Statement of Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology
Before the
Subcommittee on Health, Committee on Ways & Means

Promoting the Adoption and Use of Health Information Technology

July 24, 2008

Chairman Stark, Ranking Member Camp, and members of the Subcommittee, thank you for holding this hearing on promoting the adoption and use of health information technology and for the opportunity to testify today.

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 earlier this year to take advantage of CDT's long history of expertise on Internet and information privacy issues and to come up with workable solutions to better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

CDT recently released a comprehensive paper calling on Congress to enact – and all stakeholders to adopt - a comprehensive privacy and security framework to cover electronic health information. Some of the points raised in that paper are highlighted in this testimony today, but I also request that the full copy, which is attached and can be found at www.cdt.org/healthprivacy/20080514Hpframe.pdf, be entered into the hearing record.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and electronic health information exchange can help 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 both the benefits and the risks 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, people have significant concerns about the privacy of their medical records. 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 the benefits of and concerns about online health information:

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

Health IT has a greater capacity to protect sensitive personal health information than is the case 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 policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.[3]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects underscore

---

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

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

[3] 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.

these concerns, and this is just one of numerous examples. The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[4]

With rare exception, national efforts to advance greater use of health IT have not adequately or appropriately addressed the privacy and security issues raised by the movement to electronic health records. 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.

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[5] Without appropriate protections for privacy and security in the healthcare system, patients will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[6] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[7] 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.[8]

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

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;

---

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

[5] 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).

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

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

[8] 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.[9]

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 than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy.

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

To build public trust in health IT, we need a comprehensive privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. In developing this comprehensive framework, policymakers, regulators, and developers of HIT systems need not start from scratch. A framework for HIT and health information exchange already exists, in the form of the generally accepted "fair information practices" ("FIPS") that have been used to shape policies governing uses of personal information in a variety of contexts – most notably the privacy regulations enacted pursuant to the Health Insurance Portability and Accountability Act (HIPAA), which established the first federal health privacy framework.[10] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's multi-stakeholder Connecting for Health initiative, would:

- Implement core privacy principles;
- Adopt trusted network design characteristics; and
- Establish oversight and accountability mechanisms.[11]

In particular, the core privacy principles of the Connecting for Health Common Framework set forth a comprehensive roadmap for protecting the privacy and security of personal health information while still allowing information to be accessed and disclosed for legitimate purposes. Those core privacy principles are:

- **Openness and Transparency**: There should be a general policy of openness about developments, practices, and policies with respect to personal data.

[9] Id.

[10] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

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

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

The HIPAA privacy and security regulations include provisions that address each of these categories – but, as discussed in more detail below, the rules are insufficient to cover the new and rapidly evolving e-health environment. To build consumer trust in e-health systems and ensure that health IT and electronic health information exchange move forward with sufficient protections for privacy and security, Congress should consider: strengthening HIPAA for records kept by traditional

health system participants; filling gaps in HIPAA's coverage where appropriate; and establishing additional legal protections to reach new actors in the e-health environment and address the increased migration of personal health information out of the traditional medical system.

Strengthening HIPAA Privacy and Security Rules to Meet New Challenges

The HIPAA privacy and security regulations that took effect in 2003 reflect elements of a comprehensive framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. The HIPAA Privacy Rule was a landmark in privacy protection, but as noted above, the regulation does not adequately cover the new e-health environment. For example:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by HIPAA privacy and security regulations.
- Personal health records and other consumer access services now being created by third parties, including companies such as Google and Microsoft, as well as by employers usually fall outside of the HIPAA rules.
- Personal health data is migrating onto the Internet through an exploding array of health information sites, online support groups, and other on-line health tools, regulated only through enforcement by the Federal Trade Commission (FTC) of the general prohibition against unfair and deceptive trade practices, such as a failure to follow promised privacy policies.
- HIPAA has never required that patients receive notice when their personal heath information is inappropriately accessed or disclosed.
- While the Privacy Rule includes criteria for de-identifying data, new technologies are making it much easier to re-identify once de-identified health information and to combine it with personal information in other databases, making it more likely that sensitive health information will be available to unauthorized recipients for uses that have nothing to do with treatment or payment.
- The HIPAA rules have never been adequately enforced. The Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services (HHS), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were

implemented, even though that office has found numerous violations of the rules.[12]

Historically, states have filled the gaps in federal health privacy laws by enacting legislation that provides stronger privacy and security protections for sensitive data, such as mental health and genetic information. The states continue to have an important role to play, but relying on the states to fill deficiencies in HIPAA's Privacy Rule – or to regulate entities outside of the traditional healthcare sphere – does not provide a comprehensive, baseline solution that gives all Americans adequate privacy and security protections, and does not offer all the entities in the e-health space a predictable and consistent policy environment.

Although it is desirable for Congress to enact legislation that fills some of the gaps in HIPAA and to enact a general privacy and security framework to govern health IT, we caution against a "one-size-fits all" approach that treats all actors that hold personal health information the same. The complexity and diversity of entities connected through health information exchange, and their very different roles and different relationships to consumers, will often require precisely tailored policy solutions that are context and role-based and flexible enough to both encourage and respond to innovation. For example, it makes little sense to have the same set of rules for "personal health records," which are often created by and controlled by patients and held by third party data stewards outside the healthcare system, and for "electronic health records," which are created and controlled by health care providers for purposes of treatment and care management. To take another example, rules for use of personal health information for treatment need to be quite different than rules for marketing or other secondary uses. Rules regarding use of health information for research need to be separately considered as well. Therefore, a second major challenge for Congress is to decide what can be legislated and what must be delegated to agency rulemaking – and what areas are best left to be developed and enforced through industry best practices.

Below we discuss in detail two critical areas that we do believe need attention from Congress: establishing privacy protections for personal health records offered by entities not currently covered by HIPAA and strengthening HIPAA enforcement. But CDT also recommends Congress address the following, either through express legislation language or by tasking HHS to modify the HIPAA privacy and security rules (or a combination of both approaches):

---

[12] "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.

- Clarify how the new entities that facilitate the electronic exchange of personal health information - including HIEs (Health Information Exchanges), RHIOs (Regional Health Information Organizations), and E-Prescribing Gateways – are covered by HIPAA (for example, by making them HIPAA covered entities or requiring them to have business associate agreements with the entities that exchange health information through them).
- Establish a federal right for patients to be notified in the event of a breach of identifiable health information.
- Tighten the definition of "marketing" in the HIPAA privacy rules to make clear that covered entities cannot use a patient's protected health information to send a communication recommending a product or service without that patient's prior authorization.
- Make clear that when entities use electronic medical records, their patients have the right to receive an electronic copy of their health information, and establish a right for patients to monitor who has accessed their health information through audit trails.
- Ensure that covered entities holding protected health information access, use, and disclose only the minimum necessary amount of information when engaging in activities related to payment and health care operations[13] and require entities to use information stripped of common patient identifiers when it is possible to do so and still accomplish the legitimate purpose for which the information was accessed.[14]
- Explore whether the current HIPAA de-identification standard - now five years old – needs to be updated given the increased public availability of data on-line and the possible greater potential for re-identification of de-identified data.

Establishing Privacy Protections for Personal Health Records

Personal health records and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers, will not be covered by the HIPAA regulations unless they are being offered to consumers by covered entities. In this unregulated arena, consumer

[13] See 45 C.F.R. 164.501 for a definition of "health care operations."

[14] For example, HIPAA rules provide for the use of a limited data set – information stripped of certain patient identifiers - for certain purposes, but its use is neither required nor expressly encouraged. See 45 C.F.R. 164.514(e).

privacy will be 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), 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.[15] 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 the HIPAA Privacy Rule to cover PHRs. But we believe that the Privacy Rule, which was designed to set the parameters for use of information by traditional health care entities, would not provide adequate protection for PHRs and may do more harm than good in its current scope. 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.

We believe tasking HHS and FTC with jointly developing 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. 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. Relying solely 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 – clear rules are needed regarding marketing and commercial uses that will better protect consumers.

Congress Should Also Consider Strengthening HIPAA Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for failure to comply with the statute – and these penalties applied to the subsequent privacy and security rules implemented years later. Unfortunately, the HIPAA rules have never been adequately enforced. As noted above, HHS has not levied a single

[15] 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.

penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented.[16] The Justice Department has levied some penalties under the criminal provisions of the statute – but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limits 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.[17]

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, even under the existing enforcement regime, there is no ability for consumers whose information is accessed or disclosed in violation of HIPAA to seek redress or be made whole.

Below are a number of incremental steps that Congress can take this year to improve enforcement of HIPAA.

Accountability for Business Associates

Under current rules, business associates who access, use and disclose protected health information on behalf of covered entities are accountable for complying with HIPAA privacy and security regulations only through their contracts with covered entities. If the covered entity does not take action to enforce the contract, there is no other mechanism for ensuring that the business associate complies with the applicable rules. Further, HHS can only hold the covered entity responsible for the actions of business associates only if the entity knew of a "pattern of activity or practice of the business associate that constituted a material breach or violation" of its agreement with the covered entity, and the covered entity doesn't take action to cure the breach or terminate the contract.[18] Of interest, if the covered entity decides that terminating the contract is "not feasible," the covered entity is required to report

---

[16] Just last week, HHS announced that Seattle-based Providence Health & Services agreed to pay $100,000 as part of a settlement of multiple violations of the HIPAA regulations. But the press release from HHS made clear that this amount was not a civil monetary penalty. http://www.hhs.gov/news/press/2008pres/07/20080717a.html.

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

[18] 45 C.F.R. 164.504(e)(ii).

the problem to the Secretary.[19] But the regulations do not give the Secretary any further authority to enforce HIPAA against the business associate or hold the covered entity responsible for the violation. Congress should take action to ensure that business associates can be held legally accountable for complying with HIPAA regulations.

Strengthening the Statutory Provisions Authorizing Civil and Criminal Penalties

Penalties for Criminal Violations. As noted above, the HIPAA statute provides for criminal penalties for intentional violations; but a DOJ Office of Legal Counsel Memo expressly limits the application of these provisions to covered entities. According to this memo, DOJ cannot prosecute employees of covered entities or their business associates for intentional violations of HIPAA unless these persons are carrying out a specific policy or business practice endorsed by the covered entity. Congress should make it clear that penalties can be assessed against covered entities, business associates, and their employees for violations of HIPAA.

Civil Monetary Penalties – Part I. The statute prohibits the Secretary of HHS from imposing civil monetary penalties if the HIPAA violation is "an offense *punishable*" under the criminal provisions of the statute.[20] A reasonable interpretation of this provision is that if a HIPAA complaint indicates a possible criminal violation, the Secretary of HHS cannot launch a civil investigation or pursue civil monetary penalties, even if DOJ decides not to prosecute the case. To avoid having the most egregious HIPAA violations go unpunished, Congress should act to give the Secretary clear authority to investigate and pursue civil monetary penalties unless DOJ decides to pursue criminal penalties.

Civil Monetary Penalties – Part II. The civil penalty provisions of the statute envision three types of HIPAA violations: those that the entity was not aware of (or could not have been aware of exercising reasonable diligence); those due to reasonable cause; and those due to willful neglect.[21] The statute also prohibits the Secretary from imposing civil monetary penalties in cases of lack of knowledge or due to reasonable cause, unless the entity is unable to correct the violation within a 30-day time period (with discretion to extend this time period).[22] The statute also gives the Secretary authority to provide compliance assistance to help the covered entity correct a violation due to reasonable cause and to waive or reduce a penalty in cases of

[19] Id.

[20] Section 1176((b)(1) of the Social Security Act.

[21] See Sections 1176(b)(2) –(3) of the Social Security Act.

[22] Id.

reasonable cause if the penalty would be excessive relative to the compliance failure involved.[23] The statute requires that the Secretary impose civil monetary penalties for HIPAA violations;[24] the statute does not give the Secretary discretion to give a covered entity a chance to correct the violation or the authority to waive or reduce penalties in cases of willful neglect. The HIPAA enforcement regulations, however, require the Secretary to first try to informally resolve all HIPAA complaints – which means there is never an investigation into whether or not the violation rises to the level of willful neglect (and thus should be subject to civil monetary penalties). Congress should act to clarify that the Secretary must investigate all complaints for which a preliminary inquiry into the facts indicates possible willful neglect and pursue civil monetary penalties in willful neglect cases.

Establishing Penalties for Re-identification of De-Identified Data

Health information that is de-identified is not covered by the protections of HIPAA. Thus, covered entities can provide de-identified data to other persons or entities without regard to the requirements regarding access, use and disclosure in the HIPAA regulations, and these entities can use this data as they wish, subject only to the terms of any applicable contractual requirements (or any state laws that might apply). If one of these persons or entities then re-identifies this data – for example, by using information available in a public database – that re-identified information would not be subject to HIPAA regulations unless the person or entity holding the data was a covered entity. Earlier in this testimony we suggest examining the current HIPAA de-identification standard to ensure that it continues to provide robust protection for patient identifiable data. But Congress could also protect individual privacy by enacting prohibitions (and penalties for) the unauthorized re-identification of de-identified data.

Other Ways to Improve Accountability under HIPAA

A significant shortfall in HIPAA is the absence of any way for the consumer whose health information privacy has been violated to pursue meaningful recourse and be made whole. 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 further consider giving consumers some right to

---

[23] Sections 1176(b)(3)-(4) of the Social Security Act.

[24] See Section 1176(a) of the Social Security Act ("…The Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000).

privately pursue recourse where there are intentional violations of the law, or in circumstances of willful neglect. As noted above, the HIPAA statute already provides for criminal and civil monetary penalties in such cases – but these penalties do not currently go to the consumers whose privacy was violated, and as structured may not be sufficient (at least with respect to civil penalties) to provide meaningful recourse for individuals.

Structuring an effective private right of action will take careful thought and consideration. Given the dwindling number of legislative days left in the year and political circumstances, we recognize that it is unlikely we can pursue implementing such a right this year. But we urge Congress to hold hearings on this issue to begin to develop a workable way to ensure that entities covered by HIPAA are directly accountable to consumers for the most egregious violations of their privacy. In the meantime, the recommendations we set forth above are ones that can be put into legislation this year and if implemented will greatly improve HIPAA enforcement.

Congress should also consider authorizing State Attorneys General to also enforce HIPAA. The HHS Office of Civil Rights is significantly under resourced, and expressly authorizing state authorities to enforce HIPAA puts more hands on the enforcement deck. Currently, only those State Attorneys General who expressly have the authority to enforce federal law in their state authorizing statutes are able to enforce the federal HIPAA provisions. State authorities are able to enforce their own state health privacy laws, but in only a handful of states are those laws are as comprehensive as HIPAA. Congress should consult with State Attorneys General about providing them with express authority to enforce HIPAA and consider taking future action in this area (particularly if the enforcement "fixes" recommended earlier in this testimony are not successful in actually improving HIPAA enforcement).

The Appropriate Role of Consumer Consent

Recently, public debates about how best to protect the confidentiality, privacy and security of health information have focused almost exclusively on whether patients should be asked to authorize all uses of their health information. The ability of individuals to have some control over their personal health information is important, and a comprehensive privacy and security framework should address patient

consent.[25] A number of states have passed laws requiring patient authorization to access, use and disclose certain sensitive categories of health information, and federal law prohibits the disclosure of substance abuse treatment records without express patient authorization. HIPAA Privacy Rules currently prohibit the use of certain types of information, such as psychotherapy notes, or prohibit use of information for certain purposes, such as marketing, without express patient authorization, and the Rules provide individuals with the right to object to certain uses and disclosures (such as in facility directories or to family members). The Rules also allow covered entities to give consumers greater rights to restrict uses and disclosures of their information. Health information systems must be structured in a way that allows these consents to honored and appropriately and securely managed.

But patient authorization is not a panacea, and as appealing as it may appear to be in concept, in practice reliance on consent would provide weak protection for consumer's health information. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is less protective of privacy and confidentiality.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated decisions about use of their health data. Most don't read the details of a consent form 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.[26] If mere patient authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are

[25] Much more should be done to improve the way in which consent options are presented to consumers in the healthcare context. Internet technology can help in this regard, making it easier to present short notices, layered notices and more granular forms of consent.

[26] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K. Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

completely outside the scope of the HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if policymakers rely on consent by an individual for any particular use of his or her information as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.

In contrast, a comprehensive approach – which puts clear parameters around who can access, use and disclose a patient's personal health information and for what purposes – puts the principal burden on the entities holding this information by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. [27]

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 health IT and electronic health information exchange to move forward. I would be pleased to answer any questions you may have.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION
Please contact: Deven McGraw
202-637-9800

[27] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

Comprehensive Privacy and Security: Critical for Health Information Technology

Version 1.0 – May 2008

In this paper, CDT calls for the adoption of a comprehensive privacy and security framework for protection of health data as information technology is increasingly used to support exchange of medical records and other health information. CDT believes that privacy and security protections will build public trust, which is crucial if the benefits of health IT are to be realized. In CDT's view, implementation of a comprehensive privacy and security framework will require a mix of legislative action, regulation and industry commitment and must take into account the complexity of the evolving health exchange environment.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and health information exchange can help improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. At the federal and state levels, policymakers are pushing initiatives to move the health care system more rapidly into the digital age.

However, health IT initiatives pose heightened risks to privacy. Recent breaches of health information underscore that the risks are real. At the same time, there is widespread confusion and misinterpretation about the scope of current health privacy laws. Some are pushing for quick "fixes" to try to address the public's privacy concerns, but fully resolving these issues requires a comprehensive, thoughtful and flexible approach.

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.

Survey data shows that Americans are well aware of both the benefits and the risks 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, people have significant concerns about the privacy of their medical

records. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[28] In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 53% were concerned about insurers gaining access to this information.[29]

Appropriate privacy protections must be incorporated from the outset in the design of new health IT systems and policies. 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 than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy.

As an Internet policy organization and privacy advocate, CDT brings a unique perspective to these issues, based on our experience in shaping workable privacy solutions for a networked environment. In this paper, we describe why it is necessary that all parties—from traditional health care entities and new developers of personal health records, to legislators and regulators—address privacy and security in health IT systems. We emphasize that all stakeholders need to begin immediately to implement and enforce a comprehensive privacy and security framework in all of the various tools and processes of health IT.

The Consequences of Failing to Act

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[30] Without appropriate protections for privacy and security in the healthcare system, patients will engage in "privacy-

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

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

[30] 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).

protective" behaviors to avoid having their personal health information used inappropriately.[31] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[32] 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.[33]

People who engage in privacy-protective behaviors to shield themselves from stigma or discrimination often pay out-of-pocket for their care; ask doctors to fudge a diagnosis; switch doctors frequently to avoid having all of their records in one location; lie; or even avoid seeking care altogether.[34] The consequences are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[35]

Health IT Can Protect Privacy – But Magnifies Risks

Health IT has a greater capacity to protect sensitive personal health information than is the case now with paper records. For example, it is often impossible to tell whether someone has inappropriately accessed a paper record. By contrast, 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

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

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

[33] 2005 National Consumer Survey.

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

[35] Id.

appropriate purposes without needing to create large, centralized databases of sensitive information 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 policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.[36]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects, and the accidental posting of identifiable health information on the Internet by a health plan, underscore these concerns, and are just two of numerous examples. The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with the lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[37]

Elements of a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

A comprehensive privacy and security framework must be implemented by all stakeholders engaged in e-health efforts. Such a framework, as outlined by the Markle Foundation's Connecting for Health, would:

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

[36] 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.

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

Congress should set the framework for national policy through legislation. Ensuring and enforcing adequate protections for privacy and security also will require coordinated actions on the part of key regulatory agencies, as well as industry best practices. The framework should be implemented in part by strengthening the HIPAA Privacy Regulation for records kept by the traditional health system participants, but also needs to address the increased migration of personal health information out of the traditional medical system.

Notwithstanding the urgent need to address privacy, health information policy initiatives - both legislative and administrative – are moving forward without addressing privacy and security at all, or they are taking a piecemeal approach that too narrowly focuses on a single activity, such as e-prescribing, or on just one aspect of fair information practices, such as the appropriate role of patient consent.

In developing a comprehensive framework, policymakers, regulators, and developers of HIT systems need not start from scratch. A framework for HIT and health information exchange already exists, in the form of the generally accepted "fair information practices" ("FIPS") that have been used to shape policies governing uses of personal information in a variety of contexts, most notably the HIPAA Privacy Regulation, which established the first federal health privacy framework.[38] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's Connecting for Health initiative, which includes broad representation from across the health care industry and patient advocacy organizations, describes the principles 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.

[38] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

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

The Connecting for Health Common Framework also sets forth characteristics for network design that can help ensure health information privacy and security.[39] These network design characteristics facilitate health information exchange not through centralization of data but rather through a "network of networks." Such a distributed architecture is more likely to protect information. Other key elements of such a system are interoperability and flexibility, which support innovation and create opportunities for new entrants.

The Role of HIPAA in the New Environment

The federal privacy and security rules that took effect in 2003 under the Health Insurance Portability and Accountability Act (HIPAA) reflect elements of this

[39] See www.connectingforhealth.org for more details on the Common Framework.

framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. The HIPAA Privacy Rule was a landmark in privacy protection, but it is widely recognized that the regulation is insufficient to adequately cover the new and rapidly evolving e-health environment. For example:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by HIPAA's Privacy Rule.
- Personal health records and other consumer access services now being created by third parties, including companies such as Google and Microsoft, as well as by employers usually fall outside of the HIPAA rules.
- Personal health data is migrating onto the Internet through an exploding array of health information sites, online support groups, and other on-line health tools, regulated only through enforcement by the Federal Trade Commission (FTC) of the general prohibition against unfair and deceptive trade practices, such as a failure to follow promised privacy policies.
- While the Privacy Rule includes criteria for de-identifying data, new technologies are making it much easier to re-identify once de-identified health information and to combine it with personal information in other databases, making it more likely that sensitive health information will be available to unauthorized recipients for uses that have nothing to do with treatment or payment.

In addition, the HIPAA rules have never been adequately enforced. The HHS Office for Civil Rights (OCR), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[40]

Historically, states have filled the gaps in federal health privacy laws by enacting legislation that provides stronger privacy and security protections for sensitive data, such as mental health and genetic information. The states continue to have an important role to play, but relying on the states to fill deficiencies in HIPAA's Privacy Rule – or to regulate entities outside of the traditional healthcare sphere – does not provide a comprehensive, baseline solution that gives all Americans adequate privacy and security protections, and does not offer all the entities in the e-health space a predictable and consistent policy environment.

---

[40] "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.

◪ National Conversations about Privacy and Security Have Been Too Focused on the Issue of Individual Consent

The ability of individuals to have some control over their personal health information is important, and a comprehensive privacy and security framework should address patient consent.[41] However, consent is not a panacea. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is less protective of privacy and confidentiality.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated decisions about use of their health data. Most don't read the details of a consent form 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.[42] If mere patient authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are completely outside the scope of the HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if reliance on consent by an individual for any particular use of his or her information is treated by policymakers as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.[43]

---

[41] Much more should be done to improve the way in which consent options are presented to consumers in the healthcare context. Internet technology can help in this regard, making it easier to present short notices, layered notices and more granular forms of consent.

[42] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K. Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

[43] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up

All Entities Should Adopt and Implement a Comprehensive Privacy and Security Framework

Regardless of whether or not Congress takes action to address these issues, states and entities developing health information exchanges and other health IT initiatives should commit to adoption of the comprehensive privacy framework outlined here. Guidance for policy development for health information exchanges can be found, for example, in the Common Framework developed by the Markle Foundation's Connecting for Health Project. Consumer access services such as PHRs must also implement the comprehensive framework through rigorous privacy and security protections.[44] Such entities should make their privacy commitment explicit in a published privacy notice. Consumers should look for these promises and should measure them against the framework. Once companies make a privacy promise, they will be bound to it under the Federal Trade Commission Act. In addition, consumer rating services can compare and assess privacy practices, measuring them against the principles outlined here.

Congress Should Establish a Comprehensive Health Privacy and Security Approach

Although states and the private sector should not wait for action by Congress to protect privacy, CDT believes that Congress should establish national policy to ensure that health information technology and electronic health information exchange is facilitated by strong and enforceable privacy and security protections.

According to recent surveys:

- 75% believe the government has a role in establishing rules to protect the privacy and confidentiality of online health information;
- 66% say the government has a role in establishing the rules by which businesses and other third parties can have access to personal health information; and
- 69% say the government has a role in encouraging doctors and hospitals to make their personal health information available over the Internet in a secure way.[45]

---

with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

[44]See, e.g. the Best Practices for Employers offering PHRs http://cdt.org/healthprivacy/20071218Best_Practices.pdf.

[45] 2006 Markle Foundation Survey.

One of the major challenges in developing a comprehensive privacy and security framework is to integrate any new rules with the HIPAA privacy and security rules. Congress should consider both strengthening HIPAA where appropriate and establishing additional legal protections to reach new actors in the e-health environment.

Congress should set the general rules – the attributes that a trusted health information system must have – based on the Fair Information Practices discussed earlier. Further, Congress should hold a series of hearings on some of the more difficult issues to resolve and develop a full record that will serve as the basis for more specific legislative action. In particular, Congress should consider:

- The appropriate role for patient consent for different e-health activities;
- The ability of consumers to have understandable information about where and how their Personal Health Information (PHI) is accessed, used, disclosed and stored;
- The right of individuals to view all PHI that is collected about them and be able to correct or remove data that is not timely, accurate, relevant, or complete;
- Limits on the collection, use, disclosure and retention of PHI;
- Requirements with respect to data quality;
- Reasonable security safeguards given advances in affordable security technology;
- Use of PHI for marketing;
- Other secondary uses (or "reuses") of health information;
- Responsibilities of "downstream" users of PHI;
- Accountability for complying with rules and policies governing access, use, and disclosure, enforcement, and remedies for privacy violations or security breaches;[46] and
- Uses and safeguards for de-identified information.

Congress Also Should Enact Legislation to Strengthen HIPAA For Health System Entities

With respect to the access, use and disclosure of electronic health information by the traditional players in the health care system, there are some immediate steps Congress could take to fill some of the gaps in HIPAA. For example, Congress can

[46] See the Common Framework, www.connectingforhealth.org.

take a number of actions to secure more meaningful enforcement of the HIPAA rules, including:

- Strengthening Office for Civil Right's (OCR's) role by requiring it to conduct periodic audits of covered entities and their business associates to ensure compliance with the rules;
- Increasing the penalties associated with failure to comply with key provisions of the HIPAA rules;
- Increasing resources dedicated to HIPAA enforcement;
- Requiring OCR to report to Congress on a regular basis on enforcement of the rules; and
- Amending HIPAA to allow for enforcement of the rule by state authorities (such as attorneys general).

Congress should also consider enacting legislative provisions to:

- Establish notification requirements and penalties for data breaches;
- Strengthen the existing HIPAA rules requiring express authorization for use of patient identifiable data for marketing; and
- Require electronic health systems to provide consumers with access to their health information in an electronic format.

Although it is desirable for Congress to enact legislation that fills some of the gaps in HIPAA and to enact a general privacy and security framework to govern health IT, it will be impossible for Congress to legislatively adopt comprehensive rules that fit all of the various actors and business models in the rapidly expanding and evolving e-health environment. Therefore, a second major challenge for Congress is to decide what can be legislated and what must be delegated to agency rulemaking – and what areas are best left to be developed and enforced through industry best practices.

↘ Strengthening Privacy and Security Will Also Require a More Tailored Regulatory Approach

While Congress should establish a strong framework for health privacy and security, it must avoid a "one size fits all" approach that treats all actors that hold personal health information the same. The complexity and diversity of entities connected through health information exchange, and their very different roles and different relationships to consumers, require precisely tailored policy solutions that are context and role-based and flexible enough to both encourage and respond to innovation. For example, it makes little sense to have the same set of rules for

"personal health records," which are often created by and controlled by patients and held by third party data stewards outside the healthcare system, and for "electronic health records," which are created and controlled by health care providers for purposes of treatment and care management. To take another example, rules for use of personal health information for treatment need to be quite different than rules for marketing or other secondary uses. Rules regarding use of health information for research need to be separately considered as well.

Congress should not attempt to develop all of the details in legislation. Rather, Congress should enact legislation specifically recognizing the importance of the privacy rights in health information across technology platforms and business models, setting out principles and attributes to guide one or more regulatory agencies in developing detailed, context-specific rules for the range of entities that collect, use and distribute personal health information in the new interconnected healthcare system. One approach would be to direct the Department of Health and Human Services to strengthen the HIPAA regulations that apply to traditional players in the health system, while also directing HHS or possibly the Federal Trade Commission to issue regulations to govern the handling of personal health information by new players who are part of the broader Internet marketplace and not part of the healthcare system. If more than one agency is to be involved, Congress could require them to work together to avoid issuing conflicting rules (as the financial services regulatory agencies did in developing security rules for financial information).

Tasking HHS and/or the FTC with the responsibility for developing detailed regulations allows for:

- A more tailored, flexible approach that will ensure comprehensive privacy and security protections in a myriad of different e-health environments, and
- More regular, active monitoring of developments in the marketplace and a more rapid response to newly emerging privacy and security issues.

Congress should maintain strong oversight over the regulatory process by:

- Requiring regulations to be developed within a particular timeframe;
- Requiring satisfactory completion of the rulemaking before federal HIT grants can be made;
- Mandating reporting by the agencies on implementation and enforcement; and
- Vigorous oversight and reporting on implementation and enforcement.

Conclusion

To establish greater public trust in HIT and health information exchange systems, and thereby facilitate adoption of these new technologies, a comprehensive privacy and security framework must be in place. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. Congress should set the framework for privacy and security by strengthening enforcement of existing law and ensuring that all holders of personal health information are subject to a comprehensive privacy framework. Congress can also take immediate steps to strengthen existing privacy rules, for example, empowering consumers to play a greater role in their healthcare by mandating electronic access to their health records. Given the broad array of entities in the e-health arena, the technological changes in the marketplace today, and the prospects for rapid innovation, much of the details of that framework should be worked out through the regulatory process. The challenge for policymakers is to find the right mix of statutory direction, regulatory implementation, and industry best practices to build trust in e-health systems and enable the widespread adoption of health IT.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact:
Deven McGraw
Director, CDT's Health Privacy Project
202-637-9800
http://www.cdt.org