epic.org

June 9, 2008

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

VIA U.S. MAIL and FACSIMILE (202-226-0092)
Rep. Edward J. Markey
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515-2107

RE: Health IT Legislation and the Need for Clear Privacy Protections

Dear Congressman Markey:

We write in response to your May 28, 2008 letter asking the Electronic Privacy Information Center (EPIC) to comment on the privacy and security implications of the May 22, 2008 Discussion Draft to Promote the Adoption of Health Information Technology circulated by the House Energy and Commerce Committee.

We commend the Committee for raising the vital issues implicated by health IT. The Discussion Draft is an important step on the path to developing new technologies to assist with the delivery of health care services. Of course, Americans also expect strong protections for their health data. For any health IT proposal to succeed, it must incorporate appropriate safeguards for privacy and security.

EPIC welcomes this opportunity to comment on the creation of a health IT infrastructure to provide strong privacy safeguards for consumers' personal medical information.

Americans Demand Strong Health Privacy Protections

Studies consistently show that most Americans support efforts to provide electronic access to their medical records, but have grave concerns about the privacy risks.[1] Three-quarters of the public supports government-mandated medical privacy rules.[2] Other research indicates that more than 50% of employees fear that their health insurance information might be used by employers to limit job opportunities.[3]

---

[1] *See, e.g.* The Markle Foundation, *National Survey on Electronic Personal Health Records*, November 2006, *available at* http://www.patientprivacyrights.org/site/DocServer/Markle_survey_dec_2006.pdf?docID=1161.

[2] *Id.* at 4.

[3] California HealthCare Foundation, *National Consumer Health Privacy Survey 2005*, November 9, 2005, *available at* http://www.chcf.org/topics/view.cfm?itemID=115694.

Strong health IT privacy protections also help ensure that individuals will seek the treatments that they need and will be forthcoming with physicians so that a complete and accurate diagnosis is possible. Comprehensive privacy and security safeguards are necessary components of federal health IT legislation. If legislation does not include sufficient privacy protections, consumers' concerns, joined with the increase in data breaches, could slow or simply halt public acceptance of health IT programs.

Health IT Data Breaches Threaten Patient Privacy

Consumers' fears about the theft and misuse of health care data are well founded. Despite citizens' unambiguous desire to keep their medical information private, their wishes have been frustrated by numerous medical data breaches. For example, in April 2008, 130,000 Wellpoint, Inc. customers learned that the health insurer disclosed their private medical records, including their social security numbers, on the Internet.[4] This followed a virtually identical February breach that disclosed health information on the Internet regarding 71,000 people enrolled in Georgia public health programs.[5] These reports make clear that numerous privacy violations have exposed millions of Americans' medical information to criminals, identity thieves, and other prying eyes.

Disclosure of medical data without patient consent creates two types of privacy violations.

First, the unauthorized disclosure of sensitive personal information is itself a violation of patient privacy. For example, at least sixty-eight UCLA Medical Center employees recently breached the privacy of numerous celebrity patients and co-workers.[6] State regulators faulted the hospital for failing to secure electronic patient records.[7]

Second, medical records contain information that can enable additional privacy violations. For example, medical records often contain patient social security numbers, addresses, financial information, and insurance details. This data can be used to steal identities and commit financial fraud. Earlier this year, a United Healthcare Services data breach disclosed hundreds of medical records containing social security numbers and

---

[4] Bruce Japsen, *Patient data faced exposure*, Chicago Tribune, April 16, 2008, *available at* http://www.chicagotribune.com/business/chi-wed-medical-records-theft-apr16,0,5204130.story.

[5] Brenda Goddman, *Georgia Patients' Records Exposed on Web for Weeks*, N.Y. Times, April 11, 2008, *available at* http://www.nytimes.com/2008/04/11/us/11records.html?_r=1&oref=slogin.

[6] Charles Ornstein, *More tied to UCLA snooping*, Los Angeles Times, May 13, 2008, *available at* http://www.latimes.com/business/careers/work/la-me-ucla13-2008may13,0,4998130.story.

[7] California Department of Health Services, *Statement of Deficiencies and Plan of Correction*, April 28, 2008, *available at* http://www.cdph.ca.gov/HealthInfo/news/Documents/UCLAMedCtrBreachRecords.pdf.

caused a rash of identity theft and tax fraud.[8] In addition, fraudulently obtained health information has been used to commit "medical identity theft," impersonation to gain access to health care. Medical identity theft is particularly troubling because it can result in the inclusion of inaccurate information in patient files through the insertion of an identity thief's charts in a victim's file.[9] "Abundant evidence exists that the creation of false [medical] records can [be] ... potentially life-threatening."[10]

Health IT remains in its relative infancy. Yet the World Privacy Forum has already received at least 20,000 reports of medical identity theft.[11] Absent effective and meaningful health IT privacy protections, such incidents are sure to rise, at great cost to patients.

Health IT Should Include Effective and Meaningful Privacy Safeguards

The Discussion Draft contains several important provisions. EPIC commends the inclusion of breach notification (Sec. 302 and Sec. 315), as well as the draft's preservation of patients' rights under state law (Sec. 321).

However, the Discussion Draft lacks several essential privacy and security safeguards, including: 1) a clear statement of Americans' right to the privacy of their health records, and their right to limit the disclosure of their health records at their discretion; 2) incorporation of enhanced privacy protections for especially sensitive health information; 3) the establishment of a patients' right of action for individuals whose medical privacy is violated; and 4) a requirement that companies take commonsense steps to secure electronic health information. Any legislation without these features exposes Americans' sensitive health records to unauthorized access by snoops and identity thieves.

Patient Consent is the Foundation of Medical Privacy

Any successful health IT legislation must give patients the ability to control their medical information. This is the public's simple expectation. Consumers want to control who accesses their medical information, and determine the extent of the data that is revealed to others. This is the purpose of Fair Information Practices, which help ensure that no secondary use of personal information occurs without the individual's consent. This expectation must be reflected by an unambiguous statement in health IT legislation

---

[8] University of California – Irvine, *Identity Theft Alert*, May 28, 2008, *available at* http://www.uci.edu/identitytheftalert/.

[9] Pam Dixon and Robert Gellman, *Medical Identity Theft: The Information Crime that Can Kill You*, May 3, 2006, at 36, *available at* http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

[10] *Id.* at 35-36.

[11] Science Daily, *Medical Identity Theft: The Importance Of Protecting Your Health Records*, October 10, 2007, *available at* http://www.sciencedaily.com/releases/2007/10/071009132111.htm.

that recognizes Americans' right to the privacy of their personal health information. Many state laws already embody this right.[12] Yet, the Discussion Draft lacks a plain statement of Americans' right to keep their health information private, or a statement requiring informed consent prior to disclosure. Federal legislation should set the standard in protecting patient health information, not lag behind existing state laws.

Particularly Sensitive Medical Records Require Enhanced Protection

The Discussion Draft does not provide enhanced confidentiality protections for especially sensitive medical information. Enhanced protections are provided under existing state and federal laws for medical information regarding such topics as mental health care,[13] substance abuse,[14] genetic data,[15] and cancer treatment.[16] These provisions recognize that some medical information is particularly sensitive, and that the release of such data can result in increased distress and heightened consequences for patients. The Discussion Draft must include enhanced privacy protections for especially sensitive medical information. Such enhanced protections could take the form of increased security requirements, heightened consent standards, or more stringent penalties for violators.

A Patients' Right of Action Would Enhance Medical Privacy

The Discussion Draft does not create a private right of action for patients. Private rights of action serve two important purposes in the health IT context. First, they enable patients, those most directly harmed by medical privacy breaches, to enforce Congress' intent. Regulators and Attorneys General have limited resources. A private right of action enables millions of Americans to assert their right to medical privacy without the expenditure of public funds. Second, a patients' right of action would provide strong incentives for health record custodians to safeguard patient privacy. A patients' right of action is not unprecedented – many state medical privacy laws include such provisions.[17]

---

[12] *See, e.g.* Cal. Civ. Code §§ 56.10, 56.20(c) (2007) (stating "[n]o provider of health care, ... shall disclose medical information regarding a patient ... without first obtaining an authorization ..."); Minn. Stat. §144.293 (2007) (requiring "[a] provider ... may not release a patient's health records to a person without a signed and dated consent from the patient ... authorizing the release."); Wis. Stat. § 146.82(1) (2007) (stating "[a]ll patient health care records shall remain confidential. Patient health care records may be released only ... with the informed consent of the patient ...").

[13] 45 C.F.R. § 164.508(a)(2) (2007).

[14] 42 C.F.R. § 2.1 (2007).

[15] Genetic Information Nondiscrimination Act of 2008 Sec. 105, Pub. L. No. 110-233.

[16] Minn. Stat. § 144.672 (2007).

[17] *See, e.g.* Cal. Civ. Code §§ 56.35; 56.36(b) (2007) (providing for recovery of actual and punitive damages); Minn. Stat. § 72A.503; 13.08 (2007) (providing for recovery of actual and exemplary damages); Wis. Stat. § 146.84 (2007) (providing for recovery of actual and exemplary damages).

The inclusion of a private right of action in the Discussion Draft would greatly enhance the law's effectiveness.

The private right of action is particularly important given the failure of current enforcement under HIPAA. HIPAA provides for regulatory enforcement of patients' privacy rights by the Department of Health and Human Services (HHS). Between April 14, 2003, the effective date of the HIPAA privacy rule, and May 2, 2008, HHS received more than 32,000 complaints of HIPAA privacy violations.[18] The HHS has statutory authority to assess civil monetary penalties.[19] In response to the complaints of more than 32,000 Americans, the HHS has imposed zero civil monetary penalties.[20] The Department of Justice (DOJ) has statutory authority to pursue criminal penalties for HIPAA privacy violations.[21] More than five years after HIPAA's privacy rule, the DOJ has prosecuted few violators, resulting in one reported verdict.[22] These statistics highlight the failure of health privacy enforcement under HIPAA. A private right of action would result in more effective medical privacy enforcement.

Security Requirements Would Increase Patients' Privacy

The Discussion Draft provides some incentives for adoption of security measures (Sec. 315), and contemplates future research regarding health IT security (Sec. 3001(c)(3)(A)(iv)). However, it does not require entities to encrypt health data, implement audit trails, or implement various other reasonable security precautions. Effective health IT privacy requires strong health IT security. The Discussion Draft should require entities to secure their patients' health information. EPIC has supported encryption and audit trail requirements in other contexts.[23] The Federal Trade Commission recognizes the value of strong security protections. The Commission has repeatedly required companies, as a condition of settling their liability for privacy

---

[18] HHS, *Compliance and Enforcement*, May 2, 2008, *available at* http://www.hhs.gov/ocr/privacy/enforcement/data/complaintsyear.html.

[19] 42 U.S.C. § 1320d-5 (2007).

[20] Michael Cassidy, *HIPAA Criminal Verdict and Enforcement Statistics*, April 12, 2007, *available at* http://www.medlawblog.com/archives/compliance-hipaa-criminal-verdict-and-enforcement-statistics.html; Rob Stein, *Medical Privacy Law Nets No Fines*, The Washington Post, June 5, 2006, Page A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html.

[21] 42 U.S.C. § 1320d-6 (2007).

[22] *U.S. v. Ferrer*, No. 06-cr-60261 (S.D. Fla. April 30, 2007).

[23] *See, e.g.* EPIC, *Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information*, August 30, 2005, available at http://epic.org/privacy/iei/cpnipet.html; EPIC, *Data Security: The Discussion Draft of Data Protection Legislation, Testimony before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection*, July 29, 2005, available at http://epic.org/privacy/choicepoint/datasec7.28.05.html.

breaches, to implement commonsense security measures, including security audits.[24] Such measures reduce the likelihood of security breaches, and enhance data privacy. It is important to implement thoughtful security practices now, before data breaches expose Americans' medical information on a massive scale.

EPIC appreciates this opportunity to comment on the privacy aspects of health IT legislation. The work of the Committee on this vital issue impacts the privacy of all Americans.

Sincerely,

Marc Rotenberg
EPIC Executive Director

John Verdi
EPIC Staff Attorney

Sai Lui
EPIC IPIOP Clerk

Ginger McCall
EPIC IPIOP Clerk

cc: Chairman John D. Dingell
Vice Chair Diana DeGette
Ranking Member Joe Barton

[24] *See, e.g.* U.S. Federal Trade Commission, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data*, March 27, 2008, *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm; U.S. Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006, *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm; U.S. Federal Trade Commission, *DSW Inc. Settles FTC Charges*, December 1, 2005, *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm.