patientprivacyrights

September 12, 2013

The Honorable Kathleen Sebelius
Secretary
The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Sebelius,

As an advocacy organization committed to ensuring patient privacy, we are very concerned about patients' ability to maintain their privacy and control their personal health information in an increasingly interconnected world. It is clear that we are not alone in our concerns; privacy is now leading the list of major issues troubling the public in the digital age.

Front page stories revealing NSA/Verizon and others spying on phone records and other personal data has created a major shift in public opinion; people do not want the government or corporations collecting and using their personal data. The reality is that millions of Americans are online sharing personal information, but are unaware of how corporations and government are using that data. However, contrary to the constant cries that "privacy is dead," the aftermath of the NSA leaks shows that Americans care deeply about protecting their personal information.[i] As a result, the public is becoming more vocal with their desire to have more transparency, awareness, and control over private information.[ii]

Research confirms that people want their most sensitive data kept private; they want all information about their minds, bodies, and families' DNA to be confidential.[iii] Yet, the nation's health data is routinely collected, sold, and used without patients' knowledge or consent. The first version of theDataMap™, which documents where people's personal data flows, reveals and details state-by-state sales of hospital data. Research also shows that prescription records from over 50,000 U.S. pharmacies in the United States are regularly sold to pharmaceutical manufacturers.[iv] Despite industry claims that personally identifiable information (PII) is safely de-identified before disclosure or sale, it is well known that re-identification is not just possible, but fairly uncomplicated as well.[v]

HHS Needs to Provide Privacy Guidance to Health Providers

As health care reforms are rolled out, privacy concerns will only increase. HHS should act now to provide guidance to health providers about existing requirements under HIPAA, as well as steps those providers should take to protect patient data. What is most troubling is that citizens cannot track the hidden flows of health data; they cannot find out where, why, and by whom their information is used.[vi] Further, the surge in the number of health data breaches affects trust in institutions holding data. Recent cases, such as Phoenix Cardiac Surgery's and Oregon Health & Science University's inappropriate use of cloud services,[vii,viii] demonstrate that data holders are still having difficulties initiating and maintaining effective data security protections. More guidance, oversight, and audits are vital. Additionally, ensuring patients can control or limit collection of health information should be a top priority in the digital era. Currently, institutions

control patient data. However, the lack of individual control over personal data harms over 10 million patients every year; people often forgo or delay diagnosis or treatment, or hide information from health professionals due to privacy concerns.[ix]

Patient Privacy Rights recognizes that there are many valid reasons for the use of citizens' personal health data. Its use for research and innovation holds great potential to improve health, treatment, quality of care, efficiency, and reduce costs. Realizing these benefits is not at odds with protecting patient privacy. In fact, "privacy" does not mean zero access, it means patients should control how, when where, why, and by whom their protected health information (PHI) is used.[x] Patients and health providers look to HHS to act to protect data and HHS will help advance patient privacy by providing guidance to providers.

HHS Should Build Strong Privacy Protections into HIEs at the Outset

Presently, the nation is spending $563 million to build health information exchanges (HIEs) in every state. This project presents an unprecedented opportunity to build systems with strong privacy protections, which will allow the public to be aware and in charge of data uses and disclosures of their sensitive information. In addition to protecting patients' privacy, this will prevent the U.S. from losing billions of dollars in business revenue due to lack of privacy.[xi] The following recommendations offer increased privacy protections for all patients:

- 1% of HIE funds should go towards building the option of an "HIE of One." At a minimum, patient-controlled data exchange and segmentation should be an option in every state; every American should be able to exchange his/her own data and selectively disclose only relevant PHI to trusted health professionals. This option is known as an "HIE of One" and allows all data flows to be directed by and visible to the patient without restriction or delay.
- State and private HIEs should permit patients' advocates and agents to use and disclose PHI on their behalf. Meaningful Use (MU) mandates the Direct Project, which enables secure email point-to-point and View/Download/Transmit (VDT) as key building blocks for the "HIE of One." Blue Button Plus (BB+) for VDT should be the preferred method of data exchange in the U.S. and required for every federally subsidized HIE.
- HHS should mandate patient and physician portals and voluntary patient enrollment for Record Locator Services (RLS). In doing so, every state can easily and inexpensively offer an "HIE of One."
- Patients should be able to segment data for privacy, research, and any other disclosures. This will prevent future "NSA-like" situations where the government and healthcare industries engage in hidden exchange, collection and surveillance of patients' entire health data records.[xii] Government-sanctioned use of unethical blanket advance consents, such as the use of "no consent," "opt-in," or "opt-out" consent for state HIEs, must also be quickly phased out.
- A complete health data map is needed to allow us to see and understand data flows across the nation and throughout the world. As it is now, Americans have no "chain of custody" for personal health data. People cannot weigh the benefits and risks of using electronic systems unless they know where their health data travels and for what purposes it is used. Federal funds should be allocated to build and maintain a complete health data map to track the hidden flows of health data.

It is not too late to ensure meaningful and comprehensive data privacy protections as the United States implements a nationwide system of electronic records and data exchanges. Restoring

patient control over use of PHI is critical to restoring trust in government, physicians, health technology, and the healthcare system. It is also critical for making real progress on The Triple Aim. HHS can help implement strong privacy-protective measures by:

- Putting 1% of HIE funds towards “HIE of One”;
- Requiring patient and physician portals;
- Ensuring patients can segment data for privacy, research, and other disclosures via voluntary patient use of email addresses for ID and for Record Locator Services; and
- Providing funds to build and maintain a complete health data map.

The public is now paying close attention to what’s happening with their personal information and speaking up about their rights to control PHI. HHS is at a critical junction; it has the opportunity to demonstrate to patients and the public that it hears them. HHS can help alleviate the public’s fear of intrusive government and corporate surveillance by meaningfully engaging them and building trustworthy health IT systems and data exchanges that put patients in control of PHI.

Sincerely,

Deborah C. Peel, MD
Founder & Chair, Patient Privacy Rights

cc: The Honorable Tom Harkin, Chair
U.S. Senate Committee on Health, Education, Labor, and Pensions

The Honorable Lamar Alexander, Ranking Member
U.S. Senate Committee on Health, Education, Labor, and Pensions

The Honorable Rand Paul
U.S. Senate Committee on Health, Education, Labor, and Pensions

The Honorable Patrick Leahy, Chair
U.S. Senate Committee on the Judiciary

The Honorable Al Franken, Chair
U.S. Senate Committee on the Judiciary, Subcommittee on Privacy Technology and the Law

The Honorable Jeff Flake, Ranking Member
U.S. Senate Committee on the Judiciary, Subcommittee on Privacy Technology and the Law

The Honorable Chuck Schumer
U.S. Senate Committee on the Judiciary, Subcommittee on Privacy Technology and the Law

The Honorable Ed Markey
U.S. Senate Committee on Commerce, Science, and Transportation

The Honorable Joe Pitts, Chair
U.S. House of Representatives Energy and Commerce Committee, Subcommittee on Health

The Honorable Frank Pallone, Ranking Member
U.S. House of Representatives Energy and Commerce Committee, Subcommittee on Health

The Honorable Joe Barton, Co-Chair
House Privacy Caucus

The Honorable Zoe Lofgren
U.S. House of Representatives Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet

The Honorable Jason Chaffetz
U.S. House of Representatives Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet

The Honorable Lloyd Doggett
U.S. House of Representatives Ways and Means Committee

The Honorable Ron Kind
U.S. House of Representatives Ways and Means Committee

Endnotes

[i] A recent poll conducted by the Washington Post and ABC News found that 74 % of Americans surveyed felt the NSA's surveillance of phone records and online activity intrudes on Americans' privacy rights. "NSA, privacy and Edward Snowden." *The Washington Post*, July 24, 2013. Accessed September 3, 2013. http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/07/24/National-Politics/Polling/release_254.xml

[ii] Alan Westin, " What Two Decades of Surveys Tell Us About Privacy and HIT Today" (keynote presented at the 2011 Health Privacy Summit, Washington, DC, June 13, 2011). Accessed September 2, 2013. http://patientprivacyrights.org/wp-content/uploads/2011/06/AFW-SUMMIT-6-13-11.pdf

[iii] Westin, "What Two Decades of Surveys Tell Us"; Deborah C. Peel, *The Case for Informed Consent*. Discussion Paper. Accessed September 3, 2013. http://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf

[iv] Robert Steinbrook, "For Sale: Physicians' Prescribing Data," *New England Journal of Medicine* 354 (2006): 2745-2747.

[v] Jordan Robertson, "Your Medical Records Are for Sale." *Bloomberg Businessweek*, August 8, 2013. Accessed September 3, 2013. http://www.businessweek.com/articles/2013-08-08/your-medical-records-are-for-sale; Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" (paper presented at the 2008 IEEE Symposium on Security and Privacy, Oakland, CA, May 18—22, 2008). Published in *Security and Privacy* (2008): 111-125, accessed September 3, 2013, doi: 10.1109/SP.2008.33

[vi] McKinsey Global Institute estimates that medical clinical information providers "could compete in a market worth more than $10 billion by 2020. McKinsey Global Institute. "Big data: The next frontier for innovation, competition, and productivity." Accessed September 3, 2013. http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

[vii] U.S. Department of Health and Human Services. "HHS settles case with Phoenix Cardiac Surgery for lack fo HIPAA safeguards." Last Revised April 17, 2012. http://www.hhs.gov/news/press/2012pres/04/20120417a.html

[viii] Erin McCann, "Fourth big HIPAA breach for OHSU." *Healthcare IT News*. July 29, 2013. Accessed September 3, 2013. http://www.healthcareitnews.com/news/fourth-big-hipaa-breach-ohsu

[ix] Several studies point to this conclusion. See 65 Fed. Reg. at 82,777; California HealthCare Foundation, National Consumer Health Privacy Survey 2005, http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005; and Terri Tanielian and Lisa H. Jaycox, eds. *Invisible Wounds of War,* The RAND Corporation, *http*://www.rand.org/pubs/monographs/2008/RAND_MG720 .

[x] This idea is based on NCVHS's definition of health information privacy, which defines it as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." National Committee on Vital and Health Statistics. "Privacy and Confidentiality in the Nationwide Health Information Network." *Recommendations on Privacy and Confidentiality* (2006—2008): 3-21. Accessed September 3, 2013. http://www.ncvhs.hhs.gov/privacyreport0608.pdf

[xi] Recent studies project a loss of $35B-$180B in US business revenue as cloud services move to nations that prevent government access to data. The loss of billions of dollars in revenue makes a strong business case for comprehensive data privacy protections.[xi] See: Sydney Brownstone, "People Are Changing Their Internet Habits Now That They Know the NSA is Watching." *Co.Exist*. August 16, 2013. Accessed September 3, 2013. http://www.fastcoexist.com/3015860/people-are-changing-their-internet-habits-now-that-they-know-the-nsa-is-watching

[xii] Patients who want to segment data can have multiple personas using voluntary email addresses, in the same way they can have multiple credit card accounts and email addresses that allow them to use different IDs in different settings. Email addresses are used to create Record Locator Services (RLS). Email addresses are used to create Record Locator Services (RLS). Using voluntary email addresses as patient IDs in an elegant, inexpensive, and highly effective solution. Potentially a federal agency could manage trusted identities for the public to use for healthcare.
One example of a trusted federal agency working on this issue is the USPS. The FCCX will streamline relationships between participating trusted identity providers and agencies by brokering externally issued digital credentials to grant people access to certain federal websites and services. See: http://nstic.blogs.govdelivery.com/

"FCCX's value also lies in demonstrating that significant privacy risks can be managed through a combination of technical design and policy. The USPS RFP requires "[t]he FCCX service shall support the privacy requirements of anonymity, unlinkability and unobservability." The vendor must employ a proven, "double blind" architecture – a novel approach that will prevent tracking of credential use among identity providers and relying parties. In simple terms, this means that private organizations that issue citizens credentials – and the agencies that accept them – will have no way to track where citizens use them." See update on progress at: http://fcw.com/articles/2013/08/21/postal-cloud.aspx?s=fcwdaily_210813