patientprivacyrights

Written testimony before the HIT Policy Committee

Deborah C. Peel, MD
Founder & Chair

September 18, 2009

My name is Dr. Deborah Peel, Founder and Chair of Patient Privacy Rights. We are the nation's leading health privacy watchdog. Our mission is to ensure the right to control your medical privacy to protect jobs and opportunities.

Patient Privacy Rights has over 10,000 members in all 50 states. We lead the trans-partisan Coalition for Patient Privacy representing over 10 million Americans.

We appreciate and acknowledge the tremendous task you have been assigned. We thank you for your service on this critical committee. Patient Privacy Rights and the Coalition for Patient Privacy stand ready to work with you and assist in any way to ensure both progress and privacy with HIT.

Ensuring privacy (i.e. control of personal information) is the only way to build trusted electronic health systems and the only way to reap the incredible benefits technology can bring to health..

Any discussion of privacy policy has to start with these crucial facts:

1. **Americans care deeply about privacy and controlling their personal information**. A final report just released from the Agency for Healthcare Research and Quality describes the results of twenty focus groups held across the country in order to understand consumers' awareness, beliefs and fears concerning HIT and to learn how consumers may wish to be engaged with HIT[1].

- A majority want to "own" their health data, and to decide what goes into and who has access to their medical records (AHRQ p. 6).
- There was near universal agreement in all focus groups that if medical data are to be stored electronically, health care consumers should have some say in how those data are shared and used. (AHRQ p.29)
- A majority believe their medical data is "no one else's business" and should not be shared without their permission. This belief was expressed not necessarily because they want to prevent some specific use of data but as a matter of principle. (AHRQ p. 18)
- Participants overwhelmingly want to be able to communicate directly with their providers with respect to how their PHI is handled, including with whom it may be shared and for what purposes. Most believe they should automatically be granted the right to correct misinformation (AHRQ p.33)

---

[1] AHRQ Publication No. 09-0081-EF "Final Report: Consumer Engagement in Developing Electronic Health Information Systems" Prepared by: Westat, (July 2009) http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf (last visited September 14, 2009)

- Moreover, another survey found that 13-17% of consumers engage in information hiding in the current system. They will opt-out of and/or block any new system that takes away their control.[2]
- According to a national survey commissioned by the Institute of Medicine last year, only one percent of Americans would allow researchers free and open access to their health information, without permission. The survey further found that over 4/5 of the population oppose having their information used without their permission EVEN IF it is de-identified and the work is supervised by an IRB. However, 87% are supportive of research, so long as they are asked and have control.[3]

2. **The right to privacy is the national consensus.** Americans in every state have enacted laws and required adherence to ethical rights to health privacy for centuries. Please see our attached letter to the Standards Committee dated September 9, 2009 and a primer on the right to health information privacy.

Any industry or government calls for a new, one-size-fits-all national privacy policy are contrary to the longstanding rights and expectations of the citizens of our nation. The only privacy policy to which everyone can agree is for each person to set their own policy. Luckily today's privacy-enhancing technologies can empower each individual to decide his/her own privacy preferences and directives. In fact, in the AHRQ Report they learned there was no support for the establishment of general rules that apply to all health care consumers. Participants thought that health care consumers should be able to exert control over their own health information **individually, rather than collectively**. (AHRQ p. 29)

3. **Privacy—consumer control over PHI—is the easiest, cheapest, and most efficient enabler of health information exchange**. Consumers' right to control PHI by giving or withholding informed consent has the added advantage of complying with every stringent state and federal legal and ethical requirement. Far from being an obstacle to data flow, privacy assures "data liquidity" by eliminating the need for expensive, complex, and cumbersome agreements among stakeholders for HIE.

4. **Patient control ensures the cooperation of all stakeholders.** Patients alone have the clear legal right to electronic copies of their records (through the HIPAA and reinforced by the ARRA).

---

[2] California Health Care Foundation, Consumer Health Privacy Survey, (June 2005) http://www.chcf.org/topics/view.cfm?itemID=115694 (last visited September 14, 2009)

[3] A.F. Westin, How the Public views Privacy and Health Research (2007) http://www.iom.edu/CMS/3740/43729.aspx (last visited September 14, 2009)

Still, the Coalition for Patient Privacy recognizes other key facts:

1. Most HIT systems today do not have patient privacy and control over access to sensitive electronic health information wired in up-front, in accordance with longstanding federal and state policies, laws, and medical ethics.

2. It will take time to build privacy into most electronic health systems.

3. Working together with industry and government to assure meaningful and comprehensive privacy protections in electronic health systems is the way to achieve progress and reap the benefits of HIT.

Today we ask the Committee to set a high bar for privacy that complies with existing law and medical ethics, meets the historic new privacy requirements in ARRA, and just as importantly, meets Americans' expectations. The healthcare and health data mining industries will not willingly build and use privacy-enhancing electronic health records and systems unless you act to set a high bar. Congress set a high bar in the ARRA. Congress recognized that the status quo for privacy will not ensure trust and required HIT systems to add new privacy rights very quickly.

In my practice I meet one-on one with my patients, who are in a vulnerable state, just as all doctors do. Whether it's lying in a paper gown on an operating table, psychotherapy or discussing diet and exercise habits, unless patients trust that doctors and health professionals respect their autonomy and privacy, they will not walk through the door and there will be no data to collect or analyze. In the policy world, it's very easy to forget that medicine is a cottage industry. One person seeks help from another—two people agree to meet.

The health care system isn't even a system; it is a fuzzy, incomplete picture or approximation derived from data amassed from billions of two-person encounters. We do not have a complete or accurate picture of the healthcare system because each patient decides whether an encounter takes place and if personal data will be disclosed. Data and trust cannot be compelled or coerced. HHS' own figures document that 600,000 people avoid early diagnosis and treatment for cancer and 2 million avoid treatment for mental illnesses because they know that their records are not private and they cannot control who sees them[4].

The only legal and ethical way to get a complete and accurate picture of Americans' health and health data is to ask for permission to use the data up front; to obtain informed consent for specific information in records that patients have checked for accuracy, and explain for what purpose, to whom and for how long the information will be used.

---

[4] 65 Fed. Reg. at 82,777 and 65 Fed. Reg. at 82,779

Writing about the recommendation of the IOM to eliminate informed consent in the Mark Rothstein took a similar stance regarding research and stated,

> Clinicians, researchers, and their institutions do not have the moral authority to override the wishes of autonomous agents. Individuals seeking treatment at a medical facility are not expressly or impliedly waiving their right to be informed before their health information and biological specimens are used for research. The recommendation of the IOM Report would automatically convert all patients into research subjects without their knowledge or consent.[5]

This committee is working very hard to devise a path towards EHRs that assure "meaningful use" by capturing data to improve quality and efficacy. These are important goals. The gap we see is the Committee has not spelled out simple, basic privacy policies that ensure patients control their personal information in EHRs certified for "meaningful use".

The key to using personal health information, whether it be for treatment, research, P4P, comparative effectiveness, quality improvement, to lower costs, to prevent duplicate tests and errors or for any other purpose is to first obtain permission from patients.

We are not talking about blanket consents, coerced consents or all-or-nothing policies. We will never have informed consent unless patients know to what they are consenting to and what information is disclosed. Choices must be truly informed to be meaningful. Patients must have access to see and correct their information and have control over where it goes. The good news is HIT systems already exist do these things, proving that privacy works.

Here is a sampling of the recent feedback received from consumers in the AHRQ focus groups. "A very large proportion of participants felt that they should be asked for their consent before their information was stored in an electronic system" (p.36)[6].

- On the consent forms you could have lines and then check boxes.
- I authorize this, this, and this, maybe not this.
- Yeah, something like that, where you've got check boxes that you could check what you would allow to be shared. You could have a consent form, but certain conditions could change, and stuff like that…They would come to you and say, "Beyond this, if this situation occurs while I am with you…?" Then you could opt to expand the information to other people.

---

[5] Mark A. Rothstein, "Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark," *Journal of Law, Medicine & Ethics*, (2009): 507-512.

[6] AHRQ Publication No. 09-0081-EF

- Researchers should not have access to your medical files unless you give consent to something like that…Even if somebody is tapping into my record just for training or something like that, I'd still have a problem. Unless they asked you "if you agree or not agree" to have that done. And if I say "yeah, go ahead and do it."
- I think that there should be a list of every single entity that could possibly access your medical records. And then you would check off the ones you would allow.

We believe, as we think you do, that technology offers the solutions to ensure privacy and progress. Technology is not an impediment. In fact, technology can offer exquisite privacy empowering patients to segment their information and exercise the control they desire as described above. We provide a few examples of privacy-enhancing technologies and systems:

NDIIC Consent Management
Behavioral treatment centers that are members of the National Data Information Infrastructure Consortium (NDIIC) have been using an open source EHR with granular, electronic, informed consent over the past 9 years. These EHRs are used in 8 states and counties covering 22 jurisdictions. Additional states are implementing NDIIC systems. Large and small provider organizations across large and small states and counties have generated over 4 million clinical records. All of these records are only disclosed in accordance with the patient's informed consent via an electronic form that is easy to complete and sensitive to time constraints. The "point and click" format allows the patient to make very specific determinations about what, if any, information is to be released to whom, for what purpose, and how long.

HIPAAT Consent Management & Auditing Solutions
Allows patients to create very simple **or** detailed consent directives based on any or all of the following: Consent type, purpose of use, who may or may not access PHI, PHI granularity – all PHI, PHI within a given time period, PHI related to a specific medical condition, specific PHI types (e.g. prescription history).

Health Record Banks
Washington State, Oregon, Louisville (KY), Kansas City (MO), and Ocala (FL) are currently building Health Record Banks. Each health record bank (HRB) is a community or state-based health data repository containing copies of complete health records that are controlled by patients. Whenever a patient receives care, the new information generated is deposited in his/her health record bank account. Non-profit community organizations provide governance and may collaborate or contract with for-profits to develop and operate the HRB. In the Health Record Bank model, the patient owns the data and controls where it goes and how it is used.

Health record banks are one solution to the challenge of storing and enabling the exchange of data inexpensively while fully protecting privacy via patient control. The

distributed system or networked approach to HIE is too complex, too expensive and cannot easily protect privacy or even assure security.

Require privacy--Patients will trust it. Require privacy--Vendors will build it. Require privacy--Physicians will buy it.

In addition, in order for the Committee to assure patient engagement, choice, and trust we recommend the following broad policies:

1) No protected health information should be "exchanged" without the informed consent of the patient.

2) The patient has a right to designate a place where their provider must send a copy of their electronic medical information shortly after each encounter at no charge;

3) All access to patient records via HIEs must be with the explicit permission of the patient, and must include the ability of the patient to selectively prevent the release of specific information to specific providers at specific times.

We also recommend that the HIT Policy Committee become informed about privacy-enhancing technologies by

1) Inviting a panel of vendors and organizations that build, use, and develop privacy-enhancing products and HIT systems to advise the committee and its work groups. We have provided the Committee a short list of suggested invitees doing innovative work on privacy. Both open source and proprietary solutions being used today permit segmentation at a granular level, easy to read audit trails, easy to understand privacy "profiles" so consumers have models of how to set their own defaults or profiles, and other consent management solutions.
2) Use these privacy-innovative vendors, patient privacy advocacy groups, legal experts who have defended consumers' rights to health privacy, and representatives from other groups like the State Health Insurance Counseling and Assistance Programs[7] to offer ongoing expertise to the Committee and its work groups.
3) Use privacy experts to help the Committee develop a timeline that ensures patient choice and control over protected health information are added to requirements for EHRs in the next 24 months with initial recommendations provided in time to inform 2013 measures for meaningful use.

We also urge you to address specifically all other privacy protections in the HIPAA and the ARRA to ensure that taxpayer dollars are not used to fund EHRs that do not comply

[7] These groups, often referred to as SHIPs or SHIBAs are in every state and highly experienced engaging and assisting individuals with Medicare, as well as those with Medicaid, in addition to private insurance.

with existing law. These important protections have real deadlines – some past, and some that are as early as February 2010. Yet thus far it seems implementation of these critical provisions have been pushed aside to be dealt with far down the road, if at all.

To highlight the privacy requirements the HIT Policy Committee has not addressed yet:

- Patients must be able to keep their information from being shared with a health plan if they pay for the care privately (required by the ARRA). Patients must be able to keep their information from being disclosed without consent if their provider agrees (required by the HIPAA). These requirements mean segmentation and a need to register a patient's choice must be functionally possible in all electronic health systems. The ARRA requires compliance by February, 2010, only five months from now. The HIPAA Privacy Rule allowed providers to agree to use informed consent in accord with patient requests and limit disclosures in 2001.
- Covered entities and business associates must first get a patient's valid authorization before selling PHI. This requires that all disclosures of PHI are tracked via audit trails so that the presence of a valid authorization for data sale can be proven. This provision is effective in 2011.
- For EHRs purchased in 2009 or later, entities must provide an audit trail to patients of all disclosures as early as 2011 and no later than 2013.

The Coalition believes these basic minimum privacy protections are current legal requirements. And, we strongly believe that patients want, expect, and are very capable of expressing their preferences about how their personal information is used and who can use it. Patients are becoming more savvy, not less. Don't underestimate the strong public will to control sensitive health information.

We have attached previous letters signed by the Coalition for Patient Privacy for the record as well. Thank you for this opportunity to be with you today and I look forward to our discussion.

Enclosures:

Letter to HIT Policy Committee dated June 26, 2009
Letter to HIT Policy Committee dated August 3, 2009
Letter to HIT Standards Committee dated September 2, 2009
(All of the above are available at:
http://www.patientprivacyrights.org/site/PageServer?pagename=PrivacyCoalition)
Primer on the Right to Health Information Privacy, Jim Pyles (attached)