patientprivacyrights

Written Testimony
Deborah C. Peel, MD, Founder & Chair, Patient Privacy Rights

Trusted PHRs: Moving Industry Forward Responsibly and Effectively With Privacy

On behalf of the 10,000 members of Patient Privacy Rights and the 50 million Americans represented by the bipartisan Coalition for Patient Privacy, I wish to thank the Co-chairs of this Subcommittee, Leslie Francis, J.D., Ph.D., and John Houston, J.D. for the opportunity to present our members' views and positions on the policies and privacy protections needed for PHRs and electronic health systems.

Today, I will talk about how my experience as a clinician led me to found Patient Privacy Rights; the need to enforce the use of the NCVHS definition of privacy; the strong existing federal health privacy law for records of substance abuse and alcoholism treatment; the resulting robust electronic consent systems in use at behavioral health treatment centers in 22 regions and 8 states, and will close by recommending that NCVHS not re-invent the wheel.

We recommend that NCVHS enforce adoption of the National Data Infrastructure Improvement Consortium (NDIIC) open source electronic consent module for substance abuse and addiction treatment; this should be the minimum standard for consent tools in PHRs and for widespread use throughout the healthcare system. This will ensure privacy and HIE. Further, we recommend that NCVHS require the strong privacy protections in 42 CFR Part 2 be extended to cover all personal health information (PHI), wherever it is held. We want to see industry build responsible and effective consumer controls over PHI in HIT systems. Patient trust is further ensured by identifying effective existing policies, laws, and privacy-enhancing technologies that have already proven effective in enabling HIE and earning consumer trust.

The willingness to use a PHR and participate in electronic systems depends on ensuring consumers' and patients' strong preferences for privacy and longstanding

rights to control personal health information. If Americans can only control personal health information in their PHRs but nowhere else in the healthcare ecosystem, the result is no privacy and no trust. It is simply not enough to control only personal health data stored in PHRs. Privacy rights and personal control must follow our data every where it goes. To be effective, privacy rights and protections must be meaningful and comprehensive.

THE FOUNDATION OF PATIENT PRIVACY RIGHTS

In an era when records were kept in manila folders in locked file cabinets, it was not difficult to ensure medical records were private. Today, we are in a different world. Employers, insurers, and law enforcement officials want access to health records. With much of this information moving to electronic media, the threat to patient privacy is very real. **My patients, and patients everywhere will tell you: existing law does not go far enough or do enough.**

Early in my career, I learned from my very first patients that privacy was essential for treating mental illness and substance. They asked if I would keep their records completely and totally private if they paid me out-of-pocket.

Psychiatry and psychoanalysis are the most privacy-sensitive fields in medicine. Psychoanalysts study the best conditions for effective psychotherapy and psychoanalysis. As it turns out, privacy enables the deepest trust; trust that is essential to those who need to disclose the most painful, disturbing, and sensitive information, as Hippocrates discerned 2,400 years ago.

- The *Hippocratic Oath*: "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."

NEED TO DEFINE PRIVACY

The lack of privacy is both harmful and deadly. Millions of Americans avoid doctors and delay care for fear their employers will find out, their insurers will drop them or a vast world of strangers will know their most intimate details.

- According to HHS, **two million** Americans with mental illness do not seek treatment for this reason.[1]
- **600,000** cancer victims do not seek early diagnosis and treatment.[2]
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek diagnosis and treatment (1 in 4 teen girls are now infected with a STD).[3]
- The California Health Care Foundation found that **1 in 8** Americans have put their health at risk by engaging in privacy-protective behavior: *Avoiding*

[1] 65 Fed. Reg. at 82,779
[2] 65 Fed. Reg. at 82,777
[3] 65 Fed. Reg. at 82,778

their regular doctor - Asking a doctor to alter a diagnosis- Paying privately for a test - Avoiding tests altogether.[4]

- The Rand Corporation found that **150,000 soldiers** suffering from Post-Traumatic Stress Disorder (PTSD) do not seek treatment because of privacy concerns.[5] The lack of privacy contributes to the highest suicide rate among active duty soldiers in nearly 30 years.

The lack of privacy as detailed above may cause more deaths than the oft-cited statistics about that 100,000-200,000 deaths/year that are caused by medical errors. Surely the harm to millions caused by the lack of privacy deserves a response at least as serious as the response to medical errors.

In addition to bad outcomes (suffering and death), the lack of privacy results in bad data (missing and erroneous data) and increased costs. When consumers and patients figure out they have no control over PHI, there may be an open revolt – more likely system failures. The costs for reengineering to add privacy to systems will be tremendous.

The example of the UK comes to mind: over 10 years nearly 50 billion dollars was wasted on HIT systems that did not allow patients to control access to or disclosure of PHI. The expensive result is that the government finally had to restore the right of consent and rebuild the system before data could be sent to the National Health System (NHS) data base.

We can learn from the British experience. We can avoid the same problems and make certain we use the stimulus billions effectively. We can save time and taxpayers' dollars by building consumer control over data into systems up front. Current solutions—the use of CCHIT, HITSP, and HIPAA-compliance----are simply not enough to ensure the public trust. Reliance on these entities and HIPAA compliance means Americans will not have meaningful consent, segmentation, control over protected health information (PHI), or privacy for years. We cannot afford to wait.

The first step toward building trusted PHRs and a trusted healthcare system is to press HHS to accept the NCVHS June 2006 definition of privacy. NCVHS defined health information privacy as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."

Today neither HHS nor Congress has defined what they mean by "privacy". The lack of any definition results in confusion about the meaning of the terms privacy, security, and confidentiality. The result is that PHR vendors all claim to protect privacy, because no one knows what the government means.

In addition, there is no trusted, independent consumer-led organization to certify the privacy of PHRs or other HIT software and systems. Government and industry

[4] CHCH Consumer Health Privacy Survey, June 2005
[5] "Invisible Wounds of War", The RAND Corp., p. 436 (2008)

certification will never be trusted by the public, because their conflicts of interest are obvious. The holders of the data want unfettered access to the vast treasure trove of data that PHRs offer without limitation on use.

OUR VISION: ROBUST ELECTRONIC CONSENT TOOLS ENABLE TRUST IN PHRs AND THE HEALTHCARE SYSTEM

Solutions already exist. Robust electronic consent tools that ensure privacy while enabling HIE have been developed and successfully implemented by a consortium of state and county-sponsored behavioral treatment centers. Electronic consent tools have been in use over 9 years, generating over 4 million clinical records. Detailed consents could easily be adapted and required for PHRs and every kind of PHI.

The interoperable and enhanced computerized "Consent to Release of Patient Information" module was created by the National Data Infrastructure Improvement Consortium (NDIIC, http://www.ndiic.org/), a not-for-profit corporation.

The NDIIC's mission is to improve state and sub-state behavioral healthcare information technology infrastructure, capacity, and awareness.

Twenty-two jurisdictions in eight states and many counties collaborated to create and share open source and non-proprietary consent tools. Three additional states are currently developing implementation plans. Both large and small provider organizations across large and small states and counties are using these electronic consents.

Moreover, the electronic consent systems have primarily been deployed in publicly funded substance abuse treatment organizations that are required to comply with the most stringent federal privacy protections as reflected in 42 CFR, Part 2.

A Part 2 consent form must include the following elements (see addendum for more details from the Texas Consent Form):

- Name or general designation of the program or person permitted to make the disclosure;
- Name or title of the individual or name of the organization to which disclosure is to be made;
- Name of the patient;
- Purpose of the disclosure;
- How much and what kind of information is to be disclosed;
- Signature of patient (and, in some States, a parent or guardian);
- Date on which consent is signed;
- Statement that the consent is subject to revocation at any time except to the extent that the program has already acted on it; and
- Date, event, or condition upon which consent will expire if not previously revoked.

The Part 2 consent offers far stronger consumer protections than HIPAA. The Amended HIPAA Privacy Rule did not define consent.

One key to successful electronic consent forms is that the permission to release confidential information portion of the record includes the following: a detailed time, provider and record content specific approach through which the patient can specifically identify the explicit parts of their record and which timeframes of their treatment episode(s) that can be shared, with whom and for how long.

Another aspect of the use of a detailed consent form with an EHR is that it must be relatively easy to complete and be sensitive to time constraints. An advantage of the "point and click" format of these consent forms is their ease of use and the ability of the patient to make very specific determinations about what, if any, information is to be released. This level of detail assures patients of their control over PHI and contributes to their increased willingness to share information. Similar benefits can be expected for PHRs if electronic consents as detailed and robust as the NDIIC "Consent to Release of Patient Information" are used to enable data exchange.

In the more distant future, our electronic consent systems or tools may be held in one place, separate and apart from all locations where PHI is held. This is so that we truly can control all our data simply and easily. In a privacy-enhanced future, all data holders will have to electronically and seamlessly check with our single independent consent tools/module before accessing or using our PHI. These independent consent tools could and should be housed separately from data bases that hold PHRs, to enable external, independent audit trails of all uses of PHI to be generated.

Just as it makes the most sense for consumers to collect and store all PHI in one PHR, for ease of use and control, a single consent tool/module in one location is the one successful way consumers and patients can easily control PHI. For now, we suggest the NCVHS should require that consents be set up at each place patients receive care. But it's easy to end up seeing multiple providers in multiple locations each year (offices, labs, hospitals, pharmacies, x-ray facilities, etc). Keeping up with separate consents at every provider location will prove difficult if not impossible. Unless patients have a method to put all their consent directives and instructions in one place, the nation will never have a truly consumer-centric, consumer-empowered trusted healthcare system.

I want to briefly mention three other independent electronic consent management systems that permit varying degrees of data disclosures, Private Access (https://www.privateaccess.info/), HIPAAT (http://www.hipaat.com/). And You-Take-Control (http://www.y-t-c.com/magnoliaPublic/Home.html). These electronic consent solutions are newer and not as widely implemented as the NDIIC consent module.

I highlighted The NDIIIC's Consent to Release of Patient Information because it has been in use the longest time, 9 years, in the most locations, and all of the implementations successfully ensure privacy and facilitate HIE. In addition, those that receive data using an NDIIC consent are prohibited from making any further

disclosures without additional consent (adding another key privacy protection, no secondary use of data without consent). The prohibition of re-disclosure for sensitive substance abuse treatment records should apply across the entire healthcare system.

Industry claims that the use of robust individualized consent in electronic health systems is an obstacle to HIE, is too expensive or too complex to be workable are proven false by the 9 successful years where NDIIC electronic consents enabled successful data disclosure from 4 million patient records.

CONCLUSIONS

According to Forrester Research, an independent technology and market company providing advice to global leaders in business and technology, "Anyone today who thinks the privacy issue has peaked is greatly mistaken…we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."

Privacy, control over one's personal health information, matters very deeply. Public outrage when the vast hidden data mining industry and false reassurances of data security and privacy become known could destroy the possibility of ever having an effective HIT system. Once trust is lost, it is very difficult to regain. See: "Cerner finds a treasure in data mining" by Mike Sherry of the Kansas City Business Journal at: http://www.bizjournals.com/kansascity/stories/2009/06/01/story5.html?b=1243828800^1835382

Patient Privacy Rights and the Coalition for Patient Privacy work to move industry forward responsibly and effectively so that the stimulus billions are used successfully and efficiently. We are working to make sure that America reaps the benefits of a successful HIT system that restores and strengthens Americans' longstanding legal and ethical rights to control personal health information.

KEY RECOMMENDATIONS

1) NCVHS should enforce adaption of the National Data Infrastructure Improvement Consortium (NDIIC) open source electronic consent module for substance abuse and addiction treatment as the minimum standard for consent tools in PHRs and for widespread use throughout the healthcare system to ensure privacy and HIE.

2) NCVHS should require the strong privacy protections in 42 CFR Part 2 be extended to cover all PHI, wherever it is held. NCVHS should require industry to build responsible and effective consumer controls over PHI into HIT systems.

   The NCVHS should identify effective existing policies, laws, and privacy-enhancing technologies that have already proven effective in enabling HIE and earning consumer trust and recommend that HHS use these policies, laws, and tools to ensure the privacy of the entire health IT system, not PHR privacy.

SPECIFIC QUESTIONS POSED

Based on this evolution, what policy concerns do you have about these patient-facing online technologies? NCVHS should enforce its definition of privacy and require PHRs to incorporate privacy-enhancing technologies, including ironclad security measures and consumer control over access and use of PHI via the electronic consent management tools developed by the NDIIC to meet the requirements of 42 CFR Part 2, including the prohibition against re-disclosure without new informed consent.

Do you believe that the legal framework resulting from the Recovery Act is adequate to protect consumers? NO.
If not, what else needs to be in place? See Letter from the Coalition for Patient Privacy to Congress at:
http://www.patientprivacyrights.org/site/DocServer/CoalitionPatPriv_Final01.14.09.pdf?docID=4701

What policies, procedures, laws and rules must be in place to ensure that consumers' privacy rights are appropriately represented and protected?
The right to health information privacy should be restored at the federal level. NCVHS should enforce its definition of Privacy. The Original HIPAA Privacy Rule had the right of consent; the Amended HIPAA Privacy Rule eliminated the right of consent. Regulatory permission for over 4 million entities and their millions of employees to make decisions about the use of your PHI must be stopped.

The Elimination of Consent

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HSS) was required to develop regulations that specified patients' rights to health privacy.	*"...the Secretary of Health and Human Services shall submit to [Congress]... **detailed recommendations on standards with respect to the privacy of individually identifiable health information."***
2001	President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent".	*"...a covered healthcare 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."*
2002	HHS amended the HIPAA "Privacy Rule", eliminating the "right of consent".	*"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, or health care operations."*

How have you attempted, or would you recommend attempting, to address concerns presented by members of the public? Our mission is to address the public's greatest concern about electronic health systems: the lack of control over PHI. See: www.patientprivacyrights.org

Should data subjects be able to add to, change, or amend their records in the PHR? Patients are in the best position to detect errors and wrong diagnoses. For example, patients typically take 5-10 years to receive a correct diagnosis of Bipolar Disorder, accumulating many false diagnoses in the meantime. The patient is in the best position to know which PHI is correct and which doctor needs to know which things about him/her. Having a way to amend or add to records is essential so that patients can ensure their providers get the most accurate and up-to-date information needed for effective treatment.

How should PHRs deal with particularly sensitive categories of information? PHRs should enable consumers to segment any sensitive data they want from disclosure. Open source electronic consent technologies that already exist prove that it's easy and cheap to let each person segment whatever they deem to be sensitive. See testimony and attachment titled "TX Consent Components".

In good faith each of us has a different opinion regarding privacy (and what is appropriate), so how do we satisfy every consumer's concerns? We can and in fact must satisfy every consumer's concerns because every consumer has individual legal and ethical rights to decide how or how little privacy he/she wants. It is a fallacy that we have to have one-size-fits-all coerced 'solutions' to the question of how much privacy patients will have. Technology enables consumers to create and modify and revoke exquisitely detailed consent directives instantaneously electronically and even be contacted by cell phone or email in real time for informed consent. Electronic consent tools remove all the barriers to robust contemporaneous consent, so there is no longer a need for illegal advance consents because technology makes it cheap, easy, and fast to contact millions of people easily about giving consent (if there is no existing directive that covers the situation)

In what ways is the model notice proposed by ONC in December 2008 helpful to consumers or not so helpful? The model notice is a good start and was obviously patterned after the findings of the Altarum study of PHR privacy policies which were extremely weak. See:
http://www.patientprivacyrights.org/site/DocServer/PHRs_Altarum_2007.pdf?docID=3321
How could it be modified to be more useful? ONC should be required to use an open and full FACA process. The website says nothing about when or where to submit public comments. It should be required to post notices of the proposed model notice to obtain extensive public input.

How do the changes to HIPAA in the Recovery Act change the landscape? There are historic new consumer privacy rights, the 'asks' in the Letter from the Coalition for Patient Privacy to Congress from the core of the new protections:

- Prohibits the sale of our medical records without consent. There are exceptions for research, public health and treatment.
- Limits marketing.

- Requires any entity using an EHR (covered entities and business associates) to keep an audit trail of all people and organizations with which they share your information.
- Requires the policy committee to consider setting standards for technology systems to segment sensitive information so we can easily keep an x-ray tech from seeing our Pap smear results.
- Requires the policy committee to consider setting standards for encryption of data.
- Increases monetary penalties for violations, grants Attorneys General authority to file suit on behalf of a state's citizens, requires monitoring of contracts and reporting on compliance.
- Grants funds for non-profits to participate in the regulatory process.
- Requires breach notification.
- Allows individuals to stop disclosure of PHI for payment and healthcare operations if treatment is paid for out-of-pocket.

Do you favor federal rules for PHRs or would you prefer rules be made by the states? Unless federal law restores Americans' strong, longstanding rights to health privacy and the right of consent and incorporates all the strongest state-level privacy protections into a new federal law, state laws should not be preempted. The new requirement in HITECH for the HIT Policy Committee to make recommendations about the right to segment sensitive PHI was designed to ensure that state-level privacy protections were not eliminated.

Are there any type of medical records that should not be included in the PHR? No.

For example, those subject to the HHS Substance Abuse rules and the strict re-disclosure regime that it imposes on recipients (even those who obtain records with patient consent)? The HHS Substance Abuse rules and strict re-disclosure regime should be required for ALL exchange and use of PHI held in PHRs and throughout the health care system. This regime has enabled HIE and trust, is open source, and inexpensive.

ADDENDUM: TEXAS CONSENT COMPONENTS

Consent = Required Field

Client Name

Client Number

Discloser

Activity Begin Date

[ ] mm/dd/yyyy

Activity End Date

[ ] mm/dd/yyyy

Release Expiration Date

[ ] mm/dd/yyyy

Disclosee

[None selected \/]

Other Disclosee

[ ]

NOTE: Any item listed below may include information that reveals a client's HIV status.

Is it okay to release the following information?	**Action**	
Screening/Intake	( ) Yes	( ) No
General Assessment Only	( ) Yes	( ) No
Medical Assessment	( ) Yes	( ) No
Employment Assessment	( ) Yes	( ) No
Substance Abuse Assessment	( ) Yes	( ) No
Legal Assessment	( ) Yes	( ) No
Family/Social Assessment	( ) Yes	( ) No
Psychiatric Assessment	( ) Yes	( ) No
Diagnostic Impression	( ) Yes	( ) No

Clinician's Assessment	( ) Yes	( ) No
Assessment Recommendations	( ) Yes	( ) No
Assessment Summary	( ) Yes	( ) No
Assessment Narrative	( ) Yes	( ) No
Wait List Record	( ) Yes	( ) No
Laboratory Results	( ) Yes	( ) No
Treatment Plan(s)	( ) Yes	( ) No
Treatment Plan(s) Evaluation	( ) Yes	( ) No
Admission Reports	( ) Yes	( ) No
Procedures and Progress Notes	( ) Yes	( ) No
Clinician's Notes	( ) Yes	( ) No
Client Progress	( ) Yes	( ) No
Medication Records	( ) Yes	( ) No
Discharge Summary	( ) Yes	( ) No
Discharge Plans	( ) Yes	( ) No
Discharge Reports	( ) Yes	( ) No

Follow-Up Reports	( ) Yes	( ) No
Compliance with Treatment Requirements	( ) Yes	( ) No
Attendance	( ) Yes	( ) No
Prognosis	( ) Yes	( ) No
Referral Information	( ) Yes	( ) No
Referral Followup	( ) Yes	( ) No
Program Case	( ) Yes	( ) No
Program Service	( ) Yes	( ) No
Client Interview	( ) Yes	( ) No
Authority to Call Phone Number	( ) Yes	( ) No
Authority to Leave Message	( ) Yes	( ) No
Residential Approval	( ) Yes	( ) No
Financial Eligibility	( ) Yes	( ) No
COSIG Voucher	( ) Yes	( ) No
ATR Voucher	( ) Yes	( ) No
ATR Voucher Services	( ) Yes	( ) No

Other Confidential Information (please specify below)	( ) Yes	( ) No

Other Information to Release

Purpose for Releasing Information

Comments

Signatures

I understand that my records are protected under the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR part 2, and cannot be disclosed without my written consent unless otherwise provided for in the regulations. I understand this information will be used or disclosed solely for the purpose specified in the form. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it, and that in any event this consent expires automatically as noted above.

Client's Signature

_____ [ ] mm/dd/yyyy

Parent, Guardian or Authorized Representative's Signature When Required

_____ [ ] mm/dd/yyyy

Staff Signature

_____ [ ] mm/dd/yyyy

This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.