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 form the basis for the privacy and security policies of a state-level HIE. These principles are:

- A state-level HIE must 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 adopt privacy and security policies consistent with privacy and security standards promulgated by the Nationwide Health Information Network (NHIN).

[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 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 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 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 which they must 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

II. – Patient Rights with Respect to Information Security

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:

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

- A patient's personal health information shall only be released in accordance with state and federal 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.
- Requirements for how researchers should 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 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 provide for preservation of the records during the migration to new technologies.

VIII. – Information Security Program

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

IX. – Accountability and Responsibilities

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

- Who is responsible for reporting violations, at both the participant and state-level HIE levels.
- 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 define who has access to patient-specific information.

These policies should specify that access to the organization's business records will be based on assigned job responsibilities.

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

[Recommend the deletion of this section.]

XII. – Records of Access

The state-level HIE shall maintain records/logs of who accesses patient information. The policies should specify how long the access records should be maintained.

XIII. – Disaster Recovery/Business Resumption Plans

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

XIV. – Information Security Awareness Training

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

~~*XV. – Monitoring and Auditing*~~

[Recommend the deletion of this section.]

XVI. – Remedies

The state-level HIE must 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.