Statement of Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology
Before the
Senate Judiciary Committee
"Health IT: Protecting Americans' Privacy in the Digital Age"

January 27, 2009

Chairman Leahy and members of the Committee, thank you for holding this hearing on "Health IT: Protecting Americans' Privacy in the Digital Age."

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

This hearing could not be more timely or more important. Now pending before Congress is economic recovery legislation that includes $20 - 23 billion to promote the widespread adoption of health information technology and electronic health information exchange (commonly referred to as health IT). Health IT holds enormous potential to improve health care quality and engage consumers more actively in their own healthcare, and building and implementing an electronic health information exchange infrastructure is critical to achieving the goals of health reform. Surveys consistently demonstrate the support of the American public for health IT.

At the same time, however, the public is very concerned about the risks health IT poses to health privacy. A system that makes greater volumes of information available more efficiently to improve care will be an attractive target for those who seek personal health information for commercial gain or inappropriate

purposes. Building public trust in health IT systems is critical to realizing the technology's potential benefits. Just two weeks ago, in a hearing before the Senate Finance Committee, the U.S. Government Accountability Office (GAO) stated that "a robust approach to privacy protection is essential to establish the high degree of public confidence and trust needed to encourage widespread adoption of health IT and particularly electronic medical 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. A commitment to spend significant federal dollars to advance health IT must be coupled with a strong commitment to enacting comprehensive privacy and security protections. Congress' role is critical here, and privacy protections must be part of any legislation that promotes electronic health records.

The privacy provisions in the proposed legislation take concrete, incremental steps toward the realization of a comprehensive framework of privacy and security protections for electronic health information, and CDT supports them. However, they are only a first step. Assuring privacy and security for electronic health information will require an ongoing commitment by Congress, the Administration, and the private sector. Congress should consider adding to the bill additional oversight and enforcement language to ensure that the stimulus funds are spent in a way that enhances rather than erodes privacy.

Why Privacy and Security Protections are Critical to Health IT

As noted above, 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. At the same time, people have significant concerns about the privacy of their medical records. 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. [1]

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 among health care system entities for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption and similar technologies can reduce the risk to sensitive data when a system is breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. Tens of thousands of health records can be accessed or disclosed through a single breach. Headlines just last year about the theft of an NIH laptop loaded with identifiable information about clinical research subjects underscored these concerns, and that was 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.[2]

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information. [3] 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.[4] 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

---

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

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

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

[4] Id.

disclosed.[5] Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.[6] The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health.

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

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

To build public trust in health IT, we need the second generation of health privacy — specifically, a comprehensive, flexible privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. Such a framework should be based on three pillars:

- Implementation of core privacy principles;
- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.

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. While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's multi-stakeholder Connecting for Health initiative provides a good model. [7]

Of particular relevance for this hearing, the core privacy principles of the Connecting for Health Common Framework set forth a comprehensive, flexible

---

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

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

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

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. 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 privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA) include provisions addressing some of these principles – but, as discussed in more detail below, the HIPAA rules are insufficient to cover the new and rapidly evolving e-health environment. To get to the second generation of health privacy and build consumer trust in e-health systems, Congress should:

- Direct the Secretary of the Department of Health and Human Services (HHS) to develop policies and programs to ensure that all entities that receive federal funds for health IT adopt and implement policies and technological solutions that address each of the principles set forth above, and to hold funding recipients accountable for complying with such policies and applicable law.
- Strengthen HIPAA for records kept by traditional health system participants (i.e., physicians, hospitals, pharmacists, health plans) and fill gaps in HIPAA's rules where appropriate; and
- Establish 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.

Congress should set the framework for national policy through legislation, but 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.

Why HIPAA is Insufficient to Meet the Challenges Posed by E-Health

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:

- The HIPAA Privacy Rule covers only certain "covered entities" as defined in the HIPAA statute: specifically, providers, plans, and healthcare clearinghouses. Many of the new entities storing, handling or managing personal health information electronically do not qualify as covered entities, and thus are not directly covered by the Privacy Rule. In some cases, other federal privacy laws may apply, but only in specific and limited contexts. As a result, we do not have a baseline set of federal health privacy protections that apply to all entities that handle personal health information. For example, state and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and/or facilitate exchange of personal health information, may not be covered by the Privacy Rule.[8] Further, sensitive health data in

[8] In December 2008 HHS issued guidance clarifying that health information networks that merely exchange data on behalf of covered entities must be business associates, but such guidance does not cover all of the network models currently in existence or in development.

personal health records offered by employers and Internet companies also is not protected by federal health privacy law.

- The Privacy Rule is based on a model of one-to-one electronic transmission of health information among traditional health care system entities and their business partners who perform health-related functions on their behalf. The Rule does not adequately account for new health information networks, which allow broader access to greater volumes of identifiable health information.
- 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, not covered by HIPAA but 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.
- The HIPAA Privacy Rule does not make it clear that patients are entitled to an electronic copy of their records, so patients themselves can transfer their records to other digital services if desired.
- The Privacy Rule's requirements with respect to "marketing" are weak and far too often permit entities to use patients' protected health information without their prior authorization to send them marketing materials regarding health care products or services. The deficiencies in the current rule may be exacerbated by the need of these nascent health data exchanges to find a viable business model to sustain start-up and long-term expenses – a need that these exchanges may seek to fulfill with advertising and other commercial re-uses of patient data.
- The HIPAA rules currently provide no incentive for covered entities to de-identify data or strip it of common patient identifiers before it is used for routine functions such as those contained in the definition of "health care operations," even though, in many instances, these legitimate purposes could be accomplished without using personally identifiable information.

Ensuring Accountability for All Entities Engaged in e-Health

As noted above, the HIPAA Privacy and Security Rules set forth requirements for the handling of individually identifiable health information by covered entities and their business associates (entities that contract with covered entities

to perform functions on their behalf). Not all entities handling personal health information are covered by the rules. In addition, the HIPAA rules were intended to set only a basic floor of protections. To establish an environment of trust that will facilitate the widespread implementation of health IT, all entities handling health information should develop and implement health information policies beyond what HIPAA may require.

The economic recovery legislation will devote an unprecedented level of taxpayer resources to the development and implementation of health IT to improve health care and lay the foundation for further health reform efforts. Persons and entities receiving such federal funds should be held accountable, both for how they use the funds, as well as for adopting and implementing the policies and technological solutions necessary to protect medical data they store and share.

The stimulus legislation includes provisions to strengthen HIPAA, and to establish a process for developing baseline privacy protections that will apply to personal health information held by entities not covered by HIPAA. However, the bill should go further to ensure that health IT is governed by a comprehensive framework of protections that builds public trust and enables the sharing of information for core health care functions. Therefore, Congress should consider adding to the bill language explicitly directing the HHS Secretary to establish policies and programs to ensure: that all entities who receive federal funds for health IT are held accountable for their use of the funds; that they adopt and implement policies and technological solutions addressing each of the core privacy principles identified in this testimony; and that they are held accountable for complying with such policies and other applicable law. Such language would help assure that, regardless of whether HIPAA applies or adequately covers an entity, there is a comprehensive framework of policies in place to protect health information and sufficient oversight and accountability for compliance with that framework. The Secretary should also be required to regularly report to Congress on how funds have been spent and how such privacy and security policies have been implemented.

◪ Strengthening HIPAA Privacy and Security Rules to Meet New Challenges

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 should take to fill gaps in HIPAA. The economic recovery legislation under consideration by Congress takes concrete steps toward filling these gaps and establishing the comprehensive framework of protections that will build public trust in health IT. For example:

Right to Be Notified in the Event of a Breach

The proposed legislation establishes a federal right to be notified in the event of a breach of protected health information, and such breach notification provisions apply to HIPAA-covered entities and their business associates as well as to any other commercial entities that maintain personal health information. These provisions would establish for the first time a national right for consumers to at least be notified when the security of their health information is compromised; currently, only three state breach notification laws expressly apply to health data.[9] Further, the proposed legislation does not require notification when the information that is breached has been rendered inaccessible to unauthorized persons via encryption or a similar technology. This provides a powerful incentive for entities holding personal health information to adopt strong encryption-type controls, significantly minimizing the likelihood of data breach.

Some industry stakeholders are calling for a "harm" standard for breach notification —i.e., patients need only be notified if there is the potential for financial loss or tangible harm, such as loss of a job or insurance. Such standards may be appropriate for breaches of financial data, where harm can be more easily quantified and remedied, but health information is not the same as financial information. Once sensitive medical data is in the public domain or in the hands of an unauthorized person, it cannot be taken back, and the potential harm is difficult to quantify and often subjective (what is sensitive to one person may not be sensitive to another). If harm were the trigger for notification, entities breaching the data would have too much discretion to decide whether the risk of harm to the patient is worth the burden (and potential damage to institutional reputation) of notifying. The provisions in the legislation take the subjectivity out of the decision – and provide strong incentives for entities holding medical data to protect it with encryption-type technologies.

Strengthening Prohibitions Against Unauthorized Use of Data for Marketing Purposes

As noted above in our testimony, more than three-fourths of consumers are concerned about the use of their health information for marketing purposes. The benefits of health IT will not be realized if entities that have access to personal health information are allowed to use it without individual authorization for marketing purposes.

---

[9] Arkansas, California and Delaware. Deborah Gage, California data-breach law now covers medical information, SF Gate (January 4, 2008), See http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U9000.DTL.

Although HIPAA already prohibits use of health information for marketing without patient authorization, the HIPAA definition of marketing includes significant exceptions.[10] These exceptions permit the use of a patient's personal information without consent to facilitate communications from health care providers and plans that can be characterized as patient education— for example, information on treatment alternatives, or benefit options, or care management tools. In fact, the only health-related communications that are clearly marketing – and prohibited without express patient authorization – are those made directly to a patient by a third party selling a product or service, where the covered entity has provided the third party with the personal information that facilitates the making of the communication.[11] However, if the same communication is sent by the covered entity to the patient, it is not marketing – even if the covered entity is paid by the third party to make the communication on its behalf.

The proposed legislation deals with this issue in three ways: (1) by prohibiting the sale of "protected" (identifiable) health information, (2) by making it clear that communications sent by covered entities that are paid for by outside entities are marketing and therefore require prior authorization from the patient, and (3) by requiring covered entities to obtain prior patient authorization before sending fundraising solicitations.

Some claim that these provisions will prohibit the sending of important health communications like flu shot and drug refill reminders. Current HIPAA rules allow covered entities, including providers, health plans and pharmacies, to use patient identifiable information to send these communications without patient authorization, and the provisions in the stimulus legislation do nothing to alter those rules. Instead, they target the inappropriate influence from outside entities over the types of communications sent to patients without their prior authorization. They also make it clear patient information cannot be used for fundraising purposes without a patient's prior authorization. Finally, by including a strong prohibition against the sale of medical records and identifiable personal health information, the legislation attacks current practices that violate patient trust and helps ensure that advances in health information exchange are not inappropriately exploited for commercial gain. These improvements in the rules regarding use of personal health information for marketing and other commercial purposes would greatly enhance patient trust in e-health systems.

---

[10] 45 C.F.R. §164.501.

[11] Office of Civil Rights Brief, Summary of the HIPAA Privacy Rule, p. 9-10.

Giving Patients a Meaningful Right to Monitor Disclosures from Their Medical Records

The HIPAA Privacy Rule gives patients the right to receive an "accounting" of certain disclosures of their health information – but this right does not apply to routine disclosures for treatment, payment or health care operations. Electronic technologies can provide covered entities the ability to track precisely who has accessed a patient's medical record. CDT understands that a number of entities using electronic health records are already employing these electronic "audit trails" to control who can access a patient's record and to internally monitor who is accessing patient records and for what purposes.

The proposed legislation would phase in a requirement for all entities using electronic health records to track disclosures from the record and allow patients, upon request, to receive a copy of such disclosures over a three-year period. When this provision was included in legislation considered in the House of Representatives in the 110th Congress, health care providers and plans weighed in with a number of concerns. Fortunately, these concerns have been addressed in the proposed legislation. For example, the provision directs the Secretary to issue regulations about what must be included in the accounting, taking into account administrative burdens and the needs of patients. Further, the requirement does not go into effect until these regulations are promulgated and standards are adopted that will ensure medical records have the technology in place that will allow them to comply. Entities with existing systems that may not have the technical capacity to comply have until 2014 to come into compliance; those who adopt newer systems must comply by 2011.

Examination of "Health Care Operations"

Under the current Privacy Rule, patient consent is not required for covered entities to use personal health information for health care operations. The definitions of treatment and payment are relatively narrow; however, health care operations encompasses a much wider range of activities, including administrative, financial, legal, and quality improvement activities (see footnote for a complete list). [12] Privacy and consumer advocates have long been

[12] Health care operations include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; (4) Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (5) Business Planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (6) Business management and general administrative

concerned that health care operations permits the use of personal health information for a broader range of purposes than should be permitted under fair information practices.

The proposed legislation addresses this issue by requiring the HHS Secretary to re-examine the health care operations definition and consider whether some functions within this definition should require prior patient authorization. The Secretary is also tasked to consider whether some operations functions can and should be done with de-identified health data (for example, activities such as quality improvement, peer review and credentialing, and business planning). De-identified data has been stripped of a number of common patient identifiers, and thus its use for routine business purposes poses less privacy risk (as long as it is protected from re-identification). We hope HHS will also look at crafting more narrow definitions of, or providing more detailed guidance regarding, some of the broad terms used in health care operations (such as "case management and care coordination") to ensure they are defined to include only core health care functions. Further, as explained in more detail below, the Secretary should also consider using the current "minimum necessary" standard to encourage or require the use of anonymized data to perform many routine health care operations functions.

Clarification of Minimum Necessary

A critical element of fair information practices is that data collection should be limited to what is needed to meet the particular purpose for which the data is lawfully sought. The HIPAA Privacy Rule requires covered entities to request – and use and disclose – only the *minimum amount* of information necessary to accomplish their legitimate purposes, except when information is being used or disclosed for treatment purposes. The minimum necessary provisions are broadly worded and meant to be flexible to respond to the particular context. Unfortunately, covered entities often say that they are confused by the minimum necessary rule – and the frequent result is misinterpretation of the law.

The proposed legislation takes concrete steps toward clarifying this provision. Most importantly, the legislation requires the Secretary to issue guidance on what constitutes "minimum necessary." As the Secretary is developing this guidance, covered entities are directed to use a "limited data set," which is data stripped of a number of common patient identifiers, to meet the minimum necessary requirements. However, in circumstances where the limited data set

---

activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.501.

would be insufficient to meet the covered entity's legitimate purposes for accessing or disclosing the data, entities may use the amount of identifiable data necessary to fulfill that purpose.

In developing guidance on minimum necessary, the Secretary should consider whether fully identifiable patient data is needed to accomplish all the activities currently included in health care operations, and whether data scrubbed of common patient identifiers, which provides greater privacy protection for patients, could serve covered entities' needs to access data without being unduly burdensome. (Such a review should be part of the Secretary's examination of health care operations, which is included in another provision of the legislation and discussed above.) For example, today covered entities may use fully identifiable data for quality assessment and improvement activities, peer review of health professionals, accreditation or credentialing, performing audits, and business planning. For each of these activities, covered entities need access to data about the care that was provided, but in most cases they do not need information that is identified to a particular patient. Using data that has been stripped of key patient identifiers can help protect privacy while allowing the use of data for important health-related functions.

The Privacy Rule includes provisions for two types of anonymized data – the limited data set and de-identified data. However, these data sets require the masking of too much data to be useful for some operations purposes. In issuing guidance on minimum necessary, HHS should set forth additional options for use of data stripped of common patient identifiers for health care operations.

Ensuring Electronic Access for Patients

The HIPAA Privacy Rule provides individuals with a right to access and receive a copy of their medical records, "in the form or format requested," if those records are "readily producible" in that format.[13] However, the access right in the HIPAA rule has not been well implemented. The failure to disclose to patients their medical records - even in paper format - is one of the top five HIPAA complaints investigated by HHS.[14] In addition, the Privacy Rule allows covered entities to charge a "reasonable cost" for copying a patient's record, which reportedly range from free to $37.00 for up to 10 pages.[15] The proposed

---

[13] 45 C.F.R. 164.524(a) & (c) (such access right is for information maintained in a designated record set).

[14]HHS, Compliance and Enforcement, Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year, http://www.hhs.gov/ocr/privacy/enforcement/data/top5issues.html.

[15] State laws may set limits on copying charges for records, which range from free for the first copy (Kentucky) to $37.00 for up to the first 10 pages of a hospital-based record (Texas). See http://hpi.georgetown.edu/privacy/records.html for more information.

legislation addresses this by making it clear that patients have the right to an electronic copy of their medical records at a nominal cost when those records are kept electronically. Congress should strengthen this provision by adding language to clarify that this right of electronic access extends to having an electronic copy sent directly to the individual's electronic personal health record.

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, will not be covered by the HIPAA regulations unless they are being offered to consumers by covered entities. In this unregulated arena, consumer privacy will be protected only by the PHR provider's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the Federal Trade Commission (FTC) may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.[16] 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.

The proposed legislation – which tasks HHS and FTC with jointly coming up with recommendations for privacy and security requirements, as well as breach notification provisions, for PHRs – proposes 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

[16] 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.

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. The legislation lays the foundation for the establishment of these rules, and tasks the FTC with enforcing breach notification provisions until these rules can be established.

In establishing protections for information in PHRs, policymakers need not start from scratch. The Markle Foundation's Connecting for Health initiative last year released a "Common Framework for Networked Personal Health Information" that sets forth practices to protect personal information and enhance individual participation in online personal health records.[17] This framework, developed through a multi-stakeholder, public-private collaboration and endorsed by major PHR vendors and leading consumer groups, could guide both governmental policies and industry best practices.

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 penalty against a HIPAA-covered entity since the rules were implemented.[18] 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, and prosecutors seeking to enforce criminal penalties against individuals have had to rely on other federal laws.[19]

---

[17] See www.connectingforhealth.org/phti for further information.

[18] In July 2008, 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.

[19] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences; see also P. Winn, "Who is Subject to Criminal Prosecution under HIPAA," 2005, http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf.

In addition, 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.[20] Of interest, if the covered entity decides that terminating the contract is "not feasible," the covered entity is required to report the problem to the Secretary.[21] 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.

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.

The proposed legislation includes a number of provisions strengthening enforcement of HIPAA and providing a mechanism for individuals whose privacy has been violated to receive some compensation:

Accountability for Business Associates

The proposed legislation closes this loophole by ensuring that business associates can be held legally accountable for complying with the HIPAA Security Rule and with those provisions of the Privacy Rule that apply to their contractual activities. The legislation does not impose additional obligations on business associates with respect to complying with the Privacy Rule (beyond the additional requirements imposed by the legislation on both covered entities and business associates); instead it ensures accountability to federal authorities when there is a failure to comply.

---

[20] 45 C.F.R. 164.504(e)(ii).

[21] Id.

Strengthened Statutory Provisions Authorizing Criminal and Civil Penalties

To remedy the effect of the Bush OLC memo, the proposed legislation makes it clear that criminal penalties can be assessed against individuals for intentional violations of HIPAA. To ensure that the most egregious HIPAA violations do not go unpunished, the legislation also clarifies that the Secretary can bring an action for civil monetary penalties in circumstances where a criminal violation of HIPAA may have occurred but the Justice Department decides not to pursue the case.

The HIPAA statute requires that the Secretary impose civil monetary penalties for HIPAA violations.[22] Another part of the statute provides the Secretary with the authority to give covered entities the chance to correct the violation, or to adjust the amount of the penalty, but only in cases where the entity did not know (and reasonably could not have known) of the violation or the violation was due to reasonable cause.[23] Unfortunately, under the Bush Administration, HHS issued regulations requiring the Secretary to first try to informally resolve *all* HIPAA complaints, and the agency pursued a policy of voluntary compliance and handled most complaints informally, even in cases where the violation rose to the level of willful neglect. The proposed legislation ensures that civil monetary penalties will be imposed in the most egregious civil cases – those involving willful neglect of the law – by requiring the Secretary to investigate all complaints for which a preliminary inquiry into the facts indicates possible willful neglect and pursue civil monetary penalties in willful neglect cases. The legislation still permits the Secretary to allow for corrective action, and to informally resolve, those cases involving reasonable cause, and where the entity did not know, and reasonably could not have known, of the violation.

Finally, the proposed legislation increases the civil monetary penalties for HIPAA violations, and creates a tiered penalty structure, so that more serious violations are penalized at a higher level. Except in cases of willful neglect, the Secretary may not impose a penalty if the offense is corrected within a 30-day time period and may adjust the amount of the penalty to match the severity of the offense.

Enhancing Enforcement Resources

The proposed legislation also requires that any penalties or settlements collected be directed to HHS for use in enforcing the Privacy and Security Rules and

---

[22] 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).

[23] Section 1176(b)(2) & (3) of the Social Security Act.

expressly authorizes State Attorneys General to enforce HIPAA. The HHS Office of Civil Rights is significantly under resourced, and devoting greater resources – in both dollars and manpower - should help ensure greater accountability for compliance with HIPAA. Currently, only those State Attorneys General who expressly have the authority to enforce federal law by state statute 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. The provisions in the proposed legislation ensure that entities subject to HIPAA will not be prosecuted simultaneously by state and federal authorities.

Providing Consumers with Meaningful Recourse

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. As noted above, the HIPAA statute already provides for criminal and civil monetary penalties, but these penalties do not currently go to the consumers whose privacy was violated. The proposed legislation directs GAO to recommend methodologies for individuals to receive a percentage of any penalties or monetary settlements collected for violations of HIPAA, and within three years the Secretary is required to establish such a methodology by regulation.

Strengthened Accountability to Congress, Raised Visibility of Importance of Privacy

Finally, the proposed legislation requires HHS to annually report to Congress on enforcement of the HIPAA rules and establishes privacy officers in each HHS regional office, which support better enforcement by both increasing Congressional scrutiny and raising the visibility of privacy as an HHS priority. As noted above, Congress should consider strengthening the legislation to ensure accountability for establishing and complying with privacy and security policies that go beyond HIPAA requirements, or for entities not covered by HIPAA.

Other Notable Provisions in the Stimulus Bill

- While the Privacy Rule includes criteria for de-identifying data, these criteria are now more than five years old – and new technologies and the increased availability of data on-line make it much easier to re-identify once de-identified health information. The proposed legislation tasks HHS with coming up with guidance on how best to implement the HIPAA Privacy Rule requirements on deidentification, providing an opportunity for an update to these provisions. CDT hosted a day-long workshop on de-

identification of data last fall, and a paper summarizing the proceedings of that workshop and suggesting areas of further inquiry is in progress.

- The proposed legislation authorizes $10 million for a comprehensive national education initiative to enhance public transparency regarding uses of health information and the effects of such uses.
- The legislation also makes it clear that stronger state privacy rules are preserved, which has always been an important component of HIPAA.

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.[24] HIPAA requires prior patient authorization before certain types of information can be accessed or disclosed, or when information is being sought for purposes like marketing or, in most circumstances, research. The proposed legislation attempts to strengthen the role of consent by requiring covered entities to honor a patient's request to restrict disclosure for payment and health care operations purposes when the patient has paid out-of-pocket for all costs of care. It is critical that where consent is either required or voluntarily sought, health information systems are structured in a way that allows these consents to be 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.

Just yesterday CDT released a paper calling for a rethinking of the appropriate role of consent in health care, which sets forth in more detail why consent is not the sine qua non of privacy protection. (www.cdt.org/healthprivacy) Among other reasons, a consent-based system places most of the burden for privacy

[24] In addition, 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.

protection on patients at a time where they may be least able to make complicated decisions about use of their health data. 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 allows health information to flow for core purposes with consent but also establishes clear rules about 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. The proposed legislation takes concrete steps toward this comprehensive approach.

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. In the economic recovery legislation, Congress must set the framework for privacy and security by: ensuring that all holders of personal health information adopt and are held accountable for complying with a comprehensive privacy framework; filling the gaps in HIPAA's protections; enacting new standards for commercial entities who hold and exchange health information; and strengthening enforcement of existing law.

Thank you for the opportunity to present this testimony in support of the need for a trusted health information sharing environment to support health IT and the provisions in the proposed economic stimulus legislation. These provisions move the nation much closer to securing comprehensive, workable privacy and security protections for electronic health information systems. I would be pleased to answer any questions you may have.

FOR MORE INFORMATION

Please contact: Deven McGraw, (202) 637-9800 x 119, deven@cdt.org