

**Privacy and Security Solutions for Interoperable Health Information Exchange  
National Conference  
March 5-6, 2007**

**The conference in brief:**

- This was the first opportunity for all 34 states who received grants under the Health Information Security and Privacy Collaboration (HISPC) project to meet as one group, and report back on the Status/Progress of each respective project.
- The conference was attended by more than 350 people. There were attendees from State's other than the 34, as well as representatives from consulting firms, and other health care related entities.
- The conference was divided into **four** tracks; Consent Issues, Data Security and Quality, Legal and Regulatory Issues, and Interpreting and Applying HIPAA.

**Welcome and Opening Remarks**

- A reoccurring theme throughout the conference was the importance of “trust” in the whole process of achieving a solution. For instance, the following messages were delivered by the opening speakers; *“Without trust and collaboration, this won’t happen”*, and *“The key to achieving standards is not technology, it is trust.”*
- An additional \$15 million in grants during FFY 2008 will be awarded to continue HISPC efforts.
- There was a lot of energy put into why this (electronic health records) are important. As an example, there is a drug that could save 14,000 people from dying from lung cancer each year. The problem is there is no way to systematically identify patients who could benefit from this drug. An electronic health record would, in part, solve this dilemma.

**Highlights of the Nationwide Summary of the Assessment of Variation (part of opening session)**

- Existing paradigm for privacy and security protection does not accommodate consumer participation in health information exchange.
- Three key assumptions are being made; decisions on how to protect EHR's should be made at local level, discussions need to happen to understand “current landscape” (variation), and stakeholders (consumers) must be involved.
- Project goals – Identify variation in practices, policies, and laws that inhibit creating/sharing EHR's, Develop solutions, and develop plan to implement.
- Sources of Variation –
  - What regulation applies (HIPAA v 42 CFR pt 2),
  - State privacy law,
  - What is Patient consent,
  - What is the “minimum necessary standard” to disclose EHR's,
  - Cultural and Business Issues,

- Technical issues (e.g. data standards, authorization protocols).

### **Session 1C: State Laws: Finding and Interpreting Them (Legal and Regulatory Track)**

- This is an assessment process each state needs to go through. The approaches were mostly the same, namely to identify barriers that inhibit the exchange of EHR's.
- An assessment process can be very labor/time intensive;
  - “500 years of codified law” (New Mexico),
  - “60 chapters of State Law” that that addressed exchanging health care information (Florida),
  - Florida has a three year plan to rectify.
- Solutions to these issues appeared to be different;
  - Identify all laws/regulations and change each one,
  - NM had different strategy – new legislation to protect/share EHR's in an electronic form with references to existing law. “Easier to get through Legislative process.”

### **Session 2B: Access and Auditing Access (Data Security and Quality Track)**

- This session was primarily a report on the technical architecture platform that Connecticut was pursuing.
- From the questions entertained by the presenter's, it appears to be on of the four conference tracks that might be the least developed.
- Who, What, where, when, and why all create different access/security issues. Policies are needed for each. Different users have different access needs.
- What should the data model be (distributed or centralized)? In a distributed model owners would have access to their data. In a centralized model, access issues creep in. In a centralized model, who becomes the “trusted” keeper of the data? Is it a RHIO?
- What is the role of government in a centralized model? In a distributed model?

### **Session 3B: Trust in Security (Data Security and Quality Track)**

- Utah's presentation focused on the sharing of data between State agencies.
- “Existing cultural barriers make the sharing of any PHI among programs taboo.”
- There is sharing on a need to know, case by case basis. Almost no sharing on a scale that would improve public policy objectives (e.g. detection of emerging health threats).
- Policy challenges;
  - Define acceptable use,
  - “System” to authorize access (role based e.g. Dr. has access to?);
  - “Break the Glass” provisions. What happens when an 85 year old comes into the ER suffering from a heart attack, and the ER doesn't have access to her complete EHR, and cannot contact the entity who has the information the ER needs to accurately treat the patient?
- California's presentation focused on their plan for implementation of EHR's.

- Establish a group specific to privacy and security to develop (table below). This seems to be a good synopsis of issues to address for success:

Infrastructure	Privacy and Security Oversight – Oversee resolution of HIE privacy and security issues.
Technology	Technology Committee – Identify security standards.
Law and Liability	Legal Committee – Identify privacy and security law/issues that affect HIE.
Rights and Responsibilities	Operational Procedures Committee – develop standard privacy guidelines and procedures.
Levels of Knowledge	Guidance & Education Committee – Improve patient education about their rights and records.
Lack of Trust	Resolve through collaboration activities

- California’s plan will take until 2014:
  - 2007 – set policies, develop governance structure,
  - 2008-2009 – publish principles, minimum required standards,
  - 2010 – publish “gold standard” for interoperability,
  - 2012 – Advance, enforce, proliferate,
  - 2014 – HIE fully operable.

#### **Session 4C: Governance (Legal and Regulatory Track)**

- California’s presentation was a continuation of their “model” of implementation (see above section).
- This session was really about what role does each state government play in developing EHR’s, and how they set up administratively to handle their task.
- CA issue – Who does the privacy and Security Oversight Board report to?
- Washington pined that the technical know how, standards, and solutions already existed. A barrier (in their eyes) was that there was no incentive to pick a particular set of standards. It reminds me of trying to decide where to go out to eat with a large family....
- Washington’s dilemma was where does the administrative/oversight body reside;
  - Under the auspices of an existing legislatively approved and funded effort,
  - Organize via a public agency mandate, or
  - Voluntarily collaborate with existing public/private entities.
- Washington adoption incentives;
  - “Safe Harbor” status,
  - Limitation of damages,
  - Requires legislation and vested regulatory authority.

#### **Session 5C: Implementation (Legal and Regulatory Track)**

- There wasn’t a lot of new information presented.

- Utah – Even though a majority of clinical records are in paper form, most claims data is processed electronically.
- Technical challenges exist with paper or electronic exchange. Accessing appropriate information, lack of search capability, authentication/verification of requestor/user. Again, establishing EHR's is not a technical issue.
- Consumers should have the right to;
  - Determine who views their information,
  - Revoke the right,
  - Request an audit,
  - Be notified of any violation.
  
- The above is necessary to gain consumer confidence (trust issue).
- It appears that Utah is going to try and leverage the work done UHIN (Utah's RHIO). Apparently there are some standards developed (Encryption, User authentication).