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

before the
California Senate Committee on Health

Health Information Technology: Current Trends, Future Opportunities

March 13, 2009

Madame Chair and members of the Committee, thank you for holding this important and very timely hearing on health information technology, and thank you for the opportunity to testify.

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 health information on-line and build consumer trust in e-health systems, so that the benefits of HIT can be realized. We are supported by a wide range of corporations, trade associations and foundations, including the California HealthCare Foundation.

Last year, CDT released a paper calling on policymakers to enact – and the healthcare industry to adopt - a comprehensive privacy and security framework to cover electronic health information.[1] More recently, we issued a paper re-conceptualizing the role of consent in the protection of health privacy.[2] We have testified three times in the past year before the U.S. Congress in support of health

[1] Comprehensive Privacy and Security: Critical for Health Information Technology (May 2008) www.cdt.org/healthprivacy/20080514Hpframe.pdf.

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

privacy improvements. Our article on privacy protections needed for electronic health information exchange was the lead article on privacy in the special health information technology issue of the health policy journal *Health Affairs* (published earlier this week).

A number of our recommendations were incorporated in the recently enacted economic stimulus package, the American Recovery and Reinvestment Act of 2009 (ARRA). That new federal law, while very significant, provides only a partial solution to the privacy and security challenges posed by the new e-health environment. CDT will be releasing soon a detailed comparison of California's Confidentiality of Medical Information Act (CMIA) and federal law as amended in the stimulus bill. Today, I will offer a preview of some of our conclusions and recommendations.

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

Health information technology (health IT or HIT) 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 HIT. 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.[3] In a 2006 survey, when Americans were asked 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

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

- 55% were concerned about insurers gaining access to this information. [4]

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. Last year, for example, an NIH laptop was stolen loaded with identifiable information about clinical research subjects.[5]

Protecting privacy is important not just to avoid harm, but because good healthcare depends on accurate and reliable information. [6] 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.[7] 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.[8] 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.[9]

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

---

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

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

[6] 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).

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

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

[9] 2005 National Consumer Survey.

- 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.[10]

These concerns can be met. Privacy and security should not be an impediment to adoption of HIT. To the contrary, sound privacy and security policies, implemented in law, corporate practice and technology design, can enable HIT. Indeed, electronic systems, properly designed and managed, have a greater capacity to protect sensitive 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. 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.[11]

◪ Unfortunately, despite the efforts of leaders such as the Chair of this Committee, the protections for health privacy remain incomplete. Even with the improvements in the stimulus, we still lack a comprehensive privacy and security framework.

Moving forward will require at both the federal and state level: (1)enforcement, which has been lacking for far too long; (2) carefully crafted regulation and other guidance to flesh out statutory requirements, including conscientious implementation of the new federal rules through regulatory action, standards activity, and legislative oversight; (3) further legislative improvements to keep pace

[10] Id.

[11] 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.

with changes in technology and business models; and (4) further attention to the issue of marketing. In our testimony today we will make some observations and recommendations in all four areas, and we look forward to working with this Committee and all stakeholders in the coming months to develop further steps.

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 HIT 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 HIT 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 HIT 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 HIT, 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.

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. The principles of fair information practices are globally recognized. They are embodied, albeit incompletely, in the regulations promulgated under the federal Health Insurance

Portability and Accountability Act (HIPAA) and in state privacy law, including the CMIA.

While there is no single official formulation of the fair information practice principles, the Markle Foundation's multi-stakeholder Connecting for Health initiative12 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.

---

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

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

The California CMIA and the federal HIPAA privacy and security regulations include provisions that address to some degree many of these principles. The HIT provisions in ARRA made major improvements. However, as discussed in more detail below, significant gaps remain, and effective implementation of ARRA will require major effort.

At both the federal and state level, in order to make the comprehensive privacy and security framework a reality, policymakers need to address at least four issues:

(1) There needs to be more effective enforcement of privacy and security rules, including oversight and auditing of the practices of the various entities handling health care information. Recent changes in both California and federal law create new opportunities for enhanced enforcement.
(2) The regulatory process at both the federal and state levels needs to flesh out some key concepts. Provisions in ARRA call for several federal rulemakings and the recently re-constituted California Office of Health Information Integrity should provide guidance as needed on implementation of the CMIA.
(3) 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. In particular, a comprehensive privacy and security framework needs to be developed for personal health records (PHRs) and other Internet-based services that operate outside the traditional healthcare structure.
(4) Further attention needs to be given to the issue of marketing, which is a major area of consumer concern.

Implementation of Recent Changes in Federal Law and the CMIA Will Require Diligent Attention

The HIPAA privacy and security regulations that took effect in 2003 were a landmark, but they fell far short of providing comprehensive protection either in the traditional healthcare arena or for the rapidly evolving e-health environment. It fell to the states to fill the gaps in federal law. California was a leader in this regard, extending its breach notification law to medical data, beginning to address the issues

posed by PHRs, enacting legislation that provides stronger protections for certain sensitive categories of data, and making entities responsible for security failings.

The provisions in ARRA represent a major advancement in health privacy; in some ways, they brought the federal law up to par with California and in other ways the federal law is now stronger than California law. Moreover, ARRA gave state attorneys general the authority to enforce federal privacy and security rules. Not only will the states have an important role in implementing the privacy enhancements in ARRA, they will continue to have an important role to play in filling in the gaps that remain in federal law even after ARRA. As a nation, for the foreseeable future, we will continue to have a hybrid system that combines federal and state protections. The challenge is to craft from this federal-state system a solution that gives patients comprehensive privacy and security protection and that offers all the entities in the e-health space a predictable and consistent policy environment.

In this section, we describe some of the changes made by ARRA, compare them with provisions of California law, and highlight important issues that deserve the attention of this committee and others who will be involved in the implementation of CMIA and the new federal provisions.

Ensuring Comprehensive Coverage - Direct Regulation of Business Associates or Contractors

Under HIPAA, "business associates" contract with HIPAA covered entities to perform particular services or functions on their behalf using protected health information (or PHI). Historically, business associates have not been directly covered by HIPAA and instead were obligated to comply with federal privacy rules only to the extent of their contracts or "business associate agreements" with covered entities. In addition, federal authorities could not hold business associates accountable for failure to comply with their contracts and could hold covered entities liable for the actions of their contractors only in limited circumstances. California law was better on this point, as obligations and prohibitions apply to "contractors" throughout the CMIA.

ARRA makes a major change in the treatment of such "contractors," and brings federal law closer to the approach taken in California. Under ARRA, business associates must abide by nearly all of the HIPAA regulations on data security (Section 13401); must directly comply with all of the new privacy provisions enacted in ARRA (Section 13404); and can be held accountable to authorities for failure to comply with any HIPAA Privacy Rule provisions made applicable through the business associate agreement (Section 13404).

The ability to hold business associates more accountable for how they use and disclose data takes an important step toward establishing a comprehensive framework of protections. However, despite the changes in ARRA, under neither federal nor state law is all health information fully protected, and there are likely entities that hold health information that fall outside of both systems. Federal and state policymakers should consider applying protections to the data itself – that is, to identifiable medical information in the hands of anyone other than the patient, without regard to who has custody or possession of it or who created it.

Ensuring Comprehensive Coverage -- RHIOs and HIEs

Prior to ARRA, state and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), intended to facilitate exchange of personal health information, might not have been covered by HIPAA privacy and security regulations. California law almost certainly covered RHIOs and HIEs, defining as health care providers any entity organized for the purpose of maintaining medical information in order to make it available to a provider at the request of the provider. In addition, and as noted above, obligations and prohibitions apply directly to "contractors" throughout the CMIA. ARRA made it clear that RHIOs and HIEs are to be treated as business associates under HIPAA. (Section 13408) As a result, those entities are now required to directly comply with key HIPAA regulatory provisions.

However, a more fundamental concern is that neither HIPAA nor CMIA permits patients to control whether or not their information is exchanged through broader networks like RHIOs in the first place. ARRA's extension of key protections to health information exchanges mitigates this problem to some extent, but so long as the business model and future direction of most RHIOs and HIE networks remain uncertain, patients should have the protection of an opt-in standard for inclusion of their information in such networks. This is an area in which California should take the lead, explicitly requiring prior opt-in for inclusion of a person's health data in a RHIO or HIE network.

Minimum Necessary and Encouraging Use of Anonymized Data

Under the collection and use limitations of fair information practices, data holders and recipients must collect, use and disclose only the minimum amount of information necessary to fulfill the intended purpose of obtaining or disclosing the data. The HIPAA Privacy Rule incorporates these principles in the "minimum necessary" standard, which requires covered entities to use only the minimum necessary amount of data for most uses and disclosures other than treatment. This standard is intended to be flexible, but the federal Department of Health and Human Services (HHS) has not issued any meaningful guidance on this standard.

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

Consistent with the data limitation principles, the HIPAA Privacy Rule also provides for two anonymized data options – 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) and de-identified data (which is stripped of nearly all identifying information and can be used or disclosed for any purpose without the need for a data use agreement). Data that meets the de-identification standard is no longer protected by HIPAA. 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. (Section 13405) 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.

California law does not have a minimum necessary standard, so the HIPAA standard applies.

We will be advocating for HHS to issue guidance on the minimum necessary standard that provides greater options for the use of anonymized data for a number of routine purposes for which fully identifiable data can now be used (for example, activities covered under the definition of health care operations), as well as for public health and research. Privacy risks are lessened when data has been anonymized to the greatest extent possible, as long as there are enforceable prohibitions against re-identification. Federal and state policymakers should also consider deferring more to the provider's professional judgment about degree of identifiability of data needed to accomplish a given purpose.

Access

The HIPAA Privacy Rule has always provided individuals with a right to access copies of their medical records at a reasonable cost; the individual can request that this copy be in paper or electronic form, and the entity has to comply with this request if it is possible to do so. However, individuals have often had difficulty

getting health care entities to comply with this requirement, as complaints about access are among the top five HIPAA complaints received by HHS. California law similarly gives patients a right to access copies of their records and sets limits on the copying charges that can be assessed.

In ARRA, Congress brings this access right into the digital age by requiring health care entities using electronic health records to provide patients with electronic copies of their records upon request. Charges for an electronic copy must be limited to the labor cost of responding to the request, since no reproduction costs are involved. (Section 13405) The individual also can direct the covered entity to send that copy to another individual or to an entity, like a PHR vendor, as long as that choice is "clear, conspicuous, and specific." This provision should help make personal health records more useful to individuals and ensure that providers and plans adopting electronic health record systems have the technical capability to easily get health information in the hands of consumers (and if they so designate, their family members).

Accounting for disclosures of protected health information

One element of the right to privacy is that an individual should be able to find out who has obtained copies of her records. The HIPAA Privacy Rule has always included the right to request an accounting of disclosures of one's identifiable health information going back for a period of six years prior to the date of the request. The right, however, was limited prior to the passage of ARRA, since it excluded disclosures for treatment, payment and health care operations. (45 CFR § 164.528) The CMIA does not address accounting for disclosures, so the HIPAA rule applies in California.

ARRA changed the federal rule on accounting for disclosures, requiring a covered entity that maintains electronic health records (EHR) to account for disclosures of PHI for purposes of treatment, payment and business operations for three years prior to the date of the request. (Section 13405) This provision will apply to both covered entities and business associates – which means it will apply to electronic health information networks like RHIOs and HIEs as well. Although this provision will not go into effect until a technical standard and regulations have been adopted to properly implement it, it represents a major change in the transparency of health data uses and flows. It recognizes that the public is less likely to trust broad sharing networks without the reassurance of being able to find out who has access to their data and for what purposes.

Breach Notification

Prior to ARRA, HIPAA did not require hospitals or other data custodians to notify record subjects of data security breaches. California took the lead, first in adopting a breach notification law and then in extending it to medical records. ARRA includes a national breach notification provision that goes beyond California law in some respects.

First, ARRA includes breach notification requirements for covered entities13 and for vendors of PHRs and the third-party applications that are offered to PHR account holders on vendors' web sites (and many of those applications involve the exchange of personal health information). (Sections 13402 and 13407) A recent change in the language of California Civil Code §56.07(a) brings some PHR vendors under the CMIA and the breach notification law, but the language is somewhat ambiguous, as discussed in more detail below in the section on regulation of PHRs. To the extent these vendors are not covered under California's breach law, they are likely covered by the new federal provisions.

The breach notification provisions covering HIPAA-covered entities are administered by HHS; those applicable to PHR vendors are administered by the FTC.

The federal breach notification provisions applicable to HIPAA covered entities cover both external breaches and unauthorized insider access in some instances. A breach is considered to be "discovered" by a covered entity when one employee (other than the person breaching the data) knows about the breach. The definition of breach for PHR vendors and some of their business partners is any access to data not authorized by the individual holder of the personal health record account.

Like California's law, the new federal breach notification provisions provide strong incentives for entities covered by the law to adopt encryption-type technologies to protect data, as individuals do not have to be notified if there is a breach of data that is protected by a technology or method that renders data unreadable, unusable or indecipherable. The Secretary of HHS is required to come up with a list of technologies and methodologies that qualify for this exemption.

For the most part, the notification requirements in ARRA are much more stringent than California's provisions. ARRA specifies how notice must be sent, the information required to be in the notice, what type of data has been compromised, how the breach occurred, and what actions the entity has taken in mitigation. Covered entities are also required to report all breaches to the HHS Secretary and

[13] Business associates must notify the covered entity of any breach, and the covered entity must then notify the individual.

report to the media any breaches of over 500 records. California's breach notification provision is more stringent than the new federal law in one respect: ARRA requires that notice be provided no later than 60 days after discovery of the breach, but in California, specific facilities covered by Health and Safety Code §1280.15(a) have only five days to notify affected individuals of a breach.

HHS and FTC must issue interim final regulations to implement the new breach notification provisions within 180 days of enactment of the legislation (August 2009), and the provisions are effective 30 days later.

These new breach notification provisions take an important step forward in increasing the transparency of EHR and PHR systems and could help prompt improvements in the security of health records.

Enforcement

In the past, neither HIPAA nor the CMIA was adequately enforced. 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.[14] 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.[15] Likewise, there had been little enforcement of CMIA, leading the legislature to take action last year when it was revealed that employees had been browsing the records of patients at major hospitals.

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 federal authorities to vindicate their rights.

---

[14] "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.

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

In ARRA, Congress took a number of steps to strengthen HIPAA enforcement. (Sections 13409-13411) Of most relevance to the Committee is the provision expressly authorizing state attorneys general to enforce HIPAA. State attorneys general can now 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.[16]

- HHS is required to impose civil monetary penalties in circumstances where the HIPAA violation constitutes willful neglect of the law.

- The U.S. Department of Justice can now prosecute individuals for violations of HIPAA's criminal provisions.

- The HHS Secretary is required to conduct periodic audits for compliance with the HIPAA Privacy and Security Rules. (The HIPAA regulations provide the Secretary with audit authority, but this authority was rarely if ever used during the Bush Administration.)

The ARRA provisions are a major advance 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 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

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

disruptive, but Congress and the states 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.

Additional Areas Key Where the Privacy Framework Still Requires Strengthening

Establishing Privacy Protections for Personal Health Records

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. 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 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.[17]

California, through a recent change in the language of Civil Code § 56.07(a), sought to bring some PHR vendors under the CMIA and the breach notification law. However, as noted above, the language is somewhat ambiguous: "Any business organized [changed from 'any business primarily organized' (emphasis added)] for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this part." It seems to us that a company like Microsoft or Google could argue that it was

[17] 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.

not organized for the purpose of maintaining health data and therefore is not covered by CMIA, despite the recent change. The application of this provision to PHRs may remain subject to interpretation until the California Office of Health Information Integrity fulfills its mandate to write regulations for the state's medical privacy laws.

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.

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). The language in this particular provision (Section 13408) is unclear, and HHS will need to clarify its meaning in regulations or guidance.

Instead of extending HIPAA to PHRs, Congress directed HHS to work with the FTC to come up with recommendations for privacy and security protections for PHRs. This PHR "study" is to be completed no later than February 17, 2009, and must also include a recommendation for which agency (HHS, FTC or both) should have responsibility for regulating these entities. The study must also include 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 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.[18] 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.

It will be important to contribute to the PHR study to ensure that the recommendations reflect consumer interests. CDT hopes it will lay the groundwork for the establishment of comprehensive privacy and security protections that can be quickly enacted into law.

Marketing

The use of sensitive medical information for marketing purposes is one of the most controversial practices affecting health privacy. Both the HIPAA Privacy Rule and the CMIA have provisions intended to limit the use of medical data in marketing, but both sets of rules are subject to exceptions. Moreover, there has been little regulatory or legislative investigation of marketing practices.

In ARRA, Congress took some steps to tighten the definition of "marketing" in the HIPAA 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, 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. We recognize that broad prohibitions restricting the right to use health information to communicate with patients for treatment purposes is counterproductive. But because treatment is broadly defined in the HIPAA Privacy Rule, this exception will 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. California should consider closing the gap, for example, by restricting who

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

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 for what are largely marketing uses.

Conclusion

Thank you for the opportunity to present this testimony in support of strengthening privacy and security protections for personal health information, which will build consumer trust and enable HIT and electronic health information exchange to move forward. I would be pleased to answer any questions you may have.

FOR MORE INFORMATION

Please contact: Brock Meeks
Director of Communications
202-637-9800