patientprivacyrights

Ensuring you control who sees your sensitive health information

December 16, 2013

Jacob Reider, MD, National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Ave. SW.
Suite 729-D
Washington, D.C. 20201

Dear Dr. Reider,

RE: Patient Identification and Matching Initial Findings

We are pleased to offer testimony to the Office of the National Coordinator for Health Information Technology for the December 16, 2103 hearing on Patient Identification and Matching Initial Findings.

Patient Privacy Rights (PPR) is a bipartisan, non-profit organization whose mission is to ensure patients control the collection, use, and disclosure of sensitive personal health information in electronic systems. PPR has over 12,000 members in all 50 states and leads the bipartisan Coalition for Patient Privacy, representing over 10.3 million Americans.

PPR speaks on behalf of the public, encourages thoughtful debate on urgent privacy issues and solutions, and created the annual International Summits on the Future of Health Privacy held at Georgetown Law Center in Washington, DC. To learn more about PPR, visit patientprivacyrights.org.

General Comments About the Initial Findings

The Initial Findings report address the problems caused by current institutional health information technology (health IT) systems and data exchanges. Institutional control over protected health information (PHI) and data exchange will be gradually replaced over the next few years as patients and physicians are able to fully participate in health IT. Fuller patient participation, such as receiving electronic copies of PHI, means innovative technologies will develop to serve patient needs and interests, as well as comply with patients' legal and ethical ' rights to health information privacy. However, the findings address today's problems without anticipating where we will be tomorrow; they did not foresee that the Health Information Technology for Economic and Clinical Health (HITECH) Act and Meaningful Use (MU) requirements can be used to resolve many of today's problems with patient identity and patient matching.

We are at the very beginning of building health IT systems and data exchanges. The

Initial Findings appear to be a way to temporize until patients and physicians are genuinely engaged as full participants in health IT systems and data exchanges. It will take a few years to move from institutional control over healthcare systems to health IT systems with fully engaged and fully participating patients and physicians.

Specific Comments About Problems with the Report of Initial Findings

- ***The report lays out a temporary, shortsighted process to improve patient identity (ID) systems and patient matching.*** The Initial Findings should have acknowledged that the US is at an early phase of health data exchange. We are at the beginning of building strong patient ID systems and there are much better ways to assure data integrity, quality, and provenance than patient matching.

- ***There is no appreciation of better future solutions****,* based on moving from institutional control of PHI to patient-controlled PHI (as required by state and federal law, constitutional law, medical ethics, and international treaties about research use of PHI).

- ***The Initial Findings offer little to improve patient engagement.*** The only recommendations to improve patient engagement are about updating personal demographics. The process of asking patients to update demographics is an annoyance and bothers the many patients who are asked to do this every time they see a physician. The lack of ability to conveniently and efficiently update demographic data is one of the top complaints the public has about HIT systems.

- ***The Initial Findings do not connect to other current health IT policy, standards, and systems developments, or to other efforts to engage patients.*** Patient engagement in identity and monitoring of PHI and data exchange can build on and expand benefits from the use of patient and physician portals, patient-controlled ID, Blue Button Plus (BB+), Direct Secure email, etc.

- ***The Initial Findings missed a tremendous opportunity to create and leverage genuine patient engagement/participation*****.**
    - Patients have more interest and stake in data integrity and patient safety than any other stakeholders. Patients want access to PHI so they can monitor their own data.
    - Patients alone know which "matches" are accurate and *want* accurate data. With an Accounting of Disclosures (AODs) from Health Information Exchanges (HIEs) and Health Information Organizations (HIOs), patients can monitor whether PHI was sent to the right places and identify errors.
    - If patients exchange PHI, they verify their own identities at each place PHI is disclosed and "match" themselves, assuring data quality, integrity, and patient safety while preventing mismatches, spotting if there was medical identity theft, etc.

Before we can understand how the Initial Findings fail to anticipate the future and how the mandated changes required for health IT systems will lead to far better solutions, a basic explanation of the current state of health IT and data exchange patient-matching is necessary.

What Is “Patient Matching” and How Does It Work?

1. Today, U.S. patients cannot control who sees, uses, or sells their most sensitive personal information: health data in electronic systems.

2. Because patients cannot disclose or share their health data between doctors, hospitals, and researchers, institutions like corporations and government agencies must collect, use, disclose, and sell patient data instead.

3. But how can institutions exchange sensitive health data without patient participation or knowledge?

4. The technique used to exchange US health data without involving patients is called "patient matching."

5. "Patient matching" means comparing our personal "attributes" or characteristics such as age, sex, DOB, SS#, demographics, etc. to try and figure out which health data is ours by "matching" or finding the same personal attributes in health records in other locations.

6. "Patient matching" enables institutions, corporations, and government agencies to exchange our health data for many uses, such as treatment, research, paying claims, and healthcare operations. *If* patients had a choice, they would probably agree to some uses and disagree with many others.

7. Electronic health records (EHRs) are accessed 100s-1000s of times every day by both humans and software.

8. "Patient matching" is a method of involuntary, hidden surveillance, much like the NSA's surveillance of phone records and metadata. It enables 1000s of hidden third parties to collect and aggregate our personal health data from many places without our knowledge or consent.

9. See theDataMap.org to track some of the hidden flows of US health data.

Today, the nation's sensitive health records are exchanged by hundreds of hidden users without meaningful informed consent. Health technology systems violate our federal rights to see who used our data and why. Despite the federal right to an Accounting of Disclosures (AODs)—the lists of who accessed our health data and why—technology systems violate this right to accountability and transparency.

PPR's Vision of the Future

Meaningful patient engagement will enable patients to fully participate in their healthcare and in electronic systems. Meaningful engagement will ensure they can access, control or delegate use and disclosure of PHI, and monitor all health data exchange automatically in real time.

Meaningful patient engagement can be leveraged to eliminate most of the difficult, complex problems caused by current patient identity systems, and by patient matching technologies and algorithms. Genuine patient engagement presents us with an opportunity to resolve the difficult problems caused by current patient identity systems and matching problems as enumerated in the Initial Findings.

How meaningful patient engagement can provide better, simpler, cheaper solutions:

- First: only patients have clear, uncontested rights to see/access, control, and move PHI. Institutional data transfers are technically very complex and legally require Data Use and Reciprocal Support Agreements (DURSAs) and contracts for exchange, which disengage patients from health IT and healthcare. Further, institutional systems for data exchange and the resultant problems caused by patient matching are far too expensive and complex for small practices and clinics to deal with. As a result, current institutional systems disenfranchise a large population of physicians and other licensed health professionals.

  - Patients should be able to send their data to whomever they wish for treatment, research, etc.; they should be able to share PHI with large institutions and small practices. Further, when patients mediate exchange of their own data, in effect, they verify their own identities at every exchange/disclosure.

  - When we have patient-control over IDs and data exchange, the serious, complex institutional problems caused by difficulties verifying patient identity, standardizing data attributes, capturing data attributes, and patient matching can be solved.

  - Without the expensive legal and contractual processes and burdens of institutions, and without the need for expensive, complex technologies and processes to verify identity, patients can move PHI easily, more cheaply, and faster than institutions. Additionally, they can move it to small practices. Patients can send PHI to the right people and places at the right time using Direct Secure email, ensuring interoperability, data provenance and integrity, data quality, and patient safety, no matter the size of the provider.

- Second: patients (or their legal delegates) are far more likely to recognize errors in their own PHI and demographic data. They are also far more likely to recognize harms and errors caused by institutional data exchange, including mismatches, data errors and omissions, and data disclosed to the wrong people/institutions. Patients know who they are and where they were treated. They are far more motivated to make sure that demographic attributes and PHI held by institutions and data aggregators are genuine and correct. Patients know and can easily correct their own demographics and errors in PHI. Their health and lives are at stake.

<u>Key Elements for Meaningful Patient Engagement Based on Fair Information Practices and Federal Law</u>

All health data holders and all health data aggregators should operate as HIPAA Covered Entities. In particular, health data aggregators should be treated like CEs, and should be known to patients. To engage patients, health data aggregators should provide Notice of Privacy Practices (NPPs), and real time AODs via patient portals. Hidden surveillance and use of PHI disengages patients and prevents trust in health IT systems. Health data aggregators should be accountable and transparent.

Examples of health data aggregators include but are not limited to:

- Master Patient Indexes (MPIs)
- Record Locator Services (RLSs)
- Health Information Exchanges (HIEs)
- Health Information Organizations (HIOs)
- Prescription Drug Monitoring Programs (PDMPs)
- Heath Insurance exchanges (HIXs such as Healthcare.gov)
- All Payer Claims Databases (APCDs)
- Pharmacies and prescription aggregators
- Clinical laboratories
- X-ray facilities

- Research health data aggregators (such as the Agency for Healthcare Research and Quality's DartNet data base, and private databases like Explorys)
- State and national health registries and health data bases (such as Ambulatory Care and Inpatient Care data bases)
- Commercial data aggregators that collect and use PHI (such as Acxiom, credit bureaus, etc).

Health data holders and aggregators should provide:

- **Notice of Privacy Practices (NPPs)**
- **Patient-controlled IDs that are voluntary, not coerced**
- **Patient and physician portals**
- **Direct Secure email between patients and physicians**
- **Blue Button Plus (BB+), automated view, download, copy**
- **Accounting of Disclosure (AODs), automated, in real time**
- **Right to electronic copies of PHI**

Conclusions

The Initial Findings were intended to assess "current industry capabilities and best practices for patient identification and matching, with a focus on matching across organizations." However, "policies and best practices" should also be based on how future health IT systems and data exchanges will operate. Additionally, they should anticipate meaningful patient and physician engagement, lowering costs, improving data quality, integrity and patient safety.

The U.S. is moving toward far better patient identity systems, where patients can have voluntary cyber-IDs that don't reveal all their attributes, and enable the use of multiple email addresses so sensitive data can be segmented to protect privacy. The National Strategy for Trusted Identities in Cyberspace (NSTIC) and Identity Ecosystem Steering Group (IDESG) processes are also developing much better systems for patient identity. There are also existing commercial patient identity systems; both Verizon and Microsoft offer far stronger systems for patient identity management than are being used in healthcare today.

We urge the Office of the National Coordinator to not focus exclusively on best practices for the current environment. We recommend that the ONC also require, promote, and incentivize the rapid adoption of technologies listed above, as well as technology design based on FIPS, alongside the proposed "best practice" fixes for institutional systems. Patients and physicians must be fully engaged and empowered, not just institutions and vendors.

Sincerely,

Deborah C. Peel, MD
Founder and Chair
Patient Privacy Rights
www.patientprivacyrights.org
Privacy Trust Framework:
http://patientprivacyrights.org/trust-framework/

SSRN Page:http://ssrn.com/abstract=2231667

SAVE THE DATE: 4th International Summit on the Future of Health Privacy: June, 4-5, 2014 in D.C.