

**Opening Remarks
HIT Policy Committee
September 18, 2009**

by

John Houston

Vice President, Privacy and Information Security & Assistant Counsel
University of Pittsburgh Medical Center

I appreciate the opportunity to speak to the committee on this important topic. As a co-chair of the NCVHS committee on, Privacy, Confidentiality and Security, as well as being responsible for privacy and information security for a large health system, I am extremely sensitive to health IT privacy and security considerations. I will keep my comments brief, as I believe that the value is in the dialog that will ensue.

As background, NCVHS is in the process of finalizing recommendations regarding the privacy of Personal Health Records. Additionally, NCVHS has made a number of recommendations regarding the privacy in the NHIN and data stewardship. The later recommendations were consolidated in two separate reports that were published by NCVHS and are available at <http://www.ncvhs.hhs.gov/privacyreport0608.pdf> ("Recommendations on Privacy and Confidentiality, 2006-2008") and <http://www.ncvhs.hhs.gov/080424rpt.pdf> ("Enhancing Protections for Uses of Health Data: A Stewardship Framework").

Meaningful Use

As a general concept, I believe that the measurement of "meaningful use" is an extremely daunting proposition. Not only do criteria need to be established, but the criteria need to be reasonably measurable across the thousands of providers in the United States. Therefore, the criteria need to be quantifiable and of a reasonable number.

Privacy

Privacy is a societal value. Each and every one of us has a good faith opinion as to what privacy means. From my work on NCVHS and as a privacy officer, I have found that these good faith positions vary dramatically. But, as consumer confidence is based on the basic proposition that a patient's health information must be kept confidential, the concept of "meaningful use" needs to encompass privacy.

However, I find it difficult to describe a set of specific and quantifiable metrics that could be used to measure privacy. If an organization meets "X", "Y" and "Z" requirements, does it have privacy? While one may argue that privacy may not exist, even if an

organization fully complies with the HIPAA privacy rule, I believe that the HIPAA privacy rule provides a framework for ensuring a reasonable level of privacy protections.

Therefore, the best method to ensure that appropriate privacy protections exist may be to ensure that the covered entity complies with HIPAA (and appropriate enforcement through OCR).

Security

HIPAA does not attempt to define specific technologies or dictate how a covered entity implements security. Rather, HIPAA recognizes that technologies evolve, new threats emerge every day and covered entities' operations may dramatically differ (based on size, organizational dynamic, geographic reach, etc). As such, I am unsure what the best method is to establish a set of quantifiable security criteria for measuring "meaningful use". As evidenced by the fact that your committee recently released a number of Privacy and Security recommendations for comment, there are a wide variety of security standards that may have applicability.

In the context of "meaningful use", security (like privacy) may be most effectively addressed through compliance with HIPAA (and appropriate enforcement through OCR). However, assuming that the committee wants to establish specific security criteria, I would caution that security criteria need to be flexible.

Data Exchange - NHIN

As I previously indicated, NCVHS has made numerous recommendations regarding privacy in the NHIN, as well as enhancing data stewardship. These recommendations were the result of substantial testimony and deliberation. I hope that they can assist the committee in forming its privacy policy recommendations.

I would like to make a number of additional comments as well. With respect to data exchange, any discussion regarding uses (including secondary used), disclosures and data stewardship must be done in the context of transparency, audit and accountability.

Again, using HIPAA as the benchmark, Covered Entities are expected to have processes in place to ensure that:

- Information is appropriately used and disclosed.
- Suspected inappropriate use is investigated.
- Patient authorization is secured for certain non-TPO uses.

With the expectation that health information will be made widely available, it is vital that analogous oversight processes be established at a macro level. From my perspective, this is an area in need of great attention. Popular or not, I do not believe that proper oversight can be accomplished without a centralized organization to provide active coordination and policing, as well as to act as an ombudsman.

By example, the central organization would be responsible for:

- Performing entity “credentialing” – entities participating in the exchange network should be subject to a rigorous process to ensure that they are prepared to meet their obligations prior to being able to access health information, whether on an identifiable or de-identified basis. Participating entities would be those who access information for treatment, as well as non-treatment purposes (such as research, quality assurance, public health, law enforcement and secondary uses)
- Providing mechanisms for patients to see where their information was disclosed.
- Assist in investigating suspected inappropriate disclosures.
- In the event that patients are provided with the ability to select which information can be exchanged, providing the infrastructure to allow the patients to make such selections.

I also believe that there are still regulatory issues that need to be addressed:

1. State preemption provided for in HIPAA will make it difficult to exchange information on a national basis.
2. HIPAA does not apply to all entities that may exchange information.

I hope that my comments are of value and I look forward to a lively discussion.