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

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

The first principle is an obvious and easily stated 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.

---

[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

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 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 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 with which they shall address privacy and security.

- 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.

II. – Patient Rights with Respect to Information Privacy and 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, 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:

[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 state-level HIE governance structure shall post a notice on its Web site of the rights patients have under law and the policies of the HIE regarding their personal health information.

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

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

- 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. Patients shall be informed of protections available under current law.

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

III. – Protection of Health Care Provider Information

The information available through the state-level HIE should be used only for public health and patient care purposes. To encourage health care provider participation in the HIE, the state-level HIE should adopt practices, policies and procedures that limit the availability of HIE information exclusively to these purposes. Accordingly, the state-level HIE must adopt practices, policies and procedures that ensure the following:

- None of the HIE information made available to the public or a researcher may contain information identifying a patient or health care provider unless authorization has been given by the patient.

- HIE information shall not be available to anyone for use in any civil, criminal, or administrative proceeding against a health care provider.

- Under no circumstances shall the HIE disclose information to the public or a researcher that is confidential under Illinois Medical Studies Act.

- None of the HIE information shall be discoverable or admissible in any legal or administrative action for the purpose of establishing a standard of medical or health care practice.

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 "research" and "researcher."
- Defining "de-identified" data.
- Whether data that includes protected health information can be made available to researchers and if so how that data will be shared .
- Defining when a research request requires patients to sign an "Authorization for Use and Disclosure of Protected Health Information for Research."[4]
- Requirements for how researchers 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 shall be considered.
- Requirement relating to the disclosure of information resulting from the research.

V. – Retention and Destruction

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

VI. – Information Privacy and Security Program

The state-level HIE shall adopt policies 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 assign responsibility and accountability to a staff role for facilitating adherence to the privacy and security policies (e.g. privacy and security officer).

[4] Form recommended by the HISPC-IL Legal Work Group for use in obtaining a patient's "authorization" for the use of protected health information.

VII. – Accountability and Responsibilities

The state-level HIE 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).
- 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.

VIII. – Access to Information

The state-level HIE shall define who has access to patient-specific information. These policies shall specify that access to personal health information will be based on assigned job responsibilities. These policies shall identify categories of information and specify who has access to information in specific classes of users.

IX. – Records of Access

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

X. – Disaster Recovery/Business Continuity Plans

The state-level HIE shall develop a policy for responding to disasters. This shall include, at a minimum:

- Data backup plan
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revision plan
- Applications and data criticality analysis

XI. – Information Privacy and Security Awareness Training

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

XII. – Remedies

The state-level HIE 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 shall be included in the participant agreements.