COALITION FOR PATIENT PRIVACY

August 3, 2009

Dr. David Blumenthal
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Ave, SW
Suite 729D
Washington, DC 20201

Re: Comments to the HIT Policy Committee on the July 16, 2009 meeting

Dear Dr. Blumenthal and Members of the Committee:

The Coalition for Patient Privacy (the Coalition) is the leading voice of consumer organizations working to protect patient privacy and encourage adoption of Health IT, representing millions of Americans. We are a diverse, multi-partisan and collaborative group united by the effort to prevent discrimination and preserve the ethical basis of the health care system.

The Coalition's three central tenets for Health IT are Accountability, Control of Personal Information and Transparency, "A.C.T. for Privacy". The Coalition worked tirelessly in 2008/2009 to lead the grassroots effort to ensure historic privacy protections were included along with the $19 billion federal investment in Health IT as part of the American Recovery and Reinvestment Act (ARRA).

Thank you for the opportunity to comment on the last HIT Policy Committee (the Committee) meeting held July 16, 2009. We comment today to raise concerns regarding the public's lack of opportunities to provide meaningful feedback to this body, the need to protect and enable patient control over protected health information at the beginning of this process, and the approved "meaningful use" matrix.

<u>Public Comment & Participation:</u>

We appreciate the Committee's attempts to invite public comment on these critical matters. We also appreciate the incredibly restrictive timeframes in place. Nevertheless, we urge the Committee to allow additional time and opportunity to hear and incorporate the public perspective. It is incredibly complicated and difficult for the public to participate in meaningful ways in this important policy making process.

The Committee has access to a tremendous wealth of expertise from the health care and information technology industries. At the end of the day, it is *the patient* that opts to share his/her personal information with a provider, and it is *the patient* that must be assured electronic health record systems can be trusted. In the "Overview of Public Comments" presentation summarizing the 792 comments received on "Meaningful Use" criteria there was

no mention of any concerns or proposals offered by any consumer or health privacy advocacy organizations. This is a striking omission from the presentation on the comments. While we will certainly do our part to ensure you hear from a large constituency, the Committee's policies will fall short of public expectations if it does not discuss any public comments from patients.

At times, the interests of the health care, HIT, research, insurance, pharmaceutical and data mining industries are in direct conflict with Americans' longstanding legal and ethical rights to control personal health information. Without additional consumer and patient engagement, expecting this process to protect consumers is like expecting foxes to design hencoops that chickens will trust. Similar to the auto, banking, and securities industries, the HIT, pharmaceutical, insurance, and healthcare industries will never add consumer protections willingly. They will always claim consumers' privacy rights are impossible, too complex, too expensive, or unnecessary to protect. However, we believe their claims are spurious and that the technical capacity and federal policy precedents are available now to add the essential consumer privacy protections to the "meaningful use" criteria and quality matrices.

Recommendations:

1) When matrices and recommendations are presented to the Committee as a whole, such information must be made available to the public a minimum of two (2) days prior. Alternatively, time must be allotted to receive public comment BEFORE the Committee approves such recommendations, so that the Committee could better understand and aggressively debate consumers' proposals. We understand formal requests for public comment published in the Federal Register are part of the formal rulemaking process that will take place after the Committee makes final recommendations. Nevertheless, we believe that our proposals and concerns should be openly addressed and debated during the deliberative stage of the Committee's work. Even an informal solicitation of public comments prior to decision making would greatly improve this process.

2) We urge you to work directly with our broad–based Coalition and any other consumer health privacy advocacy organizations accountable to the public.[1]

<u>Greater Attention to Protecting and Enabling Privacy</u>

Generally speaking, the discussions from this Committee are driven from an industry (health care and information technology) point of view primarily. Providers' points of view are secondary in the process, and patients seem to fall into the mix last – the caboose -- if at all. We strongly urge a complete reversal of these perspectives. *First, the patient's needs and rights must guide policy. Second, these needs and rights must be addressed on the front end, not the back.*

The Coalition hears from our far-reaching constituencies that having control over who can access and use their most personal information, or privacy, is their paramount concern. We

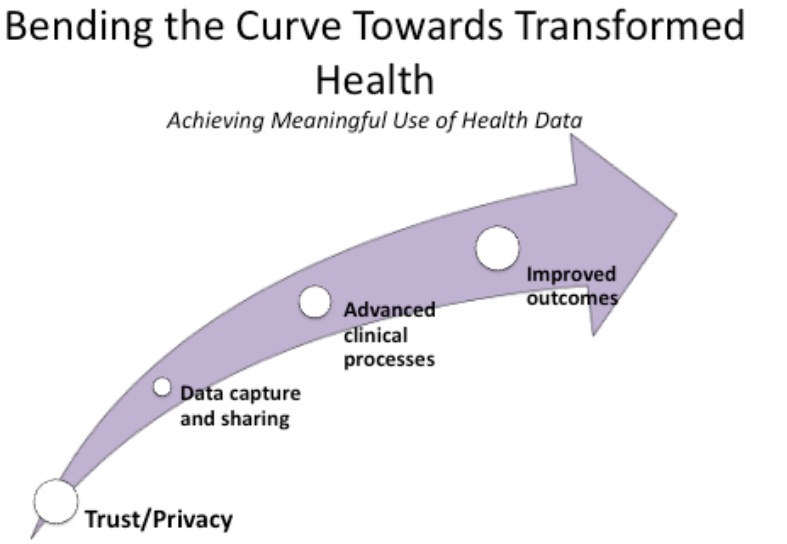
[1] We note the language creating the HIT Policy Committee requires it to "serve as a forum for broad stakeholder input" and it "shall ensure an opportunity for the participation …of outside advisors, including individuals with expertise in the development of policies for the electronic exchange and use of health information, including in the areas of health information privacy and security. . . "

cannot reach the ultimate vision for HIT, nor meet the key goals to improve quality, safety and efficiency, engage patients and families, improve coordination, improve public health and reduce disparities, and ensure privacy and security protections, if we begin with what is easy rather than what is crucial. While ensuring privacy may be challenging, it is workable and more importantly, essential.

First, while we certainly appreciate the need for gradual implementation, the key technology features needed to ensure public trust, items such as segmentation, consent management and audit trails need to be addressed now. Likewise, policy matters such as how Americans can control their information and how they can opt-out of systems are not a matter that can or should be dealt with later. Clearly Committee member Dr. Sweeney heard this concern, as did other members.

Second, the issue of privacy is raised countless times during the Committee's meetings; but we have yet to see any comprehensive or cross-cutting attention given to privacy in the Committee's recommendations. The few privacy measures will not be addressed until 2015. Further, the Committee does not have an agreed upon definition of privacy. "Privacy" is an easily used term, often mixed with "security" or "confidentiality" causing confusion and making it impossible to measure progress. Privacy is essential for quality healthcare; it should be a quality metric measured as part of the "meaningful use" criteria.

Finally, we note that quality healthcare depends on privacy[2]. In the slide used for the Meaningful Use Workgroup Presentation entitled, "Bending the Curve Towards Transformed Health", the starting point for the arrow in the slide is "data capture and sharing." Again, having TRUST is essential before patients are willing to give providers any data to capture. Trust and privacy (and security) need to be the starting point; we suggest an alternative approach:



[2] "The **entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life." "An assurance of privacy of health information is **necessary to secure effective, high quality health care.**" 65 Fed. Reg. at 82,467

Accurate and complete information cannot be obtained by force. We know from the California HealthCare Foundation's National Consumer Health Privacy Survey (2005) that 12.5% of the population avoids their regular doctor, asks doctors to alter diagnoses, pays privately for a test, or avoids tests altogether due to privacy concerns. If we do not restore patient control over PHI, we can expect electronic health data to have error and omission rates of 12.5 % or more. The breakthroughs and benefits possible with technology-enhanced research will never be reached with such a high rate of errors and omissions.

The lack of privacy drives patients away from doctors. We know from HHS' findings that every year 600,000 people refuse early diagnosis and treatment for cancer and 2,000,000 avoid treatment for mental illness because of fears their treatment will not be private[3]. The lack of privacy causes death, suffering, and, most importantly, bad outcomes. This is happening right now and will only get worse as we migrate to electronic health records. Given that 68% of the public have little confidence that electronic health records will remain confidential, the Committee needs to act immediately to ensure the public's fears are alleviated by policies and standards that ensure EHRs can be trusted.[4]

Recommendations:

1) The Committee should adopt a definition of privacy. We urge adoption of the NCVHS definition of health information privacy: "*individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."*

2) Ensure that <u>the patient perspective</u> is prominently represented and, in fact, heard in <u>each</u> of the three workgroups. The Coalition is happy to assist the Committee with feedback for each workgroup as recommendations are developed to ensure privacy is addressed.

3) Reject any recommendations that call for collecting all "comprehensive data available" and to "record all available data" without first laying the groundwork for privacy and ensuring consumer control and informed consent.

<u>Approved "Meaningful Use" Matrix</u>

In addition to our previous comments about meaningful use, we note that we were encouraged to see among the 2011 objectives for Privacy and Security in the Meaningful Use Matrix (7.10.09) compliance with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Framework).

This Framework includes the strong privacy principle that "*Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information."* Compliance with the Framework is stated as a 2011 objective. Yet there does not appear to be any actual requirement for this key privacy policy, nor any way to verify compliance. We applaud many of

[3] 65 Fed. Reg. at 82,779 and 82,777.

[4] See the survey data from the Employee benefit Research Institute and Mathew Greenwald & Associates presented by the Privacy and Security Work Group to the HIT Standards Committee on July 21, 2009

the principles and policies set forth in the Framework but note that they are not all being addressed as part of the “meaningful use” matrix.

The key critical function needed in every EHR to enable "meaningful use" of EHR data is the ability of patients to control the uses and disclosures of all protected health information (PHI). We recommended previously that the Committee adopt existing open source technology that enables detailed control over disclosures as a baseline model or floor for consent technologies. The open source technology we recommended has the added advantage of enabling robust segmentation, so adoption of the functions in this technology as a minimum standard for privacy and segmentation would allow these two critical consumer protections to be quickly implemented as requirements for “meaningful use” in EHRs. We believe that ultimately, certification of systems for “meaningful use” that do not require consumer control over data fail to meet public’s expectations.

With regard to measures and objectives for the accounting of disclosures for treatment, payment and healthcare operations, we remind the Committee that ARRA requires no later than 2013 for EHRs purchased after January 1, 2009 audit trails be in place. For these “new” EHRs, an audit trail is required by 2011, and no later than 2013. As such, it is essential that the Committee develop the needed policies now.

Acknowledging the time needed for implementation, we also urge the Committee to recommend policies that will guide the development of new privacy-enhancing technologies. Early attention is needed for the successful implementation of segmentation and consent management features. If these protections are placed on the backburner, EHRs will be purchased and used over the next four years without those critical features and make retrofitting for privacy a burden.

Recommendations:

1) Include compliance with the policies and principles in the Nationwide Privacy and Security Framework as a 2011 measure so that these principles are both required and verified. The Committee could delay some portions of this framework until 2013, but 2011 should be the goal.

2) Add minimum standards for basic consent management tools to the “meaningful use” criteria. We recommend that EHRs must include consent and segmentation capabilities at least as detailed and specific as those in the open source electronic consent controls developed by the NDIIC, as recommended in our previous comments.

3) Add consumer control over PHI in EHRs as a “meaningful use” quality measure, tracked and improved over time.

4) Include objectives for audit trails, segmentation and consent management in 2011 and 2013 as part of the meaningful use matrix. Even if these objectives are not required for federal funds (for segmentation and consent management), the steps towards 2015 implementation should be articulated as early as possible.

Our Coalition is committed to working closely with you and the HIT Policy Committee to ensure patients and consumers are represented and that we achieve progress by protecting privacy. Thank you for your time and consideration. Please do not hesitate to contact us.

Sincerely,

The Coalition for Patient Privacy

American Association of People with Disabilities
American Civil Liberties Union
Center for Digital Democracy
Clinical Social Work Association
Consumer Action
Electronic Frontier Foundation
Electronic Privacy Information Center
Just Health
Multiracial Activist
National Center for Transgender Equality
National Coalition for LGBT Health
National Coalition of Mental Health Professionals & Consumers
Patient Privacy Rights
Private Citizen
Tolven, Inc.
U.S. Bill of Rights Foundation

For more information, please contact:

Ashley Katz
Executive Director, Patient Privacy Rights
akatz@patientprivacyrights.org (512) 732-0033