HISPC-Illinois II

The Public-Private Partnership Moves Forward on Privacy and Security

RECOMMENDATIONS ON PRIVACY AND SECURITY POLICIES

For Consideration by the Governance Structure of an Illinois State-Level Health Information Exchange

The public-private partnership that came together during the work of the Electronic Health Records Taskforce (EHRT),[1] is intent on facilitating the creation of a state-level health information exchange (HIE) by providing recommendations on privacy and security policies to its governance structure. The Health Information Security and Privacy Collaboration (HISPC) – Illinois II project (hereafter referred to as HISPC – Illinois II) has been developed to accomplish this task.

HISPC – Illinois II determined that three overarching principles ~~should~~shall form the basis for the privacy and security policies of a state-level HIE. These principles are:

- A state-level HIE ~~must~~shall meet all applicable federal and state privacy and security laws.

- Privacy and security policies of a state-level HIE shall be understandable and clearly explain to the public how health information is to be protected.

- The governance structure of a state-level HIE ~~must~~shall adopt privacy and security policies consistent with privacy and security standards promulgated by the Nationwide Health Information Network (NHIN).

Formatted: Tabs: 0.79", List tab + Not at 0.5"

Formatted: Tabs: 0.75", List tab + Not at 0.5"

Formatted: Tabs: 0.96", List tab + Not at 0.5"

[1] Created by Public Act 94-646, effective Aug. 22, 2005. Sponsors: Representatives Julie Hamos - Elizabeth Coulson – Sidney Mathias - Paul D. Froehlich - Sara Feigenholtz, Mike Boland, Mary E. Flowers, Richard T. Bradley, Coreen M. Gordon, Elaine Nekritz, Karen May, Cynthia Soto, William Davis and Constance Howard; Senators William R. Haine - Steven J. Rauschenberger - Jeffrey M. Schoenburg. Report issued December 27, 2006

The first principle is an obvious and easily state guideline, however, the governance structure of a state-level HIE will have to filter through a myriad of interpretations as to how state and federal law privacy and security laws are to be applied to HIE.

Public support of HIE is essential for it to become an effective tool to improve health care. That support cannot be achieved if the public does not understand or trust how the state-level HIE will safeguard of personal health information.

One of the major functions of a state-level HIE will be to connect local/regional HIEs[2] and health care providers with the NHIN. "To participate in the NHIN, an organization will be required to use a shared architecture, adhere to adopted standards and provide certain core services."[3] Ensuring the state-level HIE's privacy and security policies are consistent with the NHIN standards will be a major task facing the governance structure. Because the NHIN has yet to establish such standards, HISPC – Illinois II can only focus on general issues.

Following are the suggestions and recommendations of HISPC – Illinois II on privacy and security policies that ~~should~~shall be considered by the governance structure of a state-level HIE.

I. – Privacy and Security Philosophy

The governance structure of a state-level HIE ~~should~~shall include a statement regarding its privacy and security philosophy. This philosophy statement is the first opportunity for the exchange to express its commitment to protecting patient health information. Building a level of trust with the public and providers will begin with a strong and clear statement from the state-level HIE. It is also important for entities connecting to the state-level HIE to understand the seriousness ~~to~~ with which they ~~must~~shall address privacy and security.

[2] Frequently referred to as a Regional Health Information Exchange (RHIE), Regional Health Information Organization (RHIO) or Sub-network organization.

[3] Gartner, *Summary of the NHIN Prototype Architecture Contracts - A Report for the Office of the National Coordinator for Health IT*, May 31, 2007, page 4, http://www.hhs.gov/healthit/healthnetwork/resources/summary_report_on_nhin_Prototype_architectures.pdf

- The philosophy shall convey a strong commitment to protecting information, but shall not imply a guarantee.
- To promote the goal of building trust, the philosophy shall include a statement of commitment to patient education and assuring that patients are fully informed with regard to the HIE
- The philosophy shall apply to all information within the HIE, not just health information

Formatted: Bullets and Numbering

II. – Patient Rights with Respect to Information Privacy and Security

Formatted: Keep with next

The EHRT recommended that the state-level HIE use a federated model in the development of the exchange process. Under this model, with the possible exception of data needed for public health or other governmental purpose, patient records are not uploaded into a central repository or database maintained by the state-level HIE. Participating providers only upload those data elements needed by the state-level HIE for entry into a master patient index. When a legitimate request for patient health information is received, the state-level HIE will search the master patient index to identify all locations where the patient has data. It will then request electronic copies from providers holding the records and transmits the information to the requesting provider. In the context of this model, HISPC – Illinois II recommends the state-level HIE adopt the following:

Comment [Eb1]: Concern/questions were raised with regard to this federated model – 1) How does this work in terms of treatment, it seems as though there would be a delay/time-lag between a request for records and delivery of records that could impair treatment; and 2) how does this work with research needs – how can data regarding public health be gathered without clinical records

- The HIE shall send patients notice of their rights on a periodic and regular basis.

Formatted: Bullets and Numbering

- A patient has the right to review their own health information contained in the HIE.

Formatted: Bullets and Numbering

- Patients shall be informed of their rights with regard to mitigation in the event of a privacy or security breach.

Formatted: Bullets and Numbering

- All participants in the state-level HIE shall guarantee that patients have the following rights.

Formatted: Keep with next

Formatted: Tabs: 0.79", List tab

Formatted: Bullets and Numbering

Formatted: No bullets or numbering

- A patient's personal health information shall only be released in accordance with state and federal law. Patients shall be informed of protections available under current law.

- A patient has the right to restrict the release of personal health information to the state-level HIE, except such information required to be reported under state or federal law.

-

- The treatment of a patient shall not be conditioned on the release of the patient's personal health information.

~~*III. – Protection of Caregiver Information*~~

[Recommend the deletion of this section. Caregiver information should not be at issue in treatment information.]

IV. – The Privileges and Obligations of Researchers

The development of policies on researchers will require a better understanding of the architecture of the state-level health information exchange. At a minimum, HISPC – Illinois II recommends that these policies include:

-

- Defining when a research request requires additional patient consent.

- Defining "researcher"

Formatted: Indent: Left: 0.5", Tabs: 0.75", List tab + Not at 0.5"

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Indent: Left: 0.54"

Comment [Eb2]: Discussion/concern regarding whether this is an opt in/opt out program

Formatted: Indent: Left: 0.5", Tabs: 0.75", List tab + Not at 0.5"

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.5"

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Indent: Left: 0.5", Tabs: 0.75", List tab + Not at 0.5"

Comment [Eb3]: The group felt this was important, providers need to trust the HIE too in order for it to be viable. Patrick and Ted will draft something addressing the uses of provider information in the HIE, e.g. "blame free" uses; the information id for improving treatment and protecting the public's health, not for litigation, enforcement, discipline

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

- When and how data that includes identifiers can be shared with researchers and a definition of “de-identified” data.

Formatted: Bullets and Numbering

- Requirements for how researchers ~~should~~shall protect the information in their custody.

- Defining researcher responsibilities to notify recipients of information of the protection requirements.

- The researchers’ expectation of accurate information. The policy for ensuring that researchers are made aware of the sources and the accuracy of information being provided ~~should~~shall be considered.

- Requirement relating to the disclosure of information resulting from the research.

~~*V. – The Rights of Society*~~

[Recommend the deletion of this section.]

~~*VI. – Collection of Information*~~

[Recommend the deletion of this section.]

VII. – Retention and Destruction

The state-level HIE shall adopt a retention and destruction policy consistent with state and federal law. The policy ~~must~~shall provide for preservation of the records during the migration to new technologies.

VIII. – Information Privacy and Security Program

The state-level HIE ~~must~~shall adopt policies ~~describe~~ describing the staff roles for a privacy and security program. This shall include responsibilities for the periodic review and maintenance of the information privacy and security policies.

- The approach to risk management shall be described in the policy
- The HIE shall have a staff position that is accountable for facilitating adherence to the privacy and security policies (e.g. privacy and security officer).

Formatted: Bullets and Numbering

IX. – Accountability and Responsibilities

The state-level HIE ~~should~~shall define specific responsibilities and accountability for information privacy and security. These include:

- Who is responsible for oversight and monitoring of the program (see above)

Formatted: Font: 10 pt

- Who is responsible for reporting violations, at both the participant and state-level HIE levels.

Formatted: Bullets and Numbering

- Who is responsible for imposing disciplinary measures on state-level HIE employees who violate privacy and security laws or policies.
- Who is responsible for imposing sanctions on participants for violations of privacy and security laws or policies.

X. – Access to Information

The state-level HIE ~~must~~shall define who has access to patient-specific information. These policies ~~should~~shall specify that access to the organization's business records will be based on assigned job responsibilities. These policies shall identify classes of information and specify who has access to information in specific classes.

~~*XI. – Classification of Information*~~

[Recommend the deletion of this section.]

XII. – Records of Access

For auditing and monitoring to assure information security, t~~T~~he state-level HIE shall maintain records/logs of who accesses patient information. The policies ~~should~~shall specify how long the access records ~~should~~shall be maintained.

XIII. – Disaster Recovery/Business Resumption Plans

The state-level HIE ~~should~~shall develop a policy for responding to disasters.

XIV. – Information Privacy and Security Awareness Training

Policies ~~should~~shall be developed regarding information privacy and security awareness-training for state-level HIE employees and participants.

~~*XV. – Monitoring and Auditing*~~

[Recommend the deletion of this section.] (covered in 8/9/12)

XVI. – Remedies

The state-level HIE ~~must~~shall adopt policies on how privacy and security violations are to be remedied. To ensure the enforceability of these policies on participants in the HIE, the remedies need to be included in the participant agreements.