patientprivacyrights

April 14, 2010

Federal Trade Commission *Via Weblink*
Office of the Secretary
Room H-135 (Annex P2)
600 Pennsylvania Avenue, NW
Washington, DC 20580

**Re**: **FTC Privacy Roundtables - Comments, Project No. P095416**

Patient Privacy Rights (PPR) is the nation's leading health privacy watchdog. PPR has over 10,000 members in all 50 states. We lead the trans-partisan Coalition for Patient Privacy representing over 10 million Americans. Our mission is to ensure the individual's right to privacy, i.e., to control his/her sensitive medical information to protect jobs and key opportunities in life. We thank you for launching this critical and timely public dialogue on the risks and benefits of information-sharing practices, consumer expectations regarding such practices, behavioral advertising, information brokers, and the adequacy of existing legal and self-regulatory frameworks. We appreciated the opportunity to participate in Panel 2 on Health Information at the FTC's third Roundtable on March 17, 2010 and now to submit follow-up comments.

We will focus our comments on health information privacy. Clearly, ironclad security protections should be required for all systems and software that handle health information. We assume the FTC will hear from many other organizations and security experts about the tough standards needed for health data security. Our expertise is privacy, an area that is rightfully married to security, but an area of key importance on its own.

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 in electronic systems. This approach is needed in both online and non-traditional environments where health information is handled. We hope to work together to build privacy-protective legal and regulatory frameworks so that Americans' longstanding rights to health information privacy are preserved and strengthened in the Digital Age.

**Control over personal health information, the most sensitive personal information of all, from prescription records to DNA, is absolutely essential for patient trust in electronic systems.** This is true in both the traditional health care sector and in all non-traditional and/or online commercial and health environments—with rare statutory exceptions.

- HHS found that health information privacy " is necessary to secure effective, high quality health care" because the "entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care provider"[1].

Without meaningful and comprehensive privacy and security protections to protect health information everywhere it exists, patients will not be willing to seek healthcare and treatment or participate in electronic health systems. 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. If personal health information is ONLY protected in traditional settings and not everywhere else, then Americans will lose their traditional rights to health privacy. Privacy protections must follow the data.

For over a decade all polls and surveys show that a majority of Americans are concerned about the privacy of their personal health information. The latest poll results confirm these concerns. Just yesterday the California Healthcare Foundation's poll on Personal Health Records (PHRs) found the same large majorities of Americans are concerned about privacy:

- 68% were concerned about the privacy of medical records
- 75% concerned about privacy of "information" in a PHR

**Further, the strongest rights Americans have to control personal information are their rights to control personal health information.** If these rights are not restored and strengthened, then we have no hope of creating and/or extending rights to information privacy and protections to all other kinds of personal information in electronic systems, from IP addresses, to financial and commercial information, to cell phone records, internet search records, information and pictures/videos on social networking sites, and GPS location records.

We use the NCVHS definition of health privacy (June 22, 2006, Report to Sec. Leavitt) as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data", because this definition fits with consumers' expectations and the meaning of the term "privacy" in the law.

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

[1] 65 Fed. Reg at 82,467 (Dec 28, 2000)

**1. Americans care deeply about privacy and controlling their personal information**. A 2009 report 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[2].

- 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 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. (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)
- Moreover, a 2005 survey for the California Health Care Foundation 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.[3]
- According to a national survey commissioned by the Institute of Medicine in 2007, 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.[4]
- Finally, a 2009 poll by NPR/Kaiser Family Foundation/Harvard School of Public Health found that 59% of Americans are not confident that medical records and personal health information stored electronically and shared online would remain confidential and 76% thought it likely that unauthorized person would get access to their electronic medical records stored and shared online. [5]

[2] 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)

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

[4] A.F. Westin, How the Public views Privacy and Health Research, Original Report - November 2007; Revised and expanded - March 2008 http://www.iom.edu/CMS/3740/43729.aspx (last visited September 14, 2009)

[5] NPR/Kaiser Family Foundation/Harvard School of Public Health (April 2009), The Public and the Health Care Delivery System http://www.kff.org/kaiserpolls/upload/7888.pdf

**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.

The President's nominee to lead CMS, Don Berwick, MD, proposed the right to health privacy as a critical tenet of a "patient-centered" healthcare system in *Health Affairs*, i.e., "Medical records would belong to patients. Clinicians, rather than patients, would need to have permission to gain access to them."[6]

Industry and government calls for a new, one-size-fits-all national privacy policy are contrary to the longstanding individual rights and expectations of the citizens of our nation and would prevent building a "patient-centered" healthcare system. The only privacy policy that everyone can agree with is ensuring each person can set their own policies, in accord with ethics and the law. Luckily today's privacy-enhancing technologies can empower each individual to choose his/her own privacy preferences and directives. In fact, the AHRQ Report reported there was no support for the establishment of general rules that apply to all health care consumers. Participants in the 20 focus groups agreed 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 to ensure research and access to information needed for treatment and personal use**. Data collection, storage, use, and exchange based on consumers' rights to control PHI by giving or withholding informed consent has the added advantage of complying with the most stringent state and federal legal and ethical requirements. Far from being an obstacle to data flow, privacy (consumer control over routine uses of PHI) assures "data liquidity" by eliminating the need for expensive, complex, and cumbersome agreements among "stakeholders" involved in HIE.

**4. Patient control ensures the cooperation of all stakeholders.** Patients alone have the clear legal right to electronic copies of their records (granted in the HIPAA and reinforced by the ARRA). Patients alone can force the end of the "silo-ing" of health data in proprietary, commercial, and government systems.

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

[6] Donald M. Berwick**, "**What 'Patient-Centered' Should Mean: Confessions Of An Extremist: A seasoned clinician and expert fears the loss of his humanity if he should become a patient." Health Affairs 28, no. 4 (2009): w555–w565 (published online 19 May 2009; 10.1377/hlthaff.28.4.w555)

1. Most HIT systems today do not ensure 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 and all other non-traditional environments where health information exists is the way to achieve progress and reap the benefits of HIT.

Risks and Benefits of the Use of Personal Health Information (PHI)

Clearly there are many benefits to using personal health information. Nevertheless, those benefits will not be realized if the very real risks of using personal information are not thoroughly addressed. Often the risks and harms of using of healthcare data are overlooked. Corporations and data miners are able to use data for purposes patients would never agree to -- for marketing, targeting, red-lining, profiling and discrimination -- all while the rest of the healthcare industry and the federal government tries to convince the public that Health IT is a golden goose that will save money, save lives, and produce miraculous new treatments. This can occur without recognizing the massive human costs and expenses being paid now because people avoid early diagnosis and treatment for many costly and deadly diseases, knowing that their jobs and insurance coverage will be affected. 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[7].

We cannot ensure accurate and complete data will be available for all the good uses of Health IT without ensuring that consumers can prevent the bad uses. Patients must be able to retain control of their own personal information and clear, enforceable guidelines and restrictions must be in place for the use and sharing of health information wherever it exists.

**Recommendations**

1. **All personal health information should be treated as "sensitive" information and receive the same high degree of protection accorded "sensitive" PHI**

This issue is more complex than an individual's desire to keep her DNA, prescriptions, sexual history or use of anti-depressants private. It today's digital era of information, complete and rich health profiles can be developed from sources other than traditional health records and health records creators. The data mining industry can piece

[7] 65 Fed. Reg. at 82,777 and 65 Fed. Reg. at 82,779

together profiles of individuals' health status and information from numerous non-traditional sources of PHI---- from online searches, social networks, public and private websites that have personal health information and sell or allow data use without informed consent. These profiles can contain a treasure trove of information on a person that can be used for many non-altruistic purposes. Truly, PHI can no longer be considered "safe" or "not sensitive" anywhere inside or outside the healthcare system. For example, even "normal" test and x-ray results collected and aggregated with other data as "baselines" are critical information to be used in the future as proof health status has changed. Considering the advanced techniques for collecting, aggregating, and matching PHI from disparate sources, no data can be considered safe anywhere, absent proof.

**2. De-identification and data anonymization are not enough to protect health data.**

Some argue that de-identification and data anonymization ensure that PHI can be used for a myriad of purposes, without informing a patient or obtaining her permission. The proof that this kind of data is "safe" is almost never offered; typically there is no external auditing or testing, nor any release of the algorithms that would enable proof of de-identification or other forms of anonymization. Techniques for re-identifying data are well-established, improve daily and are used because health information is the most valuable personal health information of all. Dr. Latanya Sweeney showed she can re-identify 87% of the population with just gender, month and date of birth and zip code.

<u>Data is either useful or anonymous, but never both</u>. Paul Ohm's recent work on the failure of anonymization is a must-read for all FTC staff.[8] Data may seem anonymous but when coupled with another set of data, the merged data set can often reveal identity.

**3. Stringent standards for informed consent, accountability, amending data, and data handling should apply to personal health data wherever it exists, in the traditional health care sector and in all non-traditional and/or online environments—with rare statutory exceptions.**

We ask the FTC to set a high bar to protect health information privacy, that complies with strong existing law and medical ethics, the historic new privacy requirements in ARRA, the requirements in 42 CFR Part 2, the strong protections for sensitive data in all 50 states, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[9], and just as importantly, meets Americans' expectations. Privacy protections must follow health data wherever it flows in order to be effective and to restore the right to health information privacy.

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

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#top

The healthcare and health data mining industries will not willingly build or 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 only legal, ethical, cost-effective, and practical way to get a complete and accurate picture of Americans' health and health data and to maximize the use of PHI for potential benefits and uses, both societal and personal, is to ask for permission to use the data up front. Obtaining information from records that patients have checked for accuracy, after the purposes, recipients, and length of time the data can be held or used is explained will enable trusted researchers to obtain richer, more accurate, and more complete data than can be obtained by the elimination of consent or the substitution of decisions by IRBs and Privacy Boards, whose interests may not coincide with patients' expectations.

Writing about the recommendations of the IOM to eliminate informed consent for most research uses of PHI in Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research[10], January 27, 2009, 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".[11]

**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

[10] See http://www.iom.edu/Reports/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research.aspx

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

where it goes. The good news is that 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)[12].

- 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.
- 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.

**Privacy-enhancing technologies and systems**

We believe, as we think you do, that technology offers innovative solutions to ensure privacy and progress. Technology is not the obstacle to obtaining informed consent for data use. In fact, technology offers exquisite privacy-empowering tools so patients can segment their information and exercise the control they desire as described above. Here are a few examples of privacy-enhancing technologies and systems:

**NDIIC Consent Management**

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 with granular, electronic, informed consent for over 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. And recipients cannot receive data unless they agree not to use it for any other purpose

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

without obtaining new informed consent. The consent module is being translated into HL7 for wide-spread use and should become the minimum set of consent functionalities/choices required for all IT systems and websites that handle PHI. The Coalition for Patient Privacy has recommended this system repeatedly to the NCVHS and to ONC/HHS in various letters, because it works and the government has already invested heavily in the development of this consent system.

### Private Access

Private Access has created technology that allows each person to grant "private access" to all or selected parts of their confidential personal information based on their particular needs and interests. It empowers patients to participate in research and can be used for consent in clinical settings and on websites. For example, one product, "Privacy Layer", is an automated, transaction-based system that responds within seconds at a cost of ales than a nickel. The answer to a researcher's query takes into account both applicable law, the record subject's wishes. Pfizer has partnered with Private Access to use the technology to recruit subjects for clinical trials, based on the preferences of the subjects. This system solves the most important research problem of all—how to do genetic research via trusted health IT systems that enable consumers' choices to be respected.

### HIPAAT Consent Management & Auditing Solutions

HIPAAT 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).

### PrivacyAlert (Imprivata)

Imprivata's "PrivacyAlert" enables audit trail functionality derived from its robust 2nd factor authentication software; so every access to clinical data (not just EHR software but to all the other HIT software tools/systems used to handle every kind of identifiable and de-identified or anonymized clinical, demographic and financial data in HIT systems) is tracked by name, date, function, etc. This technology is used by hospitals and large clinic systems to monitor all access to PHI by employee name, by suspicious common patterns of inappropriate access, etc. on a dash board without going to the IT dept to have them laboriously and expensively pull specific or random records for review. This technology demonstrates that audit trails can be to put in place now to ensure robust accountability for uses and disclosures of PHI. Virtually all authentication systems could develop audit trail software because it's such a logical additional use of the authentication transaction data. And since robust authentication is required of all HIT systems by ARRA, audit trails are actually easy to provide.

**e-MDs Electronic Health Records**

e-MDs EHRs enable physicians to segment data before disclosure, and the data sent can either be ‘flagged’ as having some elements missing or sent with empty data fields. This EHR has received the highest ratings from the ACP and the AAFP. It enables segmentation of data, as required in all 50 states for sensitive PHI. This system could easily be adapted to allow patients to express their preferences about which data is segmented, not just physicians. Systems that handle PHI must be improved to meet the laws in EVERY state that require the ability to segment many kinds of sensitive data. e-MDs proves that the functionality of segmentation can be built into all EHRs.

**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.

**In conclusion:**

In addition, in order for the FTC to assure consumer engagement, choice, and trust in commercial and government practices for the use of personal health information, across all environments, we recommend the following broad policies:

1) No protected or personal health information (whether aggregated, de-identified or anonymized) should be collected, used, disclosed, exchanged, or held without the informed consent of the consumer. Technology can enable instant real-time contact with consumers via email or cell phones to obtain consent if their consent directives do not cover a particular situation. There should be no secret databases or secret health data mining industry using Americans’ personal health information.

2) The patient should have 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) Independent certification of It systems that handle PHI will be essential for consumer trust that they control their data, in accordance with ethics, the law, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

4) The FTC should consider partnering with Patient Privacy Rights and other organizations in the 'Do Not Disclose' campaign to set up an online system to educate Americans about privacy choices and enable them to set up basic directives about their privacy choices that all holders and users of personal health information must check with before the use or disclosure of PHI. See: http://patientprivacyrights.org/do-not-disclose/

We also recommend that the FTC become informed about innovative privacy-enhancing health technologies by

1) Inviting a panel of vendors and organizations that build, use, and develop privacy-enhancing products and HIT systems to meet with and advise relevant FTC staff and senior personnel. We have provided the FTC with a short list of suggested invitees to consider. Both open source and proprietary solutions being used today permit accountability, 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[13] to offer ongoing expertise to the FTC.
3) Use national privacy experts to help the FTC develop a timeline that ensures patient choice and control over protected health information in commercial, government, and online environments are added to all IT systems in the next 24 months.

A recent article from the UK Times Online[14] demonstrates the kind of public outcry we can expect if we fail to protect and strengthen Americans' rights to health information privacy. British patients were outraged. They suspected the Labour party used the government's NHS (Natl Health Service) data base to find cancer patients and pressure them to vote against the other parties. But even if NHS data was not used, clearly commercial health data for sale in both the UK and the US can be used to find cancer victims and their addresses. Allowing the secret US data mining industries that steal,

[13] 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.
[14] Times Online, Labour (Party) attacked over mailshot to cancer patients. See: http://www.timesonline.co.uk/tol/life_and_style/health/article7094604.ece#cid=OTC-RSS&attr=797084

collect, aggregate, and sell all Americans' sensitive personal health information, searches, posts on social websites, purchases, and email about health to continue doing business-as-usual is a prescription for disaster.

We strongly believe that patients and consumers want, expect, and are very capable of expressing their preferences about how their personal health information is used and who can use it. Patients are becoming more savvy, not less. We urge you to avoid underestimating 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 work with you on this critical matter.

Sincerely,

Deborah C. Peel, MD
Founder & Chair

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)