

Center for Democracy and Technology Transition Memo
Theme: Protecting Consumer Privacy
Issue: Privacy As Enabler of Health Reform

★ Issue/Problem. Better access to information is key to achieving health system reform. Health information technology (“health IT”) - including electronic health records in doctor’s offices, consumer-controlled personal health records largely accessed through Web portals, and electronic health information exchange among providers and payers – facilitates the access to health information that will drive improvements in health care quality and help empower patients to play a greater role in their care. Consequently, every serious proposal for health care reform includes increased use of health IT.

A majority of Americans support greater use of health IT. At the same time, consumers have significant concerns about the privacy of their medical records on-line. While technology has a greater capacity to protect sensitive personal health information than is the case now with paper records, the electronic movement of data also magnifies the privacy risks, requiring strong privacy and security safeguards.

Implementing a comprehensive framework of privacy and security protections for electronic personal health information is critical to building public trust in health IT. Without appropriate protections for privacy, patients will withhold information from their doctors rather than risk its being disclosed or used inappropriately. According to a recent poll, one in six adults – 38 million persons – engage in such “privacy-protective” behavior. 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 will bolster trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits.

However, with rare exception, federal efforts to advance use of health IT have not adequately or appropriately addressed privacy issues. The Bush Administration announced in 2006 they were working on a framework of overarching privacy and security principles that would govern all federal health IT efforts; to date that framework has not been released. The health information privacy rules under HIPAA provide inadequate protection even to traditional data flows among providers and plans and do not even cover new and rapidly evolving services. (For example, HIPAA does not cover the electronic health information exchanges being implemented across the country, which link together unaffiliated doctors in a state or region.) Further, existing federal health information privacy laws do not extend to personal health records (PHRs) being offered by Internet companies and employers or the personal health information being collected by a growing array of Internet health sites. In addition, federal health privacy laws we have on the books have not been adequately enforced.¹

¹ For example, with respect to the HIPAA Privacy Rule, HHS acknowledges that there have been numerous violations of the Rule, but the Department has opted to achieve compliance through voluntary

★Policy History. The Bush Administration has made some progress in establishing nationwide health information exchange but has done little to resolve the privacy issues. A confusing variety of bodies have been chartered to advance health IT and address privacy.² However, progress on achieving health IT adoption has been agonizingly slow, and none has provided comprehensive, actionable guidance on privacy. Further, the Administration has failed to act on the recommendations made by the National Committee on Vital and Health Statistics (NCVHS), which was chartered by Congress to provide guidance on health data privacy issues.

In its efforts to promote HIT, Congress has considered privacy. Indeed, in the past year, there seemed to be an emerging consensus on Capitol Hill around a set of privacy enhancements, although a variety of factors ultimately prevented legislation from passing. The Senate Wired for Health Care Quality Act (S.1693) was marked up by the HELP Committee in August 2007. In 2008, the bill's co-sponsors accepted a privacy amendment from Sen. Leahy but attempts to pass the bill by unanimous consent failed. In Summer 2008, the House Energy & Commerce Committee marked up and reported the PRO(TECH)T Act (H.R.6357), which included comprehensive privacy protections. The House Ways & Means Health Subcommittee held a hearing on health IT in July 2008, and Members of the Subcommittee introduced their own bill, with similarly strong privacy provisions (H.R. 6898). However, time ran out before the House bills could receive further consideration. CDT supported the Leahy amendment and House bills.

To some extent, the debate over health privacy has focused unduly on the issue of "consent." Enhancing the role of individual consent is one key element of privacy protection, but consent is not a panacea. A more nuanced approach to consent is needed. On the one hand, consent may not be needed on a disclosure-by-disclosure basis for treatment and payment, while on the other hand, there must be protections against the obtaining of consent on an uninformed or blanket basis for marketing or other problematic uses.

★What the Obama Administration and New Congress Should Do. To build public trust in health IT, the Obama Administration should use existing authorities and work with Congress to fill statutory gaps in order to achieve a comprehensive, flexible privacy and security framework that sets clear rules for access, use and disclosure of personal health information by all entities engaged in e-health. Congress has a role in setting a legislative framework of protections that apply across the board; but relevant administrative agencies (in particular HHS and FTC) should fill in the details with regulations and guidance targeted to meet the unique issues raised by the different health IT models.

adherence and has not levied a single civil monetary penalty in the nearly five years since the Rule was implemented.

² Federally sponsored bodies that have addressed various privacy aspects of HIT include the American Health Information Community (AHIC), the Certification Commission for Health IT (CCHIT), the Health Information Technology Standards Panel (HITSP), and the Health Information Security and Privacy Collaboration (HISPC).

In particular, President Obama should --

(1) Adopt a broad policy framework that is based on fair information practices and applies to all federal efforts to advance health IT, and that can serve as a guide for further legislation and regulatory action on a more detailed level. One model for such a framework, which has been supported by a wide range of stakeholders, is the “Common Framework” proposed by the Markle Foundation’s Connecting for Health Initiative.

(2) Strengthen the HIPAA Privacy Rule for electronic records kept and exchanged by traditional health system entities and back it up with more vigorous enforcement. Much of this can be accomplished through modifications to the Privacy Rule and issuance of agency guidance.

(3) Work with Congress to develop appropriate legislation so that all entities that handle personal health information are required to comply with a baseline of privacy protections.

See **Appendix** for more detailed recommendations.

★ **Campaign Platform.** During his campaign, President Obama pledged to invest \$10 billion a year over the next five years to move the U.S. healthcare system into the digital age while also ensuring that patient privacy is protected. Campaign materials did not include details on privacy protections for health information.

★ **Other Voices.** The health care sector is perhaps the most complex in the U.S. economy, with many entrenched interests. A comprehensive framework approach will be endorsed by consumers and employers who support health IT and are seeking a workable approach to resolving privacy concerns. However, health industry stakeholders who want to preserve the status quo with respect to HIPAA may oppose attempts to revisit particular provisions of the Privacy Rule. Entities not covered under HIPAA or any other federal health privacy law may resist efforts to regulate them.

★ **For More Information.**

CDT issue expert: Deven McGraw, deven@cdt.org, 202-637-9800 x119

Resources:

- CDT, “Policy Framework for Protecting the Privacy and Security of Electronic Health Information” (2008)
<http://www.cdt.org/healthprivacy/20080514HPframe.pdf>
- Markle Foundation Policy Brief – We Need a 21st Century Approach to Privacy (September 2008)
http://www.connectingforhealth.org/resources/20080822_policy_brief.pdf
- Beyond Consumer Consent (2008)
<http://www.cdt.org/healthprivacy/20080221consentbrief.pdf>

- CDT Testimony before the House Ways & Means Health Subcommittee (July 2008) <http://cdt.org/testimony/20080724mcgraw.pdf>
- CDT Testimony before the House Energy and Commerce Health Subcommittee (June 2008) <http://www.cdt.org/testimony/20080604mcgraw.pdf>

November 26, 2008

Appendix – Privacy Solutions That Enable Health IT

- Ensure that all entities that collect, store or manage personal health information are required to comply baseline health information privacy and security protections:
 - Adopt a broad policy framework based on fair information practices that governs all federal efforts to advance health IT. (Can be done administratively by executive order; can also be imposed using the government’s power as a purchaser of health care)
 - Ensure that traditional health system entities who are covered by HIPAA and entities that handle personal health information on their behalf (“business associates”) are at least held accountable to the minimum standards in the HIPAA rules. (Likely requires legislation)
 - Ensure that health information exchanges (commonly known as HIEs or Regional Health Information Organizations (RHIOs)), which today are not covered under HIPAA, are required to comply with HIPAA requirements, either as covered entities or business associates depending on their structure and functions. (Likely requires legislation)
 - Establish privacy and security protections for personal health information stored with or managed by non-health care entities (such as employers and Internet companies). It is neither sufficient nor effective to extend the HIPAA Rule to these entities. Instead, Congress will probably have to pass a statute with some parameters and authorize the FTC, in consultation with HHS, to develop and enforce appropriate protections. (Likely requires legislation)
- Establish a federal, individual right to be notified in the event of a breach of identifiable health information; such a requirement should probably include an exemption for information that is encrypted. (Requires legislation, although details can be delegated to HHS to develop in regulations; could also be imposed as a funding condition).
- Ensure appropriate standards are in place for the use of data that has been stripped of identifiers so that it is anonymous to the data holder. Includes revisiting the current standards in the Privacy Rule for de-identification and use of what are called “limited data sets” to ensure they continue to minimize the risk of re-identification while serving the needs of researches and others (HHS can do by regulation), and establish penalties for re-identification that apply to all data recipients (requires legislation).
- Establish clear rules regarding the use of personal health information for marketing and commercial purposes that are not solely reliant on patient authorization. Includes tightening the definition of marketing in the Privacy Rule for HIPAA covered entities (HHS can do by regulation), as well as setting clear standards for the use of

data for marketing and other commercial purposes by non-health care entities (likely needs legislation; authorize FTC to set and enforce rules, working with HHS).

- Ensure strong oversight and accountability for all entities handling health information. Will require strengthening HIPAA enforcement by: (1) clarifying the HIPAA statute so that criminal penalties can be imposed against individuals, and to ensure civil monetary penalties are imposed in cases of willful neglect of the rules; and (2) providing additional enforcement resources, such as through an increase in appropriations to HHS and/or by expressly authorizing states to enforce. (May require legislation; at a minimum, requires HHS adopt stronger enforcement focus) Will also require FTC to take a more active role to ensure enforcement of consumer protections against non-health care entities.
- Revisit the scope of the concept of “health care operations,” a category of uses under the current Rule that does not require patient authorization. Reconsideration of the scope of the exception is particularly appropriate for situations where data is shared outside of a HIPAA-covered health care entity for such purposes. Require the use of anonymized data for health care operations that do not need identifiable data. Consider whether some purposes under “operations” should require patient authorization. (HHS can do by regulation)
- Strengthen the role of patient consent by requiring opt-in before patient health information is stored in or shared through an electronic health information exchange, particularly where the exchanges are used for purposes beyond treatment (requires legislation), and by ensuring that health information stored in personal health records and other consumer-facing tools is accessible only with patient authorization (may require legislation or enhancing current legal authorities). Consider also strengthening the HIPAA “right to restrict” the access and disclosure of health information, particularly for more sensitive health data (HHS can reach HIPAA covered entities by regulation; legislation is required to reach other data holders).
- Ensure individuals can promptly obtain electronic copies of their health information from health care providers and plans (HHS can do by HIPAA guidance) and require entities with electronic health record systems to provide audit trails of uses and disclosures to individuals upon request (HHS can do by regulation for HIPAA covered entities; may require legislation for others).
- Devote more resources to education about health privacy and the protections under current law, for both patients and for those required to comply with the laws, and develop and disseminate model privacy notices (a one-page summary notice and a longer, more detailed notice) that more clearly explain how information can be used and disclosed and patient’s rights under current law. (May require increased appropriations; otherwise HHS and FTC can do through regulation and policy)

For assistance in developing specific language, please contact Deven McGraw, Director, Health Privacy Project at CDT, 202-637-9800 x119, deven@cdt.org.