epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 5, 2017

The Honorable Tim Murphy, Chair
The Honorable Diana DeGette, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: Hearing on "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships"

Dear Chairman Murphy and Ranking Member DeGette:

We write to you regarding the hearing "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships."[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal health data has led to staggering increases in identity theft, security breaches, and fraud in the United States. Congress should develop meaningful safeguards for the privacy and security of Americans' health information.

The Electronic Privacy Information Center was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[2] EPIC has also filed amicus briefs regarding medical data privacy.[3]

---

[1] *Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships* 115th Cong. (2017), H. Comm. on Energy & Comm., https://energycommerce.house.gov/hearings-and-votes/hearings/cybersecurity-heath-care-sector-strengthening-public-private (April 4, 2017).

[2] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf; Letter from EPIC to the U.S. House Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on FTC Oversight (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf.

[3] *See e.g.* Brief of *Amicus Curiae* EPIC, *IMS Health v. Sorrell*, 564 U.S. 562 (2011).

As EPIC stated in an amicus brief in the U.S. Supreme Court case of *IMS Health v. Sorrell*:

> Health care providers face the unique challenge of providing quality, affordable health care, while protecting each patient' s fundamental right to privacy. The use of electronic databases reduces institutional costs, integrating applicable data from multiple sources, and allowing patients to receive a higher and more accurate level of care, but without proper safeguards, these databases pose a serious threat to privacy.[4] However, this transition to centralized depositories for health care information may lead to the disclosure of private medical records to secondary actors, such as researchers, economists, statisticians, administrators, consultants, and computer scientists.[5]

In 2016, approximately 300 health care sector data breaches compromised the health data of over 4 million patients.[6] Recent data breaches affecting over one million people in the health care sector include:

- ***Banner Health (2016)***. In August 2016, Banner Health, one of the largest nonprofit health care systems in the country, announced that cyber attackers may have gained access to patient information of approximately ***3.7 million people***.[7]
- ***21st Century Oncology (2016)***. In March 2016, cancer-care giant 21st Century Oncology notified patients of a data breach via unauthorized access to their database. The compromised database included names, Social Security numbers, physician's name, diagnosis and treatment information, and insurance information of ***2.2 million patients*** nationwide.[8]
- ***Premera Blue Cross (2015)***. In March 2015, health insurance provider Premera announced that hackers gained accessed to names, birthdates, addresses, telephone numbers, SSNs, member ID numbers, bank account information, and claim information of ***11 million customers***. The hackers also gained access to private health information.[9]
- ***Anthem (2015).*** In February 2015, health insurance giant Anthem announced that a breach exposed the names, birthdates, SSNs, health care ID numbers, home addresses, email addresses, and employment information for ***78.8 million people***.[10]

---

[4] See Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. LAW, MED., & ETHICS 98, 98-99 (1997) (summarizing industry and research use of personally identifiable health care information).

[5] Brief of *Amicus Curiae* EPIC at 12-13*, IMS Health v. Sorrell*, 564 U.S. 562 (2011).

[6] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, https://www.privacyrights.org/data-breaches.

[7] Press Release, Banner Health, *Banner Health Identifies Cyber Attack* (Aug. 2, 2016), *available at* https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack.

[8] Press Release, 21st Century Oncology, *21st Century Oncology Notifies Patients of Data Security Incident, Offers Protection* (Mar. 4, 2016), *available at* http://www.prnewswire.com/news-releases/21st-century-oncology-notifies-patients-of-data-security-incident-offers-protection-300230892.html.

[9] Premera Blue Cross, *About the Cyberattack* (2016), https://www.premera.com/wa/visitor/about-the-cyberattack/; Identity Theft Res. Ctr., *Data Breach Reports* 136–37 (Dec. 31, 2015) [hereinafter "ITRC 2015 Report"].

[10] ITRC 2015 Report, *supra*, at 152; Anthem, *How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services* (Aug. 25, 2015), https://www.anthemfacts.com/.

Unlike financial sector breaches where accounts can be closed and account numbers reissued to minimize further risk, privacy cannot be restored after data breaches of health data.[11] Strong data privacy protections must be built in to electronic health systems to protect patients from the life-long impacts of health data breaches. In her essay *The Future of Health Privacy*, EPIC Advisory Board member and President of Patient Privacy Rights Dr. Deborah Peel provides examples of privacy-enhancing technologies that should be required to be implemented in health care IT systems, including:

- Strong voluntary cyber IDs or credentials;
- Secure e-mail communications systems;
- Tough data access control systems;
- Consent management systems;
- Electronic health records that allow patients to segment (hold back) sensitive information;
- Health databanks; and
- Automated downloading of both personal data and lists of all data users.[12]

The implications of weak security requirements for health care IT systems are far-reaching. If Congress fails to develop appropriate safeguards, the country will face growing risk.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on Oversight and Investigations on these issues.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

[11] Dr. Deborah Peel, *The Future of Health Privacy*, in PRIVACY IN THE MODERN AGE 174-180 (Marc Rotenberg, Julia Horwitz, and Jeramie Scott eds., 2015).
[12] *Id.* at 179.