patientprivacyrights

February 15, 2011

Patient Privacy Rights Testimony for the HIT Policy Committee & HIT Standards Committee PCAST Workgroup

Patient Privacy Rights (PPR) is the leading voice for patients and consumer organizations for privacy and health IT. PPR's 12,000 members in all 50 states and the 10.3 million members of the organizations in the diverse, multi-partisan Coalition for Patient Privacy are united in our efforts to prevent discrimination in employment and other key opportunities based on health information. Patients will only trust the healthcare system if privacy and the right of consent are assured.

We appreciate the opportunity to comment on "Realizing The Full Potential Of Health Information Technology To Improve Healthcare For Americans: The Path Forward", the Report to the President from PCAST, December 2010.

I. Patient Privacy Rights applauds the sophisticated focus on security, privacy, and patient consent as essential underpinnings of an electronic health record system:

We believe that Section V (Privacy and Security Considerations) provides an encouraging discussion of the absolute need for system design to ensure that patient health records are stored in a way that is secure and private. This follows the NCVHS definition that "health information privacy is defined as an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data" [1]. We are also happy to see a focus on patient consent in the report.

The report asserts as a desideratum, "A health IT infrastructure needs to provide significantly better security than traditional paper records in all respects". We would add that a health IT infrastructure should also provide significantly better protection for privacy than traditional paper records in all respects. The report also states "A solution to this perceived privacy problem must underpin any overhaul of the medical-data ecosystem." We agree with this sentiment as well.

As a technical matter, broadly speaking we concur that the outlined meta-tag architecture could be used to provide the foundation for building a secure, private, and consent-based electronic health infrastructure. We found the scenarios discussed on

---

[1] NCVHS June 2006, Report to HHS Sec. Leavitt, on "Privacy and Confidentiality in the Nationwide Health Information Network".

pages 51 and 52 (and elsewhere in the report) to be particularly encouraging, as they sketch this possibility in a concrete way.

II. However, we are concerned about the implementation timelines in light of a lack of specifics about privacy and consent: We resist the rush to implement.

Despite our enthusiasm about the discussion in Section V and the scenarios, we are concerned that the proposed timeline for implementation does not pay adequate attention to protecting patient privacy. Moreover, scenarios notwithstanding, there were numerous references in the Report to secondary uses of PHI without consent for research that made it hard to interpret the Report's intent to ensure privacy. We acknowledge that the scope of this report was primarily technical and aimed at a level below system design where privacy principles must be applied. Nonetheless, we felt that certain technical issues did not receive adequate treatment:

- **Designing large, complex health data base systems and exchanges that capture and express patient privacy directives is a remarkably difficult engineering problem.**

Design of secure systems is a substantial engineering challenge[2]. The recent Wikileaks fiasco indicates the dangers in having centralized databases that support poorly designed access models and arbitrary queries. Ensuring that a health infrastructure accomplishes the goal of providing better privacy and security than paper records will be challenging, but we believe that attention to such issues must come first on any implementation timetable. As Ross Anderson wrote,

> "Creating large data bases of sensitive personal information is intrinsically hazardous. It increases the motive for abuse, and the opportunity for abuse, at the same time. And even if the controls work perfectly to prevent unlawful abuse (whether by outsiders or insiders) the existence of such databases can lead to lawful abuse---powerful interests in society lobby for, and achieve, access to data on a scale and of a kind that sensible people would not permit."

- **De-identification[3] is much harder than the Report indicates and also requires extensive work[4].** It is well known that PHI is nearly impossible to de-

---

[2] "*Security Engineering, A Guide to Building Dependable Distributed Systems, Second Edition*", 2008, by Ross J. Anderson. Publisher: Wiley Publishing, Inc.

[3] "*Broken promises of Privacy: Responding to the Surprising Failure of Anonymization*", by Paul Ohm. VER. 0.99 SSRN: 8/14/2009: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006&rec=1&srcabs=1446862

[4] "Weaving Technology and Policy Together to Maintain Confidentiality" by Latanya Sweeney, Journal of Law, Medicine, and Ethics, 25 (1997): 98-110

identify[5], and supposedly anonymous aggregated health data can easily be re-identified[6]. There is an emerging consensus (in light of the celebrated attacks on the "anonymized" Netflix database, for instance) that in general de-identifying large databases of personal information is a surprisingly challenging problem. The Report did not, in our opinion, adequately address this matter. We do not believe that any timetable for system implementation should ignore the development of sensible and safe standards for handling attempts to identify safe and unsafe de-identification scenarios.

III. Beyond technical issues, there is a real absence of a sensible legal and regulatory framework.

There is a great deal of evidence that the public expects to be able to decide who can see and use PHI for research and public health. The Report explicitly acknowledges this, and we have corroborating survey data available at http://patientprivacyrights.org/patient-privacy-poll. But the existing legal frameworks for protecting patient privacy are manifestly inadequate:

- Broad "research" and "public health" loopholes in HIPAA[7] enable widespread data misuse, sale and theft. The health data mining and health IT industries use these loopholes to acquire and sell patient data for uses the government never intended. Selling PHI is a business model for many corporations. See "Evidence of Disclosure" [8] by Patient Privacy Rights. When the stimulus funds run out, we can expect to see more health-related corporations and organizations sell data to pay for the costly health IT systems and data exchanges.

- Federal agencies have failed to develop policies and standards to ensure HIT systems and data exchanges comply with stronger privacy protections in state law and with ethical and professional standards, as HIPAA requires.

---

[5] *"A Little Privacy, Please, Computer scientist Latanya Sweeney helps to save confidentiality with "anonymizing" programs, "deidentifiers" and other clever algorithms. Whether they are enough, however, is another question"* by Chip Walter, Scientific American, July 2007. See: http://www.scientificamerican.com/article.cfm?id=a-little-privacy-please

[6] *"Is Deidentification Sufficient to Protect Health Privacy in Research?"*, by Mark A. Rothstein, The American Journal of Bioethics, 10(9): 3–11, 2010

[7] "The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order to not interfere with such laws [affording a right of consent] and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a 'best practices' standard. Thus, professional standards that are more protective of privacy retain their vitality." 67 Fed. Reg. at 53,212 (August 14, 2002).

[8] See: http://patientprivacyrights.org/media/Evidence_of_Disclosure.pdf

- Enforcement of existing federal and state health privacy statutes is spotty. Typically, enforcement of the older privacy protections in 42 CFR Part 2 and § 7332 is strong, but enforcement of the newer HIPAA and HITECH privacy protections has been weak/nonexistent.

Informed consent is essential, but not sufficient for data use, disclosure, and for secondary uses. We need a supporting framework of strong, sensible, and enforceable laws and regulations to strengthen privacy and to enable patients to hold providers responsible for breaches.

IV. As the Report acknowledges, without protection for patient privacy, electronic health record systems will have adoption problems and cause significant social harms.

Patients do not just say they want privacy; they take quantifiable actions to keep personal data private, even risking their own health to do so. The lack of health privacy has caused serious social harms, which began to be studied over a decade ago.

Accurate and complete information cannot be obtained by force. The California HealthCare Foundation's National Consumer Health Privacy Survey [9] of November, 2005 found that 1/8 of patients or 12.5% of the population avoided their regular doctor, asked doctors to alter diagnoses, pays privately for a test, or avoided a test altogether, prior to current efforts to implement an interoperable national electronic health system. Developing and maintaining trust is essential before patients are willing to even give providers data to capture. Trust, privacy, and security need to be the starting point[10].

Polls and surveys going back over a decade show Americans consistently demand privacy. The 2010 PPR/Zogby Poll shows huge majorities of Americans want to control PHI[10] .

But the most destructive effect of the lack of privacy is the actions patients take to prevent personal health information from being revealed. People will actually avoid treatment, risking suffering and loss of life:

- In 2000, HHS estimated that 586,000 Americans did not seek earlier cancer treatment due to privacy concerns. [11]

---

[9] See CHCF survey at: http://www.chcf.org/topics/view.cfm?itemID=115694

[10] See: http://patientprivacyrights.org/wp-content/uploads/2010/11/Zogby-Result-Illustrations.pdf

[11] 65 Fed. Reg. at 82,779

[12] 65 Fed. Reg. at 82,777

[13] 65 Fed. Reg. at 82,778

[14] See privacy polls at http://patientprivacyrights.org/media-center/polls/

- In 2000, HHS estimated that 2,000,000 Americans did not seek treatment for mental illness due to privacy concerns. [12]

- Millions of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.[13]

If the HHS studies were repeated again, we would likely find even greater avoidance of treatment because Americans' recognition that electronic systems have poor security and privacy protections is growing.[14]

And finally the Rand Corporation found that 150,000 soldiers suffering from Post Traumatic Stress Disorder (PTSD) do not seek treatment because of privacy concerns.[15] The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years.

The Economist held a 10-day online debate and vote in December on the subject of whether the lack of privacy in health IT is a significant harm. The motion debated was whether "any loss of privacy from digitizing health care would be more than compensated for by the welfare gains from increased efficiency". Only 37% voted in favor. 63% opposed the motion and opposed sacrificing privacy for increased efficiency[16.]

V. Conclusions

While we applaud the writers of the PCAST report for their excellent focus on privacy, security, and consent, we strongly resist the timetable for a rapid implementation of the recommendations in the absence of both technical and legal underpinnings for the

---

[15] "Invisible Wounds of War", The RAND Corp., p.436 (2008)

[16] See: http://www.economist.com/debate/debates/overview/189

protection of patient privacy17,18 It is clear that without suitable protections for privacy and suitable means to incorporate patient consent, electronic health record systems will not achieve their goals and will provoke significant backlash and noncompliance. We strongly recommend a slow, deliberate approach to implementation, with the development of the necessary foundations for privacy and consent as a precondition. It is too important to get this right.

Sincerely,

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

Professor Andrew Blumberg
University of Texas at Austin

[17] See: http://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf

[18] *"The Hippocratic Bargain and Health Information Technology"* by Mark A. Rothstein, Journal of Law, Medicine, & Ethics, Spring 2010, Pages 7-13