Comments to Notice and Draft Description of Health Information Technology Extension Program

CENTER FOR DEMOCRACY & TECHNOLOGY
Keeping the Internet Open, Innovative and Free

June 11, 2009

Charles Friedman
Deputy National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
United States Department of Health and Human Services

Dear Mr. Friedman:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive policies to protect the privacy and security of health data as it is increasingly exchanged through the use of information technology. We submit these comments in response to the request for information issued by the Department of Health and Human Services (HHS).

Health information technology (HIT) and electronic health information exchange have the potential to improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers – because they believe such access is likely to increase their quality of care.

At the same time, however, people have significant concerns about the privacy of their medical records, posing the risk that people will not trust, and therefore will not use, electronic health records systems if they do not protect privacy and security. Protecting privacy is important not just to avoid harm, but because good healthcare depends on accurate and reliable information.[1] Without appropriate protections for privacy and security in the health care system, patients will withhold information from their health providers due to worries about how the medical data might be disclosed.[2]

New technologies, new obligations imposed by the economic stimulus legislation, and the likelihood of further changes resulting health reform mean that providers will face a

[1] 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).

[2] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Health Privacy Survey, California HealthCare Foundation, http://www.chcf.org/topics/view.cfm?itemID=115694. *See also* Harris Interactive, "Many U.S. Adults are Satisfied with Use of Their Personal Health Information," (March 2007), http://harrisinteractive.com/harris_poll/index.asp?PID=743.

barrage of unfamiliar and challenging implementation and compliance issues when it comes to privacy and security protection. It is critical that providers receive early, effective guidance on how to navigate these new responsibilities and implement a comprehensive framework of privacy and security protections for health data. Further, privacy and security must be incorporated from the outset in the design of HIT systems and information sharing policies. It is often difficult to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult (and costly) than building it in at the start.[3] This holds true not just for the technical attributes of an HIT system, but also the manner in which privacy and security policies are developed and implemented and health professionals are trained. Regional extension centers should play a vital role in providing the right technical assistance, policy advice and training assistance in privacy and security to health care providers at these early stages of HIT adoption.

Accordingly, we ask HHS to:

- Include privacy/security as a pervasive component of the missions of regional extension centers; and
- Establish extension centers as an interface with regional privacy officers.

We have also endorsed letters submitted by the Markle Foundation and the Consumer Partnership on eHealth that address broader issues that should be included in the mission of the extension centers. This letter focuses exclusively on the centers' responsibilities with respect to promoting privacy and security.

I. Include privacy/security as pervasive component of the mission of regional extension centers

Section 3012 of the American Recovery and Reinvestment Act of 2009 (ARRA)[4] authorizes HHS to create regional extension centers to provide technical assistance and disseminate information in support of HIT implementation. The Section identifies the objective of extension centers as enhancing the adoption of HIT, and lists six missions of extension centers to accomplish this objective. Mission (C) is to disseminate best practices and research on the effective use of HIT to protect the privacy and security of health information.[5] We applaud the inclusion of privacy and security as a best practices topic. However, HHS should explicitly incorporate privacy and security more pervasively into the missions of the extension centers.

Per Section 3012, mission (A) requires extension centers to assist with the implementation and effective use of HIT and electronic health records to health care

---

[3] *See* Center for Democracy and Technology, "Comprehensive Privacy and Security: Critical for Health Information Technology," (May 2008), http://cdt.org/healthprivacy/20080514HPframe.pdf.

[4] Pub. L. 111-5.

[5] ARRA Sec. 3012(c)(3)(C).

providers.[6] HHS should explicitly define "effective use" as encompassing privacy and security practices. Health care entities that apply weak or improper privacy safeguards to their HIT systems are not using HIT effectively. Insufficient privacy and security protections can interfere with patient care, expose the health care entity to liability, and undermine trust for HIT as a whole. As HHS notes, robust technical assistance is key to ensuring health care providers overcome the complexities of implementing HIT.[7] The privacy and security measures that are crucial to the success of HIT are likewise complex, and health care providers should have all the technical support necessary to operate HIT in compliance with privacy laws and meaningful use criteria.[8] HHS should explicitly require extension centers to assist health care entities with privacy and security compliance and implementation as essential elements of the effective use of HIT.

Mission (F) requires regional extension centers to integrate HIT in the training of health professionals.[9] For the reasons mentioned above, HHS should explicitly require privacy and security to be components of the training health care professionals receive from extension centers.

Finally, HHS will award financial assistance on the basis of merit to entities seeking to become regional extension centers.[10] To ensure that these extension centers can provide effective guidance on privacy and security, center applicants should be required to demonstrate that they have, or can contractually acquire, sufficient knowledge, expertise and experience in health information privacy and security. Extension center applicants also should be required to specify in detail how privacy and security issues will be integrated into the training and technical assistance offered to health care entities.

II. Establish extension centers as an interface with regional privacy officers.

ARRA Section 13403 calls for privacy officers to be installed in HHS regional offices. HHS should position regional extension centers as both an interface and a feedback loop for those officers in order to improve privacy practices in the field. Privacy officers should be encouraged to maintain a dialogue with extension centers to gain information about the privacy and security issues facing health care entities adopting HIT. Because

---

[6] *Id*. at (A).
[7] HHS Notice, Fed. Reg. Vol. 74, No. 101, Pg. 25550.
[8] Patient data privacy and security should be core requirements of meaningful use criteria. The Markle Foundation has released a report containing a consensus framework for defining both "meaningful use" and "certified or qualified EHR." The framework lays out seven principles for defining these terms, with major emphasis on protecting patient privacy. *See* Markle Foundation, "Achieving the Health IT Objectives of the American Recovery and Reinvestment Act," (April 2009), http://www.markle.org/downloadable_assets/20090430_meaningful_use.pdf.
[9] ARRA Sec. 3012(c)(3)(F).
[10] ARRA Sec. 3012(c)(2).

extension centers will serve multiple providers, they are likely to have an overarching perspective of the implementation challenges facing the region.

Privacy officers should also be encouraged to offer guidance to extension centers that can then be passed on to health care providers. Because extension centers should provide comprehensive training and technical assistance to health care providers, the guidance that extension centers receive from privacy officers can ripple out to a broad number of providers. However, these comments should not be seen as limiting the additional importance of direct, one-on-one relationships between privacy officers and individual health care providers without extension centers as intermediaries. Rather, we recommend that extension centers operate as trusted intermediaries offering supplemental guidance in coordination with regional privacy officers in order to improve privacy and security practices in the field.

We further maintain that extension centers are not a replacement for the official oversight of the HIPAA privacy and security regulations conducted by the Office of Civil Rights or the Centers for Medicare & Medicaid Services. It is not the role of extension centers to interpret HIPAA rules. Instead, extension centers should be viewed as vehicles for educating providers on official interpretations of the rules and assisting entities implement privacy and security policies and procedures that are consistent with fair information practices[11] and that comply with any federal funding requirements and applicable laws.

III. Conclusion

We appreciate the opportunity to provide these comments in response to HHS' notice and draft description on the regional extension center program. In summary, we ask HHS to:

- Include privacy/security as a pervasive component of the missions of regional extension centers; and
- Establish extension centers as an interface with regional privacy officers.

Please let us know if you have any questions or would like further information.

Sincerely,

The Center for Democracy & Technology

[11] For example, extension centers could give providers guidance on how to establish policies and procedures that are consistent with the National Privacy and Security Framework released by HHS in December 2008. *See* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html.