and could grow with the increasing flow of data. With computerization, tens or hundreds of thousands of health records can be accessed or disclosed through a single breach.

Protecting privacy is important not just to avoid harm, but because good healthcare depends on accurate and reliable information. [3] Without appropriate protections for privacy and security in the healthcare system, patients will withhold information from their health providers due to worries about how the medical data might be disclosed.[4] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[5] 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.[6]

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

- The quality of care these patients receive may suffer;
- Their willingness to access health information on-line and seek support from social networking sites will be diminished;
- 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.[7]

These concerns must be addressed – and it is possible to do so. Privacy and security should not be an impediment to adoption of health IT. To the contrary, sound privacy and security policies, implemented in law, corporate practice and technology design, can enable health IT. Indeed, electronic systems, properly designed and managed, have a greater capacity to protect personal health information than is the case now 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.

---

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

[3] 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).

[4] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

[5] Harris Interactive Poll #27, March 2007.

[6] 2005 National Consumer Survey.

[7] Id.

Electronic health information networks can be designed to facilitate data sharing for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been breached. Privacy and security practices are not 100% foolproof, but the virtual locks and data management tools made possible by technology can make it more difficult for bad actors to access health information and can help ensure that, when there is abuse, the perpetrators will be detected and punished.[8]

The American Recovery and Reinvestment Act of 2009 (ARRA)[9] included a number of improvement to federal health information privacy rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), many of which had been recommended by CDT.[10] However, these provisions present numerous implementation challenges, and gaps in protections remain to be filled. Current policies still fall short of the comprehensive framework of privacy and security protections that will enable us to realize the tremendous potential of health IT. These comments touch on some of the critical work that lies ahead

We do need to act with some urgency. Privacy experts widely agree that it is often difficult or impossible to establish effective privacy protections retroactively. Restoring public trust that has been significantly undermined is much more difficult than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy. CDT and others call this "privacy by design."

A Basic Question: What Is Privacy?

A comprehensive privacy and security framework for health IT will --

- Implement core privacy principles;
- Adopt trusted network design characteristics; and
- Establish oversight and accountability mechanisms.

What do we mean by "core privacy principles?" Although privacy is one of the most deeply cherished of rights, it is also one of the most misunderstood concepts. We use the word "privacy" to mean many things, ranging from communications privacy (such as the privacy of email or telephone calls) to privacy in the context of intimacy, sexuality and the family. The specific aspect of privacy that is at issue in the health IT debate is "information privacy," which focuses on how information is used to provide a service to people or to make decisions about them. The concept of information privacy goes well beyond what is kept secret or hidden. After all, even without health IT, medical information flows from doctor to nurse to office administrator to pharmacy to insurance company to public health authority. The modern healthcare system is a complex eco-system with many entities requiring access to health data to deliver and pay for care. Even with the most rudimentary technology, information is copied, shared and used for a variety of purposes that go beyond treatment and payment. Health privacy must account for all these uses. Therefore health privacy, comprehensively conceived, would provide a set of rules for who gets access to what information, under what conditions, and for what purposes.

---

[8] See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

[9] Public Law 111-5 (referred to herein as ARRA).

[10] For a summary of the privacy provisions in ARRA, see http://www.cdt.org/healthprivacy/20090324_ARRAPrivacy.pdf.

This concept of privacy is sometimes referred to as "fair information practices," a term that conveys the notion that data will be used and exchanged but must be handled by all parties in a way that is fair to the individual. While there is no single official formulation of the fair information practice principles, the Markle Foundation's multi-stakeholder Connecting for Health initiative[11] outlined them as follows:

- **Openness and Transparency**: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

- **Purpose Specification and Minimization**: The purposes for which personal data is collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

- **Collection Limitation**: Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

- **Use Limitation**: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

- **Individual Participation and Control**:
    - Individuals should control access to their personal health information:
        - Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
    - Individuals should have the right to:
        - Have personal data relating to them communicated within a reasonable time (at an affordable change, if any), and in a form that is readily understandable;
        - Be given reasons if a request (as described above) is denied, and to be able to challenge such a denial:
        - Challenge data relating to them and have it rectified, completed, or amended.

- **Data Integrity and Quality**: All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete and current.

- **Security Safeguards and Controls**: Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

- **Accountability and Oversight**: Entities in control of personal health data must be held accountable for implementing these information practices.

[11] See www.connectingforhealth.org for a more detailed description of the Markle Common Framework.

- **Remedies**: Legal and financial remedies must exist to address any security breaches or privacy violations.[12]

The federal HIPAA privacy and security regulations include provisions that address to some degree many of these principles. As noted above, the privacy provisions in ARRA made major improvements – but significant gaps remain, and effective implementation of will require major effort. These comments focus on establishing privacy protections for personal health records, which are largely offered by entities outside the traditional medical system. The comments also address a number of key issues that arise with respect to access, use and disclosure of health information by health system participants, including: downstream data uses; new health information exchange networks; data that qualifies as de-identified under HIPAA; stronger implementation of collection limitations through the minimum necessary standard; and tighter rules on use of data for marketing. The comments also briefly address standards for minors' information.

Establishing Privacy Protections for Personal Health Records

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.[13] 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.[14]

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 has cautioned against this 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 HHS, which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

---

[12] In comments submitted by CDT to the FTC in November 2009, we urged FTC to adopt an updated, comprehensive set of FIPs for Internet privacy based on those more recently issued by the Department of Homeland Security. See http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf. The Markle Connecting for Health framework was largely designed to apply to patients and health care industry management of health information, but the FIPs in both the Markle and DHS models are similar.

[13] 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.

[14] 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.

It seems that Congress in ARRA agreed with CDT, for Congress did not extend HIPAA directly to PHRs. But to the extent that PHRs enter into agreements with covered entities to allow those entities to offer a PHR to their patients, they may be covered as business associates (which would make them directly accountable for complying with key HIPAA provisions).[15] CDT has argued for a narrow interpretation of this provision.[16]

Instead of extending HIPAA to all PHRs, Congress directed HHS to work with the FTC to come up with recommendations for privacy and security protections for PHRs. This PHR "study" must also include a recommendation for which agency (HHS, FTC or both) should have responsibility for regulating these entities – as well as a "timeline" for regulation, although Congress stopped short of calling for specific regulations.

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 applications – likely suppliers of health-related products and services. It will not be adequate, in our view, to depend heavily on consumer authorization. Consistent with CDT's views about the role of consumer consent in protecting health information, relying too heavily 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.[17] For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – clear rules are needed regarding marketing and commercial uses that will better protect consumers. CDT has testified before the National Committee on Vital and Health Statistics (NCVHS) on protections for PHRs, and is finalizing a comprehensive paper to be released this spring. See Appendix A for a copy of CDT's comments to NCVHS.

Ensuring Comprehensive Coverage – 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.[18] 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.[19] The agreements also are required to establish both the permitted and required uses and disclosures of health information by the business associate,[20] and to 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."[21] Business associates are also required to, at the termination of a business associate agreement and "if feasible," return or destroy personal data they receive from a covered entity. If return or destruction is not feasible, the contract must limit any further uses and disclosures to those that make the return or destruction of the information infeasible.[22]

---

[15] ARRA, Section 13408.

[16] See http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis/.

[17] See Rethinking the Role of Consent in Protecting Health Information Privacy (January 2009) http://www.cdt.org/healthprivacy/20090126Consent.pdf.

[18] 45 CFR 164.502(e)(1) & (2).

[19] 45 CFR 164.504(e)(2)(i).

[20] Id.

[21] 45 CFR 164.504(e)(2)(ii)(A)

[22] 45 CFR 164.504(e)(2)(I).

This combination of provisions place clear limits on what a business associate can do with health information received from a covered entity. However, one large business associate has been accused of using data they receive from covered entities to support other business objectives,[23] and some privacy advocates have long suspected that such practices are more widespread.

If such practices by business associates are in violation of the terms of their contracts with covered entities, ARRA strengthened the ability of government authorities to hold business associates accountable for such violations. Historically enforcement of a business associate agreement was largely in the discretion of the covered entity, and authorities could hold covered entities liable for the actions of their contractors only in limited circumstances. However, under ARRA, federal and state authorities can hold business associates directly accountable for failure to comply with their contracts.[24] Resolving these concerns may primarily be an issue of stronger enforcement of the law. But it's also possible that the contracts expressly or implicitly authorize more expansive uses and disclosures of data (presumably based on interpretations of the Privacy Rule). CDT will be exploring this in more detail in 2010, because, as explained in more detail below, organizations that facilitate the exchange of personal health information are now covered under HIPAA as business associates. It will be critical to ensure that an exchange's use, access and disclosure of data is both lawful and also consistent with building public trust in health IT.

The Uncertainty of Exchange Networks

In an effort to promote the more widespread exchange of electronic health information among health care providers, electronic information exchange networks are cropping up across the country to facilitate exchange among providers in local communities, or in states or geographic regions. ARRA includes significant funding to states to facilitate health information exchange, and the HHS Office of the National Coordinator for Health IT is targeting additional funding to 15 communities who have established basic electronic health information exchange infrastructures to enable them to more rapidly progressed to more advanced levels of data exchange to improve treatment and overall health outcomes.[25]

Exchange networks will play an essential role in achieving the data liquidity that is essential to meaningful health reform. However, there are numerous policy issues that will need to be resolved to ensure the promise of these networks can be realized. Critical questions include who can access data from these networks and for what purposes; what level of security should be required; how can networks be leveraged to enhance patient access to data; and how will policies and standards applicable to networks be enforced. Until the passage of ARRA, it was uncertain whether these exchanges would be covered by HIPAA. ARRA made it clear that at least some models of exchange are to be treated as business associates under HIPAA.[26] As a result, those entities are now required to directly comply with key HIPAA regulatory provisions.

But the application of the HIPAA business associate rules to these networks does not resolve many of the critical policy questions that must be addressed. So long as the business model and future direction of most networks remain uncertain, consumers and patients should ideally have an least have an option to opt-out of having their health information accessible through these networks.

---

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

[24] ARRA, section 13404.

[25] http://healthit.hhs.gov/blog/onc/index.php/2009/12/02/beacon-communities-a-proving-ground-for-health-it/

[26] ARRA, Section 13408.

The HIPAA De-Identification Standard

HIPAA's protections do not extend to health information that qualifies as "de-identified" under the Privacy Rule. Thus, 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.[27] 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. This is not the case today. A number of researchers have documented how easy it is to re-identify some data that qualifies as de-identified under HIPAA.[28] 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. At the same time, policymakers should enact provisions to ensure data recipients can be held accountable for re-identifying data.[29]

Minimum Necessary and Encouraging Use of "Lesser Identified" Data

Although the HIPAA provisions for de-identified data need improvement, CDT also recognizes that privacy risks are lessened when data has been anonymized to the greatest extent possible, as long as there are enforceable prohibitions against re-identification. In particular, many non-treatment uses of health data -- including quality, research and public health -- can be 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 "lesser identified" 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 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 the Department of Health and Human Services (HHS) has not issued any meaningful

---

[27] 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).

[28] See, for example, Salvador Ocha, Jamie Rasmussen, Christine Robson, and Michael Salib, Reidentification 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).

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

guidance on this standard. As a result, covered entities and their business associates frequently express concerns about how to implement it.

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 (as long as the covered entity enters into a data use agreement with the data recipient). These anonymized data sets provide greater privacy protection for individuals, but a significant amount of identifying information must be removed before data qualifies as a limited data set or de-identified under HIPAA. Thus, a number of health industry stakeholders have raised concerns that these data sets have limited utility for a range of important health care purposes.

ARRA attempts to strengthen the Privacy Rule's collection and use limitation 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.[30] This section of ARRA also requires the HHS Secretary to issue guidance on how to comply with the minimum necessary standard; when such guidance goes into effect, the directive to use the limited data set expires. CDT will be advocating for HHS to issue guidance on the minimum necessary standard that provides greater options for the use of "lesser identified" data for a number of routine purposes for which fully identifiable data can now be used, with sufficient accountability for re-identification.

Marketing

The use of sensitive medical information for marketing purposes is one of the most controversial practices affecting health privacy. 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 by third parties are marketing – even if those communications would otherwise not be construed as marketing because they relate to an individual's health or suggest treatment alternatives. But even this new provision includes exceptions that could swallow the rule. For example, entities do not need a patient's authorization to send remunerated communications about a drug or biologic that the patient is currently taking.

In addition, ARRA specifies that entities may receive outside payment for "treatment" – which suggests that communications sent for treatment purposes that are paid for by third parties can be sent without requiring patient authorization. CDT recognizes that broad prohibitions restricting the right to use health information to communicate with patients for treatment purposes are counterproductive. But because treatment is broadly defined in the HIPAA Privacy Rule, this exception may result in some purely marketing communications being made with patients' health information without their prior authorization.

Securing the right set of provisions to protect patients from abuse of their personal health information for marketing purposes has been difficult to achieve at the federal level. One way to close this gap in the Privacy Rule is to restrict who may access data for treatment or care management purposes to professional caregivers directly involved in the individual's treatment. Such a measure could greatly restrict access to and abuse of protected health information from provider or health plan electronic medical records (or health information exchanges) for what are largely marketing uses.

[30] ARRA, Section 13405.

Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but those rules have never been adequately enforced.[31] 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.[32] 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.[33]

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 steps to strengthen HIPAA enforcement.[34] State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA. Although state authorities are limited in the civil monetary penalties they can pursue (such fines can only be imposed at the previous statutory level - $100 per violation, with a $25,000 maximum for repeat violations), the additional enforcement resources under HIPAA should help ensure that the law is more vigorously enforced.

Other important improvements to HIPAA enforcement include the following:

- 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.[35]

- 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

---

[31] Richard Alonso-Zaldivar, "Effectiveness of medical privacy law is questioned," Los Angeles Times, 9 April 2008.

[32] "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.

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

[34] See Sections 13409-13411 of ARRA.

[35] Of note, the increased penalties went into effect on the day of enactment – February 17, 2009.

HIPAA Privacy and Security Rules. (The HIPAA regulations provide the Secretary with audit authority, but this authority was rarely if ever used during the Bush Administration.)

The ARRA provisions are a major advancement in enforcement of federal health privacy laws, but individuals are still dependent on federal or state authorities to enforce the law, as there is no private right of action. ARRA does require the HHS Secretary to establish a methodology to allow individuals harmed by HIPAA violations to receive a percentage of any civil penalties or civil monetary settlements obtained by the government – but this falls short of giving individuals the tools to directly enforce their rights. CDT believes that a private right of action should be part of any enforcement scheme. We recognize that providing a private right of action to pursue every HIPAA complaint – no matter how trivial – would be inappropriate and disruptive, but Congress should give consumers some right to privately pursue recourse in certain 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.

Minors

The FTC has specifically asked for input on whether minor's information should be subject to more stringent privacy standards. As the FTC may be aware, a number of states permit "mature" minors to obtain certain types of health care without parental or guardian consent.[36] The HIPAA Privacy Rule essentially defers to state law with respect to access to minor's health information by a parent, or whether the minor has the right to control access to his or her information.[37] Restrictions on the extent to which minors can seek and share health information on-line (or parental consent requirements) could significantly undermine the intent of mature minor laws, which is to ensure that minors are not deterred from seeking appropriate medical care.

Placing stricter controls on information that can be sent to minors also implicates free speech. The First Amendment protects *both* the right of minors to receive the information and the right of speakers to reach an audience of minors. We urge FTC to review the final report of the Internet Safety Technical Task Force on Enhancing Child Safety & Online Technologies, which we are also submitting as comments for this Roundtable.[38]

Conclusion

Thank you for the opportunity to present these remarks in support of strengthening privacy and security protections for personal health information.

Deven McGraw
Director, Health Privacy Project
deven@cdt.org
202-637-9800 x119

---

[36] See http://www.guttmacher.org/pubs/tgr/03/4/gr030404.pdf for a general discussion of these laws.

[37] 45 CFR 164.502(g)(3)(ii) and Office for Civil Rights, HHS, Guidance on Personal Representatives (April 3, 2003) available at http://www.hhs.gov/ocr/hipaa/guidelines/personalrepresentatives.pdf.

[38] http://cyber.law.harvard.edu/pubrelease/isttf/

Appendix A

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

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

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 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

[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.

[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.

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 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

[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.

[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.

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 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;

[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).

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

- 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 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

[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/.

[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.

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.

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

[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).

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.