patientprivacyrights

The Case for Informed Consent
August 2010

Why it is Critical to Honor What Patients Expect–
for Health Care, Health IT and Privacy.

On July 8th, 2010, ***HHS Secretary Sebelius*** *announced a new* ***"Administration-wide commitment to make sure no one has access to your personal information unless you want them to."***

"A patient-centered health care system would be one where medical records would belong to patients. Clinicians, rather than patients would need to have permission to gain access to them."

Donald M. Berwick, MD
Administrator of the Center for Medicare & Medicaid Services (CMS)

Deborah C. Peel, MD
Founder

Patient Privacy Rights
www.patientprivacyrights.org
P.O. Box 248
Austin, Texas 78746
(512) 732-0033

With the assistance of:

Ashley Katz deJong

With acknowledgement and appreciation for assistance on legal issues to:

James C. Pyles
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, NW
Washington, D.C.

Overview

The Hippocratic Oath states "Whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will keep inviolably secret."
5th Century B.C.

For centuries, patients have come to physicians seeking help. They reveal embarrassing symptoms and share unsettling fears and concerns, because they trust clinicians to keep their information private.

Today, patients still think doctors protect their privacy. In their most vulnerable states, patients trust that health professionals, hospitals, and medical facilities will respect their privacy.

And yet, as we move forward with electronic health records (EHRs), health information exchanges, and innumerable health databases, keeping records private becomes more and more difficult. ***Personal health information is being used and shared in ways patients never imagined.***

A patient shares personal health information in order to receive treatment. However, once these details are shared to receive treatment, that personal information is used in many other ways, passed on and shared with other strangers in companies and government agencies that have no direct relationship with the patient; this is "secondary use" of personal health information.

Patients have not been told about secondary uses of their health information. Patients have not given consent for the secondary uses of their health information. This practice violates patient trust and the right to health privacy.

The monetary value of personal health information is staggering. The health information technology (health IT) industry has estimated annual revenues of $8-9 billion dollars/year. The annual revenue of the stealth health data mining and data sales industry is likely two to ten times more. Examples are not easy to uncover, but the estimate for just one small electronic health record (EHR) company with revenues of $100 million dollars/year from software sales is that it could earn $250 million dollars/year more by selling patient data.[1]

Tremendous good can be achieved using health IT, but we must first face and deal with misuse and harm from the systemic practice of data mining and data theft.

Protecting privacy is not just a moral or ethical necessity, but a practical one. Billions of dollars have been allocated in the American Recovery and Reinvestment Act to establish an EHR for every American. *If patients cannot control personal information stored in EHRs, they will not trust health IT systems or data exchanges and will avoid them.*

[1] C. Anderson, *Free, The Future of a Radical Price*, Hyperion, NY, pg. 104 (2009).

KEY POINTS

A majority of Americans believes their medical data is "no one else's business" and should not be shared without their permission.
AHRQ Publication No. 09-0081-EF

Americans have a right to health information privacy.

If patients cannot control personal information stored in EHRs, they will not trust health IT systems or data exchanges and will avoid them.

Health IT can enable patient control and protect privacy.

Consent technologies can
~lower costs,
~simply the process,
~encourage patient participation.

Patients know what they want.

A black market for totally private treatment will develop for those who can pay to protect themselves and their families from discrimination and reputational harm. If patients refuse to adopt and use EHRs because they cannot control who can see and use the data, it will be a tremendous waste of taxpayer dollars and our investment in health technology.

The powerful healthcare, health IT, and data mining industries are extremely resistant to changing existing primitive, privacy-destructive systems. As a result, patients have been forced to use health IT systems that allow others to decide when to use and disclose their sensitive records. Arguments are made that patient control over data is too technically difficult, too expensive, or too complex to build and require. Often industry executives argue that patients don't know what they want, or that patients simply don't understand health care.

Patient Privacy Rights strongly disagrees. Robust privacy-enhancing technologies are in use <u>now</u> that ensure both progress and privacy. Technology can *lower* costs by enabling individual control over protected health information (PHI) today. Using consent will *simplify* data exchange by eliminating the need for complex and expensive data-sharing agreements between "stakeholders" such as covered entities, business associates, and other secondary and tertiary businesses and corporations. Moreover, patients know what they want and expect their right to health information privacy.

It is a mistake to design health IT in a paternalistic manner -- assuming a corporation, vendor, provider or government agency knows what is best for each individual patient. Instead, we should build 'patient-centric' health IT systems. In the words of Don Berwick, MD, Administrator of the Centers for Medicare and Medicaid Services (CMS), we should build systems that ensure

"medical records belong to patients. Clinicians, rather than patients would need to have permission to gain access to them".[2]

Today, the majority of providers, insurers and major corporations fail to offer even basic electronic consent tools. Policy makers and industry have set the privacy bar too low. Today, health care and health IT industries are not complying with existing state and federal privacy laws or our ethical rights to health information privacy.

We can do much better.

This paper considers the foundation of privacy and medical ethics. Next we outline key findings that demonstrate the public's expectations for medical privacy. We address key arguments against patient control over personal health information. Finally, we conclude by offering technical, process, and policy solutions and recommendations for moving health IT forward with patient control.

Privacy is a long-established individual right. The public clearly expects that this right be recognized and accommodated in standards and policies. Privacy is not a new concept, but the foundation of trust in the physician-patient relationship. The federal government must require industry to build in patient control as an integral part of the foundation of all HIT systems as they are developed.

Patient Privacy Rights
www.patientprivacyrights.org
P.O. Box 248
Austin, TX 78746
(512) 732-0033

Patient Privacy Rights thanks the Rose Foundation for its generous support to help make this body of work possible.

[2] Donald M. Berwick, What 'Patient-Centered' Should Mean: Confessions of An Extremist, Health Affairs 28, no.4 (2009): w555-w565 (published online May 19, 2009

Privacy: An Ancient Tradition, Protected on Many Levels

The right to keep health information private is reflected in the Hippocratic Oath dating from 5th Century B. C. This Oath is still taken by graduates of American medical schools. It is a core ethical principle reflected in the standards of professional ethics of all health professions.[3] Patients expect that what they say in the doctor's office will stay in the doctor's office.

There is a clear national consensus for the right to health information privacy. The consensus developed in state laws, federal law, common and tort law, Constitutional law, and the ethical codes of all the health professions over the course of our nation's history. Federal courts have found consistently that the right to informational privacy, as distinct from the right to decisional privacy, is protected by the Fourth, Fifth and Fourteenth Amendments to the United States Constitution.[4] In fact, the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it.[5]

Ten states have a right to privacy expressly recognized in their state constitutions. A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia.[6] A psychotherapist-patient privilege is recognized in the laws of all 50 states and the District of Columbia and has been recognized by the Supreme Court as a matter of federal common law.[7] The HITECH Act signed into law in February of 2009 expressly recognizes such privileges and provides that nothing in the Act is intended to constitute a waiver.[8] All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information.[9]

Americans Care Deeply About Their Privacy

What exactly does privacy mean? The right to privacy is generally defined as the right of the individual to control who sees their health information.[10] Without the ability to control the use and disclosure of health information, the individual has no right to health information privacy. In other words, privacy means control over personal information. **Without control, we have no privacy**. The National Committee on Vital and Health Statistics defined privacy as "an individual's right to

---

[3] 65 Fed. Reg. at 82,472; The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993, R. Orr, M. D. and N. Pang, M. D.
[4] Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001), ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005)
[5] Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000)
[6] The State of Health Privacy, Health Privacy Project (2000)
[7] Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996)
[8] HITECH Act, section 13421(c).
[9] HHS finding 65 Fed. Reg. at 82,464
[10] HHS finding 65 Fed. Reg. at 82,465; Letter from National Committee on Vital and Health Statistics to HHS Secretary Leavitt, p. 2 (June 22, 2006).

control the acquisition, uses, or disclosures of his or her identifiable health data". [11] As long as health care-related corporations and government agencies control the use and disclosure of our health information, we have no way to keep our information private.

A final report recently released from the federal Agency for Healthcare Research and Quality (AHRQ) describes findings from twenty focus groups held across the country. The focus groups were designed to elicit and understand consumers' awareness, beliefs and fears concerning health IT. Further, AHRQ wanted to learn how consumers may wish to be engaged with health IT[12].

The findings solidly confirm Americans' desire to control their personal health information. Americans are generally supportive of health IT, but they want to be well informed about the consequences of disclosures and have the ability to restrict access and use of their information.

- A majority want to "own" their health data and to decide what goes into and who has access to their medical records.
- There was near universal agreement in all focus groups that if medical data are stored electronically, health care consumers should have some say in how those data are shared and used.
- A majority believes 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.
- Participants overwhelmingly want to be able to communicate directly with their providers with respect to how their PHI (protected health information) 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.

[11] NCVHS June 2006, Report to HHS Sec. Leavitt, on "Privacy and Confidentiality in the Nationwide Health Information Network".
[12] 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)

Americans Will Go "Off the Grid" to Ensure Privacy

The California Healthcare Foundation found that 13-17% of consumers engage in information-hiding in the current system. **One in eight** Americans puts their health at risk *because of privacy concerns*. These individuals take the following actions:

- Avoid seeing their regular doctor,
- Ask their doctor to alter a diagnosis,
- Pay for a test out-of-pocket,
- Avoid tests.[13]

Millions of Americans will opt-out of and/or block new systems that take away their control of sensitive records. A survey by the California Healthcare Foundation in 2010 found that sixty-eight percent of Americans are concerned about the privacy of medical records.[14] Because privacy concerns are not addressed in today's electronic health systems, real harm occurs now. Patients avoid care, suffer needlessly, and die.

- HHS estimated that **586,000** Americans did not seek earlier cancer treatment due to privacy concerns. [1]
- HHS estimated that **2,000,000** Americans did not seek treatment for mental illness due to privacy concerns. [2]
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.[3]
- The Rand Corporation found that **150,000** soldiers suffering from PTSD do not seek treatment because of privacy concerns.[4]
- The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years.

[1] 65 Fed. Reg. at 82,779
[2] 65 Fed. Reg. at 82,777
[3] 65 Fed. Reg. at 82,778
[4] "Invisible Wounds of War", The RAND Corp., p.436 (2008)

[13] California HealthCare Foundation, Consumer Health Privacy Survey, (June 2005) http://www.chcf.org/topics/view.cfm?itemID=115694 (last visited September 14, 2009)
[14] California HealthCare Foundation, National Consumer Survey on HIT, (January, 2010) http://www.chcf.org/topics/view.cfm?itemID=134205 (last visited April 20, 2010)

We Do Not Have a Transparent, Patient-Controlled Health Care System

A key problem in our current system is a false sense of the security and privacy of electronic health systems. In large part this is caused by misinformation about what the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule really says. The HIPAA Privacy Rule as originally written during the Clinton Administration required patient consent before any information could be shared:

2001

> *"....a covered health care provider* ***must obtain the individual's consent,*** *in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*
> ***65 Fed. Reg. 82,462***

During the Bush Administration, the Department of Health and Human Services (HHS) made changes to the HIPPA Privacy Rule that remain in effect today. Most importantly, the right of consent was eliminated. Healthcare-related businesses are no longer required to ask our consent for countless uses of personal health information. Consent is no longer required before health-related corporations or government agencies can use our records for "treatment, payment and healthcare operations."

2002

> *"The* ***consent provisions…are replaced*** *with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*
> ***67 Fed. Reg. 53,183***

Over 4 million "Covered Entities" and millions more "Business Associates" still have broad permission to use all protected health information; neither patient consent nor advance notice are required. The terms 'Covered Entities' and "Business Associates" include providers, employers, government agencies, insurance companies, billing firms, pharmacy benefits managers, pharmaceutical companies, collection agencies, marketing firms and data miners.

It could be argued that most patients provide 'implied' consent or grant explicit permission for their information to be used for treatment and claims payment. But patients are not aware that their health data is used for "healthcare operations" purposes. This data-use category is extremely broad and subject to abuse.

Here is the definition of *healthcare operations* from the Code of Federal Regulations (CFR):

Health Care Operations, 45 CFR 164.506:

(1) Conducting **quality assessment and improvement** activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, **case management and care coordination**, contacting of health care providers and patients with information about **treatment alternatives**; and **related functions** that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, **training of non-health care professionals**, accreditation, certification, licensing, or credentialing activities;

(3) **Underwriting, premium rating, and other activities** relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

(4) Conducting or arranging for **medical review, legal services, and auditing** functions, including **fraud and abuse** detection and compliance programs;

(5) Business planning and development, such as conducting **cost-management** and planning-related analyses related to managing and operating the entity, including **formulary development** and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer service, including the provision of **data analyses** for policy holders, **plan sponsors, or other customers**, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
(iii) Resolution of **internal grievances**;
(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of §164.514, **creating de-identified** health information or a limited data set, and **fundraising** for the benefit of the covered entity.

Patient consent is no longer required before widespread sharing or disclosures of electronic health records. **No matter how embarrassing or intensely personal the contents may be,** our information **can be shared.** Your doctor may wish to protect your information, but once the records leave his/her office, he/she cannot control how the recipient uses your information.

According to Professor Latanya Sweeney, the secondary use of Americans' personal health information in electronic health systems today is "unbounded, widespread,

hidden, and difficult to trace."[15] Without the power to control personal health information, patient trust is difficult, if not impossible, to achieve and maintain. Most patients expect their doctors to do the 'right thing' by keeping their records private. Few patients are aware that as soon as health information leaves a provider's office, the misuse and sale of this very personal information by unknown third parties increases exponentially. Surveys show that individuals have a "common belief" and "strong expectation" that their personal health information will not be disclosed without their consent.[16]

It is gratifying to see that HHS is moving to meet consumers' expectations and to restore the right of informed consent by changing flawed privacy policies. On July 8, 2010, HHS Secretary Sebelius announced an "Administration-wide commitment to make sure no one has access to your personal information unless you want them to." Dr. David Blumenthal, the National Coordinator for Health Information Technology, joined her at the press conference to state that "we want to make sure it is possible for patients to have maximal control over PHI (protected health information)."[17]

Our position is that privacy is a long-established individual right. The public clearly expects healthcare providers, the health care system, and health technology vendors to recognize and accommodate this right in standards and policies. Privacy is not a new concept, but the foundation of trust in the physician-patient relationship. The federal government must require industry to build in patient control as an integral part of the foundation of all HIT systems as they are developed.

De-identification and Data Anonymization are not Enough

Some argue that de-identification or stripping names (anonymization) from data ensures that PHI cannot be re-identified; and therefore, data can safely be used for a myriad of purposes with no need to inform patients or obtain their permission. Industry claims that de-identified or anonymized data cannot be re-identified are unproven; no external audits or proof that de-identification or anonymization actually work are required or offered. There is no requirement to release the algorithms/methods used to enable experts to verify the methods of de-identification or anonymization.

Furthermore, techniques to re-identify data are improving daily. They are used commercially and for government surveillance (Fusion Centers). The reason these techniques are used is personal health information is far more valuable than other kinds of personal information. Professor Latanya Sweeney of Carnegie Mellon and Harvard, has proven that 87% of the population can be re-identified with just

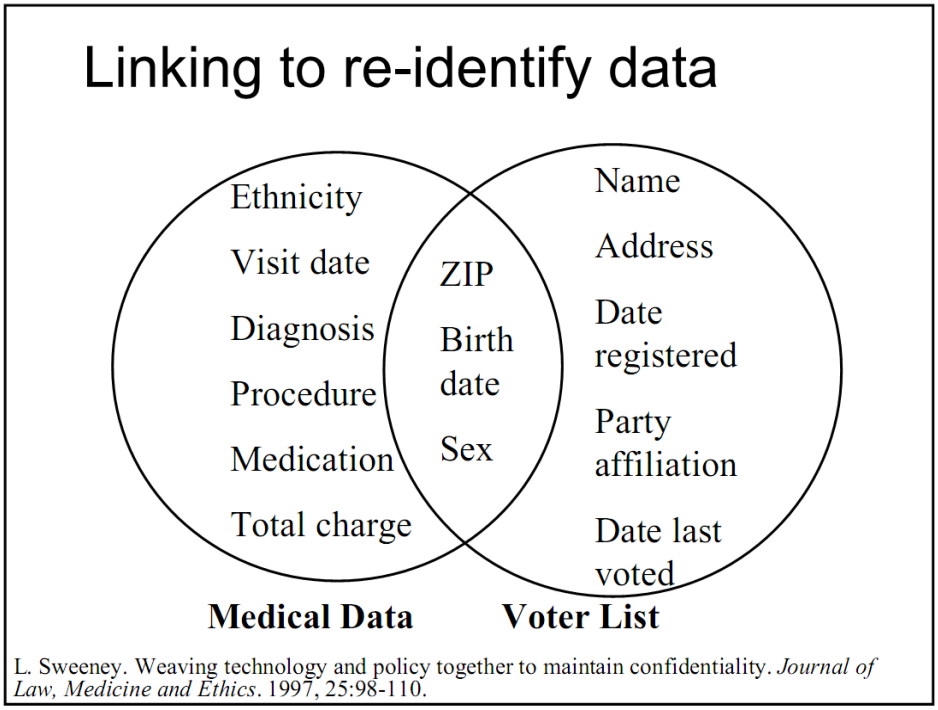
---

[15] "Designing a Trustworthy Nationwide Health Information Network (NHIN) Promises Americans Privacy and Utility, Rather than Falsely Choosing Between Privacy or Utility", Testimony of Latanya Sweeney, PhD before the 21st Century Healthcare Caucus Roundtable April 22, 2010, see: http://patientprivacyrights.org/wp-content/uploads/2010/04/Sweeney-CongressTestimony-4-22-10.pdf

[16] HHS finding 65 Fed. Reg. at 82,472-473.

[17] http://www.hhs.gov/news/imagelibrary/video/2010-07-08_press.html

gender, month or year of birth and zip code. **Data is either useful or anonymous, but never both**.[18] Data may seem to be anonymous but when electronically cross-matched with other sets of public or proprietary data, the merged data sets can reveal identity.



L. Sweeney. Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine and Ethics*. 1997, 25:98-110.

All Personal or Protected Health Information (PHI) is "Sensitive".

This issue of what health data is "sensitive" and whether patients can protect what they consider to be sensitive data from use and disclosure is much broader than an individual's desire to keep his/her sexual history, use of anti-depressants, or genetic test results private. In today's digital information age, the health data mining industry knits together rich, comprehensive profiles of every individual's health status. These profiles include data from traditional sources like health records systems, along with non-traditional sources including data from reward cards and grocery and pharmacy purchase cards. Health data miners use online searches, social networks, and public and private websites to continuously flesh out and update profiles of personal health data. They acquire or buy information from the many corporations that obtain our records without consent. These profiles are treasure troves of sensitive personal information that can be used for many harmful purposes, for health financial scores, to harm reputations, and for job and credit discrimination.

[18] Paul, Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" VER. 0.99 SSRN: 8/14/2009

Truly, PHI is no longer "safe" or "protected" anywhere. The techniques for collecting, aggregating, and matching PHI from disparate sources are very sophisticated. Most Americans have no idea how much personal health information is collected about them online and from the healthcare system. For example, even "normal" blood test results collected as "baseline information" are critical information; they can be used in the future as proof health status has changed.

Americans Do Not Support Giving Researchers a 'Free Pass'

According to a national survey commissioned by the Institute of Medicine (IOM) in 2008, **only one percent** of Americans would allow researchers free and open access to their health information without permission. The survey found that over 4/5 of the population opposes having their information used without their permission EVEN IF it is de-identified and the research was approved by an Institutional Review Board. However, eighty-seven percent are supportive of research, as long as they are asked and have control.[19]

Despite Americans' overwhelming rejection of open access to the nation's electronic health records, most of the health care industry and the IOM propose eliminating informed consent for research using electronic health records. Writing about the IOM's recommendation, Mark Rothstein remarked:

> "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".[20]

There is No Longer a Need for a One-Size-Fits-All Privacy Policy

Industry and government calls to create a new, one-size-fits-all national privacy policy are contrary to the longstanding rights and expectations of the nation's citizens. The only privacy policy that everyone can agree with is that each person should be able to set his/her own policies.

In fact, AHRQ's Report found no support for the establishment of general rules that apply to all health care consumers. Citizen participants thought that they, as health care consumers, should be able to exert control over their personal health information **individually, rather than collectively**.[21] A very large proportion of

---

[19] 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)
[20] Mark A. Rothstein, "Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark," *Journal of Law, Medicine & Ethics*, (2009): 507-512.
[21] AHRQ, p. 29

participants felt that they should be asked for their consent before their information was stored in an electronic system"[22].

AHRQ Sample of Feedback

- On the consent forms you could have lines and then check boxes.
- I authorize this, this, and this, maybe not this.
- You could have a consent form, but certain conditions could change…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.
- Researchers should not have access to your medical files unless you give consent. Even if somebody is tapping into my record just for training, 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.

Health CARE Should Focus on Patient Needs

Don Berwick, MD, also wrote eloquently about the importance of keeping patients at the center of their own health care and health information. In a 2009 Health Affairs article, he argued that an ideal practice is one whose patients would say "They give me exactly the help **I need and want** exactly when **I need and want it**." [emphasis added].[23]

In the debate over health IT and its potential benefits, those who seek health care are rarely at the table. What patients want from electronic health systems ranks dead last. Industry, government, providers, insurers, third parties and technology vendors get what *they* want and need first, before patients. We would be wise to heed Dr. Berwick's call:

> "I suggest that we should without equivocation make patient-centeredness a primary quality dimension all its own, even when it does not contribute to the technical safety and effectiveness of care." [emphasis added][24]

[22] AHRQ Publication No. 09-0081-EF
[23] Berwick, w558
[24] Ibid, w559

Dr. Berwick's definition of "patient-centered care" is:

> *The experience (to the extent the informed, individual patient desires it) of* ***transparency, individualization, recognition, respect, dignity and choice*** *in all matters, without exception, related to one's person, circumstances and relationships in health care.*

Dr. Berwick's definition reflects exactly what Americans want. **Health IT must enable patient autonomy and choice if it is to be successful.** The primary goal of policy makers, regulators, health IT vendors and other stake holders should be to honor patient consent decisions and to build health IT systems that enable patients' directives to control data use and disclosure, unless otherwise required by law. Privacy protections must be comprehensive and meaningful to ensure trust and protect personal health information throughout the healthcare system and online throughout cyberspace.

Arguments Against Consent

Some argue that relying on patient consent will result in patients signing the same kind of blanket, advance, coerced 'consents' that have long been used to grant broad access to paper medical records. We agree that blanket "consents" are both harmful and illegal, because it is impossible to give informed consent to disclose information that will be created in the future.

Blanket Consents

There are two key ways to prevent blanket, advance consents from being used. First, enforce existing laws. Enforce the HIPAA requirement that anyone, including insurers, ask only for the 'minimum necessary' information needed for a specific purpose. For example, a patient should not be asked to disclose his/her entire record of a consultation visit or disclose his/her full chart to an insurer for claims to be paid. Insurers do not need entire records to pay claims. Those who seek access to PHI should obtain meaningful informed consent from the patient. Informed consents should be direct "one-to-one" consents, with a specific purpose and time frame. Those who are granted access should be clearly named or described.

Second, require the use of existing and newly developed technologies that enhance privacy and consent. In the future, all consents will be electronic. Consent tools can offer simple check boxes and systems that empower patients to 'slice and dice' exactly what data they share with whom. **Electronic consent technologies make it remarkably easier and far cheaper to do the following:**

- Contact individuals in real time for consent, eliminating the need for advance, blanket consents;
- Change and update preferences instantly online;
- Segment sensitive information (i.e., keep separate from routine information);
- Set broad directives for some uses and be contacted for any exceptions; and
- Automatically grant permission to access or receive updates to trusted doctors or others;
- Eliminate the use of Institutional Review Boards (IRBs) and Privacy Boards for granting access to thousands of patients' electronic medical records for research. Patients can be automatically contacted by cell phone or email easily and cheaply.

The use of privacy-enhancing technologies will eliminate the need for broad, blanket consents. **Fortunately, decision makers can now require "patient-centric" health systems to be built using innovative consent technologies.** We can use advanced technologies to protect our privacy rights and meet patients' needs. Health IT that protects privacy will assure public trust.

Recently at the Consumer Choices Technology Hearing in Washington, DC, seven privacy-enhancing technologies were demonstrated and discussed. The hearing is now available on video and the testimony of the technology developers and users is available online.[25] Because the technology is available today, policy makers can require providers and health data exchanges to use modern electronic consent tools; these systems will improve patient engagement and trust, and enable providers to easily comply with existing laws and medical ethics. For example, providers could be prohibited from receiving Federal Medicare or Medicaid payments or any stimulus dollars if they do not use effective, robust electronic consent systems. Providers should be required to use systems that ensure patients control personal health information.

Relying on Consent is Too Burdensome for Patients

Some argue that patients are not capable of making informed decisions about the use of their health records and will feel burdened by having to give consent. But obtaining patient consent was the standard of practice in the United States before 2002 when the right of consent was eliminated by the Bush Administration.[26] Since then, state and federal government and industry have added more policies and standards that limit patients' rights to control the use and disclosure of PHI.

Yet these policies have never been publicly debated. The status quo, where PHI is used freely without patient knowledge or consent, shocks and angers average Americans. Government and the health care industry should not assume that

[25] Privacy and Security Tiger Team: Past Meetings, June 29, 2010, Consumer Choices Technology Hearing. See testimony at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910 See the video at: http://nmr.rampard.com/hit/20100629/default.html

[26] HHS finding 65 Fed. Reg. at 82,474.

patients cannot understand or manage their electronic health information. Further, deciding that patients do not deserve the autonomy to choose who can see and use their PHI violates the right to privacy and our fundamental national principles.

Quality health care can only take place in trusted relationships. Providers, covered entities, and business associates that want access to PHI should build direct relationships with patients if they wish to use sensitive records. They should make time for education and have conversations with patients about the real risks and benefits of disclosing health information.

Dr. Berwick recommends that providers and researchers take on the "burden of giving real meaning to the phrase 'a fully informed patient' including a "mature dialogue."" If over time patients make unwise decisions, he recommends that "we should seek to improve our messages, instructions, educational processes and dialogue to understand and seek to remedy the mismatch."[27] We have the right to health privacy and expect all individuals, organizations, government officials, or corporations seeking access to our personal information to ask before using our PHI. ***If you cannot explain in a clear, understandable manner why you need or want my health information, you cannot use or have it.***

Solutions & Recommendations

The only legal, ethical, and practical way to get a complete and accurate picture of Americans' health and health data is to require those who want to use health data to ask permission first. Asking first is the only way to create trusted electronic systems. Paradoxically, patients will be willing to collect and share far more information with health professionals, knowing they control who can see and use it. Trusted systems based on informed consent will create the richest, most complete, and most accurate data for research. The better the data, the greater the potential benefits---both societal and personal---that we can reap from health IT.

If we substitute 'consent' decisions made by IRBs and Privacy Boards, whose interests often conflict with patients' rights and expectations, for patient consent, the result will be less data and less reliable data. Alternatively, using information from records that fully-informed patients have checked for accuracy will improve the accuracy of research. Trusted researchers will obtain richer, more accurate, and more complete data. The integrity, detail, and reliability of information obtained with patient consent is far superior to and more complete than data obtained without informed consent.

Restore Privacy in the Privacy Rule

Clearly, Americans believe they should be in control of their personal health information. But few consumers are aware of the vast number of corporations and government agencies that use personal health information without their

[27] Ibid, w561

permission. The right of consent must be restored to the HIPAA Privacy Rule. The blanket authority granted to millions of covered entities and business associates to use our PHI without consent for purposes of "treatment, payment and health care operations" must be eliminated. None of those uses of data should occur without explicit patient permission.

Examples of Electronic Consent Systems Demonstrated at the Consumer Choices Technology Hearing[28]

Health IT can enable privacy and patient control. A number of examples that are in effect today were recently demonstrated for policy makers. These are just a handful of solutions that show control is not overly technical, complex or expensive.

Behavioral treatment and substance abuse treatment centers, that are members of the **National Data Information Infrastructure Consortium (NDIIC),** have been using an open source EHR for over 9 years. This open source EHR provides granular, electronic, informed consent. These EHRs are used in 9 states and regions, covering 22 jurisdictions. Additional states are implementing NDIIC systems. Large and small provider organizations, across large and small states and counties have generated and exchanged over 4 million clinical records point-to-point. Records are only disclosed with informed consent.

A "point and click" format allows clinicians to quickly and easily enter the patient's specific consent directives. This makes it easy to know what information is released to whom, for what purpose, and for how long. Recipients cannot receive data unless they agree to use it only for the specific purpose requested. They must agree to obtain a new informed consent for other uses. This consent module is being translated into HL7 computer language for wide-spread use; the set of consent functionalities/choices in the NDIIC consent modules should be the minimum functionalities required for our health information in all IT systems and websites that handle PHI.

Another solution is **HIPAAT**'s consent management tools that work with any EHR. HIPAAT allows patients to create very simple or detailed consent directives. Any or all of the following are parameters that may be selected: Consent type, purpose of use, who may or may not access PHI, and PHI granularity including all PHI, PHI within a given time period, PHI related to a specific medical condition, or specific PHI types (e.g. prescription history).

Private Access has created technology that allows each person to grant "private access" to all or selected parts of their confidential personal information. The individual makes a decision based on his/her particular needs and interests. It empowers patients to participate in research that matters to them and can be used

[28] Privacy and Security Tiger Team: Past Meetings, June 29, 2010, Consumer Choices Technology Hearing. See testimony and video at:
http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910

for consent in clinical settings and on websites. For example, one Private Access product, "Privacy Layer", is an automated system that responds within seconds at a cost of less than a nickel. The answer to a researcher's query for health records takes into account both applicable law and the potential research subject's wishes. Pfizer has partnered with Private Access to use the technology to recruit subjects for clinical trials, based on the privacy directives of the potential research subjects. This Private Access product solves the most important research problem of all: how to do genetic research via trusted health IT systems and enable consumers' choices to be respected. This consent system costs about $5/year per patient.

e-MDs' EHRs enable physicians to segment patients' sensitive data so that it is not disclosed. The records sent can either be 'flagged' as having some data elements missing or simply sent with empty data fields. e-MDs' EHR has received the highest ratings from the American College of Physicians and the American Academy of Family Practice. And it complies with laws in all 50 states that require the segmentation of sensitive data and separate consent for its release. This system could be easily adapted to allow patients to choose which data is segmented. Every system that handles PHI must be improved to meet the laws in EVERY state that require the ability for patients to segment many kinds of sensitive data. e-MDs proves that the capacity for segmentation can be built into all EHRs.

Tolven Institute's open source personal health record system (PHR) is being deployed in the Netherlands, where only patients can disclose their data, unlike the U.S. In the Netherlands, data can be disclosed and shared only from PHRs with patient consent. Once a patient consents to having a PHR, no further consent is needed since all importing and exporting of information in and out of the PHR occur because of the patient's explicit actions. Doctors, hospitals, labs, pharmacies, etc are never allowed to share or disclose health information in the Netherlands; only patients can share their electronic medical records.

The **Department of Veterans Affairs** demonstrated open source consent technology available at no cost. It enables patients to decide what information they do or do not want to share, under which circumstances they wish to share, and with whom. Patient choices are captured in an electronic consent directive that assures that any restrictions patients place on disclosing their PHI are applied to their data at all times health information is exchanged. This consent technology is fully interoperable; it is capable of sharing the patients' choices and directives with other healthcare organizations. The technology is scalable, standards-based, and can be used without replacing or changing existing legacy EHR systems. The system is being piloted in San Diego, where records will be shared with patient consent between the VA and Kaiser Permanente. When fully operational, the entire population of six million US veterans will be served.

InterSystems Corporation's HealthShare Consent Framework was designed to enable patient consent to share data via Health Information Exchanges (HIEs) and over the Nationwide Health Information Network (NHIN). This software was built

to work with InterSystems' "Cache" health data bases. Cache data bases are used by 67to 85% of healthcare-related entities in the US. For example, the VA and EPIC EHRs both use Cache data bases. To date, only opt-out consent is offered by HealthShare Consent Frameworks. "Opt-out" consent means that all our data will automatically be shared with the HIE or via the NHIN unless we object and opt-out of HIEs or the NHIN completely before our data is disclosed, i.e., it is not possible to keep any sensitive health information from being widely disclosed. Patients are forced to allow access to everything in order to have the benefits of health IT. The "opt-out" consent approach violates our rights to selectively share health information. This deceptive way to force consumers into sharing data is used now in New York and Indiana, and proposed in many more states. According to InterSystems, their consent frameworks could offer robust consumer consent filters; patients could segment sensitive data by data type or class of information, date range of events, by the selection of certain users, and hide the presence of information at any location or facility.

The four HIEs now using **HealthShare** were ***not*** willing to offer patients any choice but opting-out of all data sharing. These four communities decided to severely limit how patients can configure their consent policies; they did not take note of patients' expectations, existing legal rights, and medical ethics. The good news is that the 67-85% of the American healthcare system based on Cache health data bases *can* support patient consent choices and directives. Technology can be improved within all HealthShare Consent Frameworks to ensure that patient privacy expectations are met; the systems can be programmed to make it happen. The bad news is that many other HIEs across the nation may also decide to offer only deceptive, unfair opt-out electronic consents.

Privacy Profiles

One way to help people learn how to use electronic consent systems is to create 'privacy profiles', i.e., sets of consent 'rules' or directives individuals can choose from. This approach offers examples of how consent directives can be set up, so patients are not overwhelmed with too many choices or too much information. If a person ranks their privacy concerns very high, they might select Patient Privacy Rights' 'privacy profile' as the default settings for consent, to ensure his/her directives are highly protective. Another person might trust the American Cancer Society and use their consent recommendations. Still another may choose a 'middle-of-the-road' 'privacy profile'. Private Access has developed a number of 'privacy profiles' using real people's consent directives as examples. Those who share their 'privacy profiles' explain why they made their choices to help others think about how to set consent preferences.

Health Record Banks

Health record banks or trusts are the simplest and best solution to the challenge of storing and enabling the exchange of data. A health record bank can make exchanges inexpensively while fully protecting privacy via patient control.

In the health record bank model, everything is done only with *consumer consent*. Consumers control their complete records in the health bank and they decide who gets to see which parts of their records. This protects privacy (since each consumer customizes their privacy policy), promotes trust, and ensures stakeholder cooperation since all holders of medical information must provide us with copies of all our health information when we request it.[29] *Patients control access* to the complete copy of their records, and they can add information (such as diet, exercise, alternative therapies, occupational and environmental factors, etc). Of course, the source of each item of information is clearly marked. This enables accurate copies of official medical records to be clearly distinguishable from consumer entries.

Washington State, 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 that houses copies of complete health records that are controlled by patients. Whenever a patient receives care, records generated are deposited in his/her health record bank account. Non-profit community organizations provide governance and may contract with for-profit corporations to develop and operate the HRB.

In addition, health banks can enable participation in research without disclosing any data to researchers. Research queries can be run on all the health data of patients who consent to have their data used for a particular research study. The health bank would then return the query results to the researchers. This system minimizes the number of disclosures of PHI. Because every disclosure of PHI exponentially increases the risk of data theft, data loss, and exposure, being able to permit beneficial uses of personal health information without risking personal harm is critically important. 'Distributed' data systems or networked approaches where personal data is searched in every location are complex, costly, and make protecting privacy much more difficult. In addition, 'distributed' data systems create a major threat to data security, since our data will only as be secure as the 'weakest link'.

Conclusion

Fortunately, innovative privacy-enhancing technologies enable patients to control personal health information, except in rare instances where disclosure is required by law. Further, they allow the patient to direct or restrict data flow from EHRs, electronic health systems, and databases with personal health information. Consumer control over PHI is the simplest, easiest, cheapest, fastest, and most efficient enabler of health information exchange. Consumers' rights to control PHI by giving or withholding informed consent has the added advantage of complying with state and federal privacy laws, legal and ethical requirements and the public's expectations. **Informed electronic consents can ensure personal health data is available at the right time, in the right place, for the right person.**

[29] For more information, see David B. Kendall, Protecting Patient Privacy Through Health Record Trusts, *Health Affairs*, March/April 2009; 28(2): 444-446. http://content.healthaffairs.org/cgi/collection/internet_and_health

Far from being an obstacle to data flow, informed consent assures “data liquidity” and “data integrity”. Informed consent eliminates the need for expensive, complex, and cumbersome legal agreements among stakeholders involved in HIE. Further it assures consumer trust along with data and claims integrity.

We urge decision makers, lawmakers, and policy makers to work diligently to make sure our national health care systems honor what patients want, what patients need, and what patients expect at every level.