patientprivacyrights

Ensuring you control who sees your sensitive health information

Patient Privacy Rights Public Comments on the Request for Information on the Nationwide Health Information Network: Conditions for Trusted Exchange

June 29, 2012

Dear Dr. Mostashari:

We appreciate the opportunity to respond to the Request for Information on the Nationwide Health Information Network: Conditions for Trusted Exchange.

Patient Privacy Rights (PPR) is the leading national and international consumer voice for building ethical, trustworthy Health IT systems. We have over 12,000 members in all 50 states and lead the bipartisan Coalition for Patient Privacy, representing 10.3 million Americans.

PPR supports and promotes:

- Meaningful informed consent for the use and disclosure of protected health information (PHI) in electronic systems to ensure patients can trust physicians and are willing to participate in electronic health systems and data exchanges.
- Comprehensive and meaningful data security and data privacy protection frameworks.
- Privacy-enhancing technologies that ensure patients can securely move the right information to the right person at the right time and enable data use with consent, while preventing unwanted sale, theft, or use of personal health information.
- Public education about the benefits and risks of Health IT and data exchange via the International Summits on the Future of Health Privacy (the 2nd summit was held in Washington DC, June 6-7, 2012. See www.healthprivacysummit.org.

General Comments on the Request for Information on the Nationwide Health Information Network: Conditions for Trusted Exchange

We agree that "a properly crafted governance mechanism could yield substantial public benefits" and that "the governance mechanism could include more prescriptive and/or more stringent policies for entities that facilitate electronic exchange than are included in the HIPAA Privacy and Security Rules."[1]

[1] Fed. Reg. Vol. 77, No. 94/Tuesday May 15, 2012/ Proposed Rules 28545

In today's environment, data exchange is anything but "worry-free." Consumers have no "chain of custody" so they can truly know who has accessed their health data; hidden data sharing and sales are widespread. The Harvard Data Privacy Lab and PPR have launched a project to map hidden health data flows called theDataMap.org. It's impossible for consumers to weigh the risks and benefits of using health IT and data exchanges when they have no idea where their data flows, who is using it, or for the purpose of its use. To enable trust and to comply with consumers longstanding rights to health information privacy, the ONC should require meaningful electronic patient consent before PHI is exchanged via the NwHIN governance and CTEs, in the Direct Project, and in Private Sector Electronic Exchanges.

Westin's 2010 study[2] of polls and surveys of public attitudes toward health IT shows a significant distrust of electronic health systems. Over the past 20 years, he found that 35-40% of the public are "health privacy intense" and:

- Distrust many government and business data practices, especially if through technology systems
- Worry about secondary uses of their personally-identified health data by insurers, employers, and government programs.
- Have concerns about researchers getting access to their personal health data without notice and direct consent.
- Are most strongly concerned about discrimination against persons with potentially stigmatizing conditions.
- Unimpressed by voluntary practices—people want legal controls and strong regulatory enforcement.

Additionally, Westin found that 35-40% of people are “Privacy Intense” when it comes to health privacy issues, which is notably higher than the 25% of people who are “privacy intense” in general consumer privacy areas.

According to AHRQ's Report[3] on 20 focus groups across the nation:

- A majority of participants believe their medical data is “no one else’s business” and should not be shared without their permission. This belief was not necessarily expressed because individuals want to prevent specific uses 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 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.

---

[2] Westin, A. What Two Decades of Surveys Tell Us About Privacy and HIT Today. (June 2011) , https://custom.cvent.com/8C4BB5624279479B8D976E45540562FA/files/7d07e389dafd4bd8958a99668d93a19d.pdf

[3] 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

Clearly, the success of electronic exchange depends on far more than "assurances that personally identifiable health information will remain confidential and secure."[4] Success depends on meeting patients' rights and expectations for both ironclad data security and ironclad individual control over where data flows (i.e., on the right of consent and control over data use and disclosures). Our strong national consensus that the right of consent is essential can be seen in medical ethics, state and federal law, and court decisions. Informed consent is essential for trust. In healthcare, trust doesn't "scale." Rather, it develops between the two individuals involved in treatment: a patient and a health professional.

Every state has developed a body of law and common law requiring consent before health information is disclosed. The nation has a very consistent national framework requiring consent and special protections for sensitive information (genetic, mental health, STDs), developed over centuries. Sensitive information may take on different meanings depending on each consumer. For example, one individual might not want the world to know he or she suffers from long term headache, but the next person may not care. The point is that we are **not** starting with a blank slate on the issue of consent; rather, the public expects consent and control over disclosures of health information.

There was a significant omission in section C. Historical Context, a. 2001-2004[5] that should be corrected in the NPRM for NwHIN governance and CTEs. This omission about changes to the right consent is the key reason that developers of health IT systems, architectures, and data exchanges did not add meaningful and comprehensive data privacy and security protections to existing or new electronic health systems.

When the HIPAA Privacy Rule was implemented in 2001, it included the right of consent:

> "*….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."*[6]

But when HIPAA was amended[7] in 2002, the right of consent was eliminated:

> *"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."*

When HHS eliminated Americans' fundamental, Constitutional right to health information privacy, Congress, the public, and the media didn't notice. However, consumers no longer had the right to decide when PHI would be used and disclosed. Instead, providers and covered entities were given new rights to control the use and disclosure of PHI. Without a right of consent in HIPAA, covered entities, including healthcare corporations and state and federal government agencies, freely use and disclose PHI for virtually any purpose. Health IT

[4] Fed Reg Vol. 77, No. 94/Tuesday May 15, 2012/ Proposed Rules 28547
[5] Fed Reg Vol. 77, No. 94
[6] 65 Fed. Reg. 82,462
[7] 67 Fed. Reg. 53,183

vendors built systems without any mechanisms to enable patient control over PHI, despite the fact that HIPAA was supposed to be the 'floor' for privacy protections. [8,9]

> "State laws that are more stringent remain in force. In order to not interfere with such laws [affording a right of consent] and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a 'best practices' standard. Thus, professional standards that are more protective of privacy retain their vitality."

Therefore, PPR strongly supports ONC's intent to add essential additional privacy protections to the NwHIN to benefit individual consumers. One of the governance mechanism's potential benefits could be the establishment of additional safeguards specific to electronic exchange that are not addressed by other Federal laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, or State laws. For example, the governance mechanism could include more prescriptive and/or more stringent policies for entities that facilitate electronic exchange than are included in the HIPAA Privacy and Security Rules.[10]

PPR recommends 5 key Conditions for Trusted Exchange:

- Technologies and systems that exchange data should comply with “gold-standard” health data privacy principles/policies,[11,12] such as the consumer principles developed by the bipartisan Coalition for Patient Privacy, which were supported by industry and consumer organizations. These principles embody Americans' longstanding rights to health information privacy articulated in common law, tort law, state and federal law, court decisions, medical ethics and Constitutional decisions.
- HHS/ONC adoption of the NCVHS definition of health information privacy[13] as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."
- A 501c3 privacy certification organization to certify other validation bodies (VBs), Nationwide Health Information Network Validated Entities (NVEs), data exchanges, and all data holders and users in the ecosystem. Certification will assess compliance with “gold-standard" health data privacy principles. The privacy certification organization should be governed by a board of patient/consumer membership organizations that focus on health privacy rights and have no commercial activity or commercial subsidiaries. The NwHIN, the Direct Project, CEHRTs, NVEs, VBs, and

[8] 67 Fed. Reg. at 53,212
[9] Fed. Reg. Vol. 77, No. 94
[10] Fed. Reg. Vol. 77, No. 94/Tuesday May 15, 2012/ Proposed Rules 28545
[11] 2007 Coalition principles, see: http://patientprivacyrights.org/media/2007_Patient_Privacy_Principles.pdf
[12] 2009 Coalition principles, see: http://patientprivacyrights.org/media/CoalitionPatPriv_Final01.14.09.pdf
[13] NCVHS June 2006, Report to HHS Sec. Leavitt, on “Privacy and Confidentiality in the Nationwide Health Information Network.

any corporations or organizations that use or handle health information must be annually certified to have state-of-the-art data security and state-of-the-art data privacy protections.

- The governance structure of the privacy certification organization should require that 2/3 of the board members represent consumer advocacy membership organizations that focus on health privacy rights and 1/3 of the board members represent physician and other health professional organizations. This structure is the only way to preserve trust in the physician-patient relationship and ensure public trust in and support for health IT and data exchange. The healthcare and health IT industries, including for-profit research and data mining corporations, have dominated the existing public-private “stakeholder” organizations, and completely failed to inspire trust in electronic health systems. Corporations' fiduciary duties to shareholders to make profits override patients' strong rights to health information privacy and interests in preserving trustworthy physician-patient relationships. Industry does not belong in policy-making positions that affect consumers, or in the governance structure of data exchanges. Industry can be advisory, but should have no power in any governance structures.
- Technologies and systems that exchange data should comply with “gold-standard” health data security principles/policies promulgated and certified by the British Standards Institute. Again, it makes sense to meet tough, state-of-the-art international data security certification standards. Does American data need less protection than European health information?

Comments on Specific Questions in the Request for Information on the Nationwide Health Information Network: Conditions for Trusted Exchange

Question 1: Would these categories comprehensively reflect the types of CTEs needed to govern the nationwide health information network? If not, what other categories should we consider?

We recommend that the Conditions for Trusted Exchange should only include as safeguards annual state-of-the-art privacy and security certification as described above on pages 4-5. All technical standards for interoperability and business should be developed by NIST. The certification/validation process must be mandatory because industry does not comply with commons sense data protection requirements. As it is, 80% of industry data bases do not comply with the HIPAA security requirements, which were "addressable" starting in 2002, and mandated in 2009.

Question 2: See pages 4-5 for PPR's 5 recommendations for Conditions of Trusted Exchange

Question 3: The need for trusted certification and governance is dire. The public has no faith in business as usual.

Question 4: Voluntary validation is a non-starter; the healthcare industry has a proven track record of not bothering to protect health information privacy or security. As of July 2012, the number of major breaches remained at 435 and has affected 20,066,249 patients and patients have no ability to control the use and disclosure of PHI in electronic systems, on the Internet, on mobile devices, in clouds, or on social media.

Question 5: The federal government should set national standards for health data privacy and security, that are equivalent to PPR's 5 recommendations for Conditions for Trusted Exchange and are the same or better than the EU Data Protection principles and standards to simplify industry's costs and burdens, enable American corporations to compete abroad, enable the international exchange of data for clinical research, while enabling the public to trust systems for health data.

Question 6: PPR's 5 recommendations for Conditions for Trusted Exchange assure all systems in the US protect patients' rights to health information privacy, which is essential for trust.

Question 7: PPR's 5 recommendations for Conditions for Trusted Exchange are the way to ensure patients' longstanding rights and protections in US law and medical ethics are built into health IT and data exchange up front. HHS has tried governance systems that are designed to protect the interests of government, industry, corporations, and research stakeholders---which directly conflict with American law and patients' right of consent. State and federal public/private 'stakeholder' committees and the federal strategic planning process have failed to protect Americans' strong rights to health information privacy or to inspire trust in health IT and electronic systems. The powerful government, industry, and research stakeholders have severe conflicts of interest and most importantly are not part of the physician-patient relationship. The real 'stakeholders' in the healthcare systems are patients, whose physicians are ethically and legally required to act as their 'stewards' and carry out their specific consent directives to protect the use of sensitive personal and protected health information.

Question 8: ONC's role should be to endorse and adopt the 5 recommendations of PPR on pages 4-5. The private sector should have no roles or responsibility for the creation of privacy or security principles, policies, or standards. The private sector's role and responsibility is to build innovative health care systems that comply with Americans' rights to health information privacy and security, and comply with their expectations to control the use of PHI for TPO.

Question 9: the public does not trust voluntary validation; see Westin's survey cited on page 2.

Question 10: See PPR's recommendations on pages 4-5.

Question 11: There are many models in the law, the absolute requirements that all cars be inspected and certified as safe to drive and all cars meet certain targets for mpg and that safety protections such as seat belts and airbags must be installed in all cars are simple and clear. We need absolute data security and privacy protections for all health data mo matter where it is to protect people from hidden data flows that guarantee generations of discrimination based on health information and genomes.

Question 12: The potential impact is the public will finally begin to trust health information exchange and electronic health systems, so the volume of information and correct information in systems will increase (information will not be withheld and treatment will not be avoided out of fear of hidden data misuse and sales). ONC should require "privacy impact assessments" before any new technologies, systems and architectures, EHR criteria, data exchanges, or etc. are implemented, analogous to "environmental impact assessments" before major construction in sensitive areas can proceed. The costs of not implementing comprehensive and meaningful data privacy and security protections must be measured and weighed against the costs; one major cost that must be accounted for is the costs in lives and quality of life and family life when millions of people annually refuse treatment for serious conditions like cancer, depression, and STDs knowing their personal information will not be private or disclosed only with consent.

Question 13: Yes. This key consumer protection came from the bipartisan Coalition for Patient Privacy. Patients have a right to know who has seen or used their PHI and the purpose for the use.

Question 14: Privacy and security certification as described on pages 4-5 should be the eligibility criteria for data exchange.

Question 15: No.

Question 16: No.

Question 17: See PPR's recommendations for Conditions for Trusted Exchange on pages 4-5. Patient governance assures unrestricted access to PHI. Anyone should be able to participate in the governance of the NwHIN only if governance is required to comply with principles, policies, and standards developed by outside certification organizations structured to ensure the protection of the public's interests, as opposed to government and industry interests, as PPR recommends.

Question 18: We agree that individuals should be able to report to and complain to the certifying organizations and that ONC and FTC can also help enforce compliance with mandated privacy and security certification. Oversight is build into annual certification. Technologies and systems must be audited sooner when complaints warrant investigation. If protections are inadequate, the system or technology must be repaired or shut down.

Question 19: We agree that it is essential for entities to be able to display evidence of certification (see pages 4-5).

Question 20: These concerns are moot when all NVEs and health data users and holders must be certified at the highest levels for compliance with privacy and security data protections. This ensures there are no secondary uses of PHI without patient consent. The Direct Project is the best method at present for data exchange.

Question 21: Certifications are annual unless complaints justify new compliance audits. PPR strongly disagrees with the EHRA industry comment that "technical conditions are unlikely to change". On the contrary, technical innovations to protect data privacy and security are desperately needed because today's technologies and systems fail to adequately protect and

ensure either privacy (robust patient control over PHI and the ability to selectively share PHI) or security. Today's systems still do not comply with the following consumer protections in HITECH: the ban on the sale of PHI, the ability to segment PHI (either sensitive or erroneous PHI), accounting of all disclosures of PHI for three years, data encryption, breach notification, and the ability of patients to prevent PHI from flowing to health plans if they pay out-of-pocket for treatment. And today's systems do not enable providers to offer a robust electronic consent process or the ability to segment "psychotherapy notes" as required by HIPAA. And other federal and state data protection and requirements for consent before the release of PHI for mental health, addiction, genetic information, STDs, and other sensitive PHI are not built into health IT systems either.

Condition [S-1] PPR recommends 5 Conditions for Trusted Exchange which sets principles, policies and standards that governance organizations must adhere to.

Question 22: No. PPR recommends that NVEs and all other entities that handle health data be certified by the British Standards Institute. Re: safeguard CTEs, NVEs should not perform any services using IIHI on behalf of health plans and health care providers unless meaningful, informed patient consent is obtained first.

Question 23: PPR recommends using the British Standards Institute for certification. PPR disagrees with the EHRA industry comments that the security requirements in HIPAA are adequate for PHI. It is widely known that 80% of the healthcare industry has failed to implement even the HIPAA security requirements or do security risk assessments, both of which should have been required, not addressable. As of June 29, 2012, according to Melamedia, "the number of major [health data security] breaches remained at 435 and has affected 20,066,249 patients." 20 million breaches prove voluntary industry implementation of health data security protections has failed.

PPR recommends that PHI have even greater protections than the HIPAA requirements and recommends external security certification by the British Standards Institute. PHI is the most sensitive personal information, bar none. NVEs and entities must assure the public that state-of-the-art, ironclad, comprehensive and meaningful security protections are in place if health information is collected, held, used, disclosed, or exchanged.

Condition [S-2]

Question 24: Every data sender, receiver, and NVE must use robust 2nd factor authentication and authorization at minimum. Patients should also be able to present in-person to authenticate themselves and establish credentials. Authentication must always be at the level of individual persons, not institutions. There should be no 'indirect authentication'. Patients are treated by specific people, not by institutions. Patients have the right to know who is involved in using PHI for TPO and what aspects of TPO were provided by specific individuals. Employees of providers, covered entities, health plans, and other entities that use PHI have no privacy rights as employees. Patients have privacy rights with respect to their PHI and should be able to have a complete "chain of custody" that shows which individuals saw or used PHI or health information. This is essential for data accountability and transparency.

Question 25: There should be no 'indirect authentication'.

Question 26: All parties in electronic exchange should meet the privacy and security certification requirements PPR proposed on pages 4-5 and be formally certified. After three successful annual privacy certifications, entities may be allowed to publically attest to adherence to the privacy certification principles and policies, and then undergo periodic formal certification.

Condition [S-3]

Question 27: The exceptions to meaningful, informed consent should be rare. Informed, meaningful patient consent with patients having the ability to segment any data or data errors should be the norm. Even though HIPAA allows providers to exchange PHI without consent, HIPAA is the 'floor' for privacy protections, and stronger state law, federal law, common law, tort law, Constitutional law, and medical ethics prevail. Industry and government seem to ignore these stronger existing privacy protections. Exceptions to users obtaining informed patient consent before data exchange should be rare (such as break-the-glass exchange for emergencies) and audited, with "cc to the patient" via Direct secure email.

And "opt-in" or "opt-out" are not meaningful forms of consent, they are coercive. No one should have to sacrifice the privacy of all their sensitive health information forever in order to benefit from data exchange. Technology and systems should be designed to serve patients' needs:

> Scott McNealy, the CEO of Sun Microsystems, famously quipped, "Privacy is dead. Get over it."
> Latanya Sweeney's response: "Oh privacy is definitely not dead. *When people say you have to choose, it means they haven't actually thought the problem through or they aren't willing to accept the answer.… [Scott McNealy] very much shares that attitude of the computer scientist who built the technology that's invasive; who says, "Well, you want the benefits of my technology, you'll get over privacy".* It's exactly the kind of computer scientist we don't want to be graduating in the future."[14]

Data exchange fails if there is no means for patients and health professionals to segment sensitive or erroneous information. Segmentation has been a federal requirement in 42 CFR Part 2 for decades; it has been built into open source and proprietary EHRs for mental health and addiction treatment. All EHRs should be required to enable segmentation. ONC should have required this key patient safety functionality and patient privacy functionality in Stage One of the Meaningful Use requirements, as recommended in the letter to HHS from the bipartisan Coalition for Patient Privacy.[15]

Consent revocation must mean that data held by entities can no longer be exchanged or used. Entities cannot continue to exchange or disclose past information.

[14] http://patientprivacyrights.org/2007/06/privacy-isnt-dead-or-at-least-it-shouldnt-be-a-qa-with-latanya sweeney
[15] http://patientprivacyrights.org/media/L-Coalition_to_HIT_PC_Meaningful_Use.pdf

Question 28: Individual choice should be required for all routine data exchange. It's what patients expect and it's a longstanding right enshrined in American law and medical ethics. Individuals should have one independent location to set electronic consent directives for routine, customary uses and be contacted for consent when users request information for exceptional uses either online or via secure cell phones. The ability to contact millions of individuals cheaply, quickly, and easily electronically means that individual electronic consent should replace the use of IRBs and Privacy Boards for research using PHI. Westin studies for the IOM found that only 1% of Americans would agree to unfettered research use of PHI.[16] Most patients have never heard of IRBs or Privacy Boards and would be shocked to learn that IRBs and Privacy Boards routinely enable research access to PHI without consent. They really are offended by research use of PHI without prior consent.

Question 29: Meaningful individual electronic consent should be required for all queries not specifically mandated in public health statutes. Meaningful choice should be supported by enabling patients to have copies of all data transmissions via their Direct email address.

Question 30: Patients can legally delegate their consent choices to guardians, trusted family members and others similar to giving others a power of attorney, but patients should not be permitted to delegate consent to corporations or businesses.

Condition [S-4]

Question 31: Data security standards do not belong in CTEs. PPR recommends requiring all data holders and users to be certified by the British Standards Institute. There should be no exceptions to this certification.

Condition [S-5]

Question 32: NVEs should provide a Notice of use and disclosure in addition to seeking meaningful informed consent for data use from patients. We do not agree that NVEs have the authority to exchange PHI without meaningful consent under strong existing health privacy law and medical ethics. Again, as ONC stated in this RFI, HIPAA is still the 'floor' for data privacy protections, not the 'ceiling'. NVEs are subject to existing stronger laws and medical ethics, which enable patient trust. HITECH requires Accounting of Disclosures of PHI from EHRs for three years. This is an important first step, but ONC should extend this 'transparency' and 'accountability' requirement to all PHI whenever it is disclosed or sold by any data user, including NVEs. See PPR recommendations for Conditions for Trusted Exchange on pages 4-5. PPR does not agree that NVEs may de-identify PHI and provide it to third parties without meaningful, informed patient consent. It is well-known that re-identifying health information[17] is easy, so every method of de-identification must require adversarial testing[18] against the many public use data bases to provide assurance that the data release

[16] See IOM Workshop Presentation by Alan Westin — February 28, 2008, Washington, DC "How the Public Sees Health Research and Privacy Issues"
[17] Narayanan, A., and Shmatikov, V. Myths and Fallacies of "Personally Identifiable Information http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf
[18] Blumberg, A. Notes About Anonymizing Data for Public Release: http://patientprivacyrights.org/wp-content/uploads/2010/10/ABlumberg-anonymization-memo.pdf

does not allow more than .04% of data to be re-identified (the HIPAA 'safe harbor' requirement).

Question 33: Summarization should not be permitted. All uses must be listed and anything not listed is not permitted.

Question 34: The cost burden is minimal; NVEs know exactly which individuals they send PHI to at the direction of patients. Every transaction is tracked and every party to every transaction is known, so the audit log of disclosures is not burdensome, but can be automatically programmed to provide the information when patients request it. The other side of this question of burden is what are the costs and harms that result from not protecting patients' privacy by providing notice and meaningful consent?

Question 35: PPR recommends that NVEs and other entities that use or handle PHI be certified for protecting privacy (see pages 4-5) and that audit trails and meaningful consent be obtained before NVEs can disclose or use de-identified and aggregated PHI.

Question 36: Providing notice on a website or broadly disseminating notice is completely inadequate. Informed consent should be obtained for the aggregation, use, and disclosure of de-identified PHI, and NVEs should also provide detailed accounting of all disclosures, recipients, and purpose to patients' email addresses on request.

Condition [S-6]

Question 37: HITECH bans the sale of PHI without consent, a key patient protection the bipartisan Coalition for Patient Privacy sought to stop the massive hidden data flows and sales of PHI, but the regulations have yet to be issued. Congress intent was to end hidden data flows and end the commoditization of PHI as a business model. HITECH requires NVEs and other entities to seek informed consent for the sale of PHI (whether IIHI or de-identified PHI), so patients can choose to sell PHI or not. PPR's recommended 5 Conditions for Trusted Exchange require informed consent before use or disclosure of PHI, preventing the sale of PHI without consent (see pages 4-5). Unless strong data privacy frameworks and the right of consent are required via PPR's 5 Conditions for Trusted Exchange, the 35-40% of the public who are "Health Privacy Intense" will not trust data exchanges and health IT systems. A 2005 CHCF survey[19] found 1 in 8 patients takes actions such as avoiding treatment or tests that puts their health at risk. ONC's belief that the risks of re-identification of PHI are exaggerated has no basis in fact. The ease of re-identification[20] is well-known and the lack of a "chain of custody" that would prevent hidden data flows means patients have no knowledge of who has their PHI or how it is being used. Until the public has an accurate map of hidden health data flows[21], there is no way to assess the risk of harms from re-identification or use of PHI by innumerable hidden secondary and tertiary data users.

---

[19] California HealthCare Foundation, Consumer Health Privacy Survey, (June 2005) http://www.chcf.org/topics/view.cfm?itemID=115694

[20] Narayanan, A., and Shmatikov, V. Myths and Fallacies of “Personally Identifiable Information http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf

[21] See theDataMap.org, a project of the Harvard Data Privacy Lab and PPR.

Question 38: Without a full and accurate map of health data flows and a "chain of custody" for each consumer's health data, it is impossible to know which entities will be affected by ending the sale of de-identified PHI. Legitimate health researchers, device manufacturers, and medical intervention designers can obtain PHI from patients using informed electronic consent. All would-be users of PHI should 'just ask'.

Condition [S-7]

Question 39: PPR agrees NVEs and all health data holders involved in data exchange should be available 14/7.

Condition [S-8]

Question 40: PPR agrees that any NVE or health data holder must provide an individual with the right to access the unique set(s) of IIHI it maintains, and should also be required to provide individuals with the right to request a correction and/or annotation to this unique set of IIHI, unless a legal exception exists. This should include MPIs, and Prescription Drug and Claims registries. Certain legal exceptions exist today that permit physicians to prevent all PHI from being disclosed to the patient, such as the exception in most states for psychiatrists who may provide patients with summaries of their records rather than disclose complete records or permit psychologists to withhold psychological testing results from patients. State and federal legislators may always eliminate or add new exceptions in the future.

Condition [S-9]

Question 41: PPR agrees that NVEs and other health data holders should honor an individual's request for a correction to the unique set of IIHI that it maintains to ensure patient safety. No one cares more about data accuracy than the patient; data accuracy and integrity can be a matter of life and death. The assumption that PHI created by providers is always accurate or more accurate than information patients provide is false. The information patients provide is the basis for diagnosis and treatment.

Question 42: No. Patients should be fully educated about the risks and benefits of correcting/amending PHI, but if a patient is competent, he/she should have the right to correct/amend PHI.

Condition [S-10]

Question 43: Providers and other data users should request consent for query responses or PHI from patients via Direct email to verify treatment relationships. Although the HIPAA 'floor' for data privacy protection permits providers and Covered Entities to use and disclose PHI without consent, this method for data exchange violates the stronger, longstanding consumer health privacy protections in state and federal law, common law, tort law, Constitutional decisions and medical ethics, which all require meaningful consent before PHI is disclosed. If health IT systems and data exchanges complied with the law and medical ethics, providers and other data users could not obtain PHI on any individuals (with or without an existing treatment relationship) unless informed electronic or paper consent was obtained. To ensure

trust in the query and response model PPR recommends the 5 Conditions for Trusted Exchange on pages 4-5.

Question 44: Consent should always be required, unless there is an emergency where other patients' data could be life-saving. Clinical analytics, data analytics, the use of "big data", population health research, comparative effectiveness research, quality improvement, P4P, public health research, biosurveillance, fraud and abuse audits, and many other uses and reporting of PHI are regarded as 'research' by patients. Informed electronic consent should be required for all research in accordance with international human rights and international treaties such as the Declaration of Helsinki. PPR's 5 Conditions for Trusted Exchange on pages 4-5 would assure informed consent for research use of PHI. Patients can set standing consent directives to enable them to be contacted for drug recalls or to participate in after market research on new medications. Research is still viewed with great distrust by many vulnerable populations, including minorities, as the after-effects of projects like Tuskegee. As Westin's study for the IOM[22] showed, even today, only 1% of the public would allow unfettered research use of PHI without consent. Another example illustrating distrust regarding research use of newborn bloodspots occurred in Texas. Parents of newborns sued the state of Texas for transferring “hundreds of infant blood spots to an Armed Forces lab to build a national and, someday, international mitochondrial DNA (mtDNA) registry without consent.[23] Large majorities of the public support research when asked and informed about the nature of the research, but unless informed and asked for consent, large majorities oppose research. Researchers should seek consent from patients for the use of PHI, to ensure the public will continue support research and reap the benefits.

C I-1

Question 45: All NVEs and others should be required to "cc the patient" via Direct secure email when patients consent to data exchange. PPR recommends that all data exchanges be made via the Direct Project between two people.

Question 46: All NVEs that provide Web access portals to authorized users (including patients) must also provide a RESTful computer-to-computer authorization mechanism to avoid sharing of passwords or other access credentials. Computer authorization standards developed by NIST or the British Standards Institute should be required.

C I-2

Question 47: Patients and health professional that wish to do so must be able to use DNS to distribute their own digital certificates. Data exchange should be via person to person using the Direct Project, not to institutions with digital certificates. Institutions should not exchange PHI unless required by law. Institutions do not have direct relationships with patients, only health professionals and researchers do. The vast majority of data exchanged should be person-to person via the Direct Model. Overzealous reliance on organizational certificates will

[22] See IOM Workshop Presentation by Alan Westin — February 28, 2008, Washington, DC "How the Public Sees Health Research and Privacy Issues”
[23] http://www.texastribune.org/texas-state-agencies/department-of-state-health-services/dshs-turned-over-hundreds-ofdna-samples-to-fed

introduce scalability and consent problems that will limit the scope of the NwHIN --and erode patient trust in electronic health systems.

Question 48: See answer to Question 47.

C I-3

Question 49: Algorithms for patient matching are not needed if all data exchange occurs with patient consent via the Direct Project from one data location to a specific person at another location. Consumers exchange/move money from banks to merchants without the need to match patient accounts via algorithms**.** In a similar fashion, health data can flow easily via Direct email from person to person. All clinicians, participants, and patients should be authenticated as individuals. Data exchange should occur between individuals, with rare exceptions for institutional receivers. Patients should be able to request and receive copies of PHI from all institutions and entities that hold PHI or patient information.

Question 50: Patients should be able to authenticate themselves to give electronic consent using identifiers such as email addresses, Direct email addresses, and mobile phone numbers. Patients should be able to match themselves and send PHI from one data holder to another.

Question 51: Patients should be able to authenticate themselves in health IT systems and data exchanges; and have accounts with different numbers each place PHI is held. Unique single IDs and patient matching techniques enable others to collect and use protected health information without informed electronic consent. Patients or their appointed designees should control PHI flow for all uses via the Direct Project, with rare statutory exceptions.

BP-1

Question 52: ONC believes that PHI should be exchanged by providers, but this model is not what patients expect. Although HIPAA allows data exchange between providers, that model violates patients' rights to control access to PHI and other personal health data. Patients' strong rights to control PHI and health information in state and federal law, common law, tort law, Constitutional decisions and medical ethics prevails over the HIPAA 'floor' for privacy. Patients should be able to match their own data held by covered entities, providers, and other entities using personal account numbers at each location. Complex data matching techniques, algorithms, and DURSAs are not needed because patients can legally and simply direct data to flow to another person using consent. Patient matching of personal is accurate, simpler, cheaper, and faster than techniques employed by third parties to match patient data without consent. It also has the advantage of being legal and ethical. Third party health data exchange is not ethical, and attempting to make it workable legally using contracts and DURSAs has failed.

Question 53: Transaction fees should not be charged for electronic data exchange. NVEs should not be permitted to control exchange environments. Health data exchange should not be impeded as a matter of patient safety and public safety. Other methods for financing

technology to support exchange can be found to ensure all PHI can flow and be exchanged using the Direct Project.

Question 54: NVEs should be able to impose requirements on other NVEs and entities only to protect patient privacy and safety.

BP-2

PPR agrees that patient and physician portals are essential and that there must be directories of potential recipients and locatable public keys.

BP-3

PPR does not support the NwHIN Exchange model, except to facilitate direct exchanges controlled by patient consent. DURSAs are difficult, expensive, and by law patient consent is required for the vast majority of data exchanges because HIPAA is the 'floor' for privacy protections. In every state stronger state and federal laws, medical ethics, and patients' Constitutional rights to health information privacy prevail over what HIPAA allows. Patients do not know about or trust 'federated entities'. The Exchange is opaque and unavailable to patients

Question 55: Reports on data exchange should not include information about individuals that could be re-identified.

Question 56: PPR recommends 5 Conditions for Trusted Exchange, see pages 4-5. PPR recommends that principles and policies be developed in accord with Americans' strong right to health information privacy and the right of consent. PPR recommends that privacy principles and policies should be enforced via privacy certification, but standards for data security should be developed and enforced via certification by the British Standards Institute and NIST.

Question 57: PPR recommends that performance and service specifications be developed by trustworthy institutions like NIST and the British Standards Institute, and not driven by industry, which has inherent conflicts.

Question 58: PPR recommends 5 Conditions for Trusted Exchange on pages 4-5, which separates the development, oversight and enforcement of privacy principles from technical, interoperability, security, and business standards. Principles and policies should be developed by a patient-led privacy certification organization, free from commercial conflicts and dedicated to defending patients' rights. Standards development and standards setting should similarly be removed from the industry-driven and industry-dominated, 'public-private stakeholder' processes which have guaranteed the undue influence of a few major corporations whose interests prevail, and whose interests directly conflict with the public's rights and interests. PPR does not support bundling CTEs or creating more CTEs. Specifically, principles and standards organizations as proposed by PPR should drive governance, not the other way around. Governance must be carried out in accordance with principles and standards developed by organizations with no commercial or other interests

that conflict with the public's rights and expectations. This means members from government and industry could be on the boards of governance organizations, but would be required to uphold privacy principles and technical, business, security, and interoperability standards developed in the public's best interest.

Question 59: Why are safe harbors needed? Please explain. Compliance with gold-standard privacy certification and standards certification processes as described on pages 4-5 should be required for all entities involved in health data exchange. Technical, security, and business process standards to improve and be updated over time. Core privacy principles are enduring and from the foundation for individual civil and human rights to privacy. Implementation of privacy principles may be updated, but core principles and rights to autonomy, self-determination, to control personal information, and to be 'let alone' are the foundation of freedom in Democracies.

Question 60: See PPR's 5 Conditions for Trusted Exchange on pages 4-5. The patient-led certification organization and the British Standards Institute should update principles, policies, and standards.

Question 61: Pilots could be conducted by the patient-led certifying organization, or by certified VBs, or by other organizations that conduct pilots according to the privacy principles of the patient-led certification organization.

Question 62: PPR recommends a very different process than the federal advisory committees, multi-stakeholder public/private processes proposed to govern the NwHIN and CTEs. See pages 4-5. Again, these structures are designed to fail because the inherent conflicts of industry, government, and research organizations ensure that the public's interests cannot prevail.

Question 63: The governance mechanism ONC proposes has proven to stifle innovation. The ONC model enables the most dominant corporations and industries to decide which proprietary, legacy systems and technologies will prevail and to set principles, policies, and standards that favor their interests over the public interest. Innovation is best promoted by the model PPR proposes, where corporations, industry, and research organizations can compete based on creating products and systems best serve the public interest. The structure PPR proposes is the only path to trust in electronic health systems.

Industry and government interests so distorted the President's Consumer Privacy Bill of Rights (CPBOR)[24] that the key new rights of consumers do not apply to health information. So principle #1, "Consumers have a right to exercise control over what personal data companies collect from them and how they use it", specifically excludes consumer control over personal health information. Without a trustworthy electronic healthcare system we will never get the data we need to improve healthcare, drive down costs, and enable transformational breakthroughs in research. Worse, we know millions annually refuse

[24] http://www.google.com/gwt/n?u=http%3A%2F%2Fpatientprivacyrights.org%2F2012%2F02%2Fwh-initiative-consumer-privacy-bill-of-rights%2F

treatment for cancer, depression and STDs[25]. The lack of privacy causes bad outcomes. Refusal to seek treatment is a bad outcome and puts health and lives at risk.

Key quotes from the CPBOR "Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy":

- "Strong consumer data privacy protections are essential to maintaining consumers' trust in the technologies and companies that drive the digital economy."
- The President concluded, "It [privacy] has been at the heart of our democracy from its inception, and we need it now more than ever."

The only way we can trust the Internet and have a vibrant global digital economy is if individuals control personal information online and in electronic systems. The right of informed consent before personal information is collected or used must be restored and built into health IT systems and data exchanges now. Once trust is lost, it is very difficult to restore.

Sincerely,

Deborah C. Peel, MD

Founder and Chair

Patient Privacy Rights
O: (512) 732-0033
C: (512) 820-6415
www.patientprivacyrights.org

[25] 65 Fed. Reg. at 82,779, 65 Fed. Reg. at 82,777, 65 Fed. Reg. at 82,778