# 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.[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
- 53% were concerned about insurers gaining access to this information.[2]

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.[3] Without appropriate

[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).

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 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]

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.[7] 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.[8]

---

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

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

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

[6] 2005 National Consumer Survey.

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

[8] Id.

## 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 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.[9]

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.[10]

---

[9] 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.

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

## 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.

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.[11] 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:

[11] 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.

- 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 Connecting for Health Common Framework also sets forth characteristics for network design that can help ensure health information privacy and

security.[12] 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 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.

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

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.[13]

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.

## 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.[14] 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

[13] "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.

[14] 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.

personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[15] 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.[16]

## 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.[17] Such entities should make

[15] 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.

[16] 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.

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

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.[18]

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

[18] 2006 Markle Foundation Survey.

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;[19] 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 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

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

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