
# Privacy and Security Work Group

## Draft Privacy & Security Policies & Recommendations


## HISPC

- The Health Information Security and Privacy Collaboration (HISPC) is a federal initiative to study privacy and security issues related to health information exchange (HIE)
- HISPC's phase 1 goals were to:
  - identify both best practices and challenges
  - develop consensus-based solutions that protect the privacy and security of health information, and
  - develop implementation plans to implement solutions.
- 33 states and 1 territory participated in the collaboration


# HISPC-Illinois
## Implementation Recommendations

1. Develop systematic, comprehensive approach to promoting HIE
2. Adopt universal standard for patient identification
3. Develop standards for consistent and available privacy and security expertise for organizations.
4. Establishment of core competencies for staff education and training in electronic health information, privacy and security.
5. Develop educational materials for consumers
6. Extend and promote, national Stark, e-prescribing and anti-kickback relief regulations.
7. Provide recommendations for use of multidisciplinary teams in the acquisition of new IT solutions.
8. Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts.


# HISPC Phase II

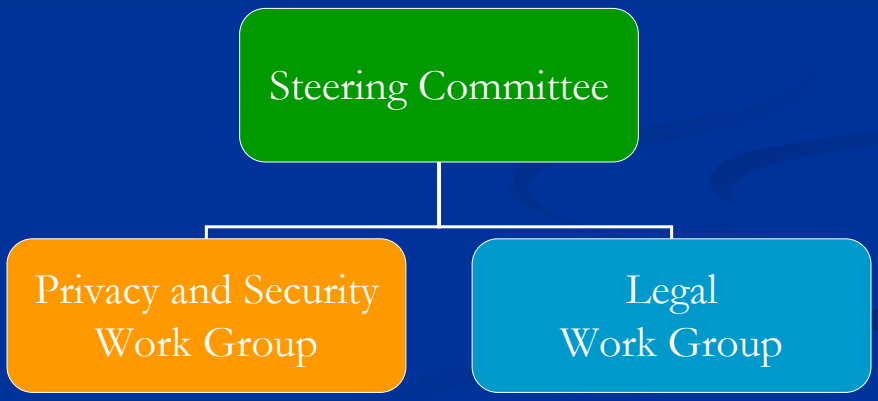
The purpose of phase 2 is to implement proposals produced during the initial phase of the project.


# HISPC-Illinois II
## Project Proposal

- The priority for Illinois as HISPC enters phase 2 is to move the public-private partnership outlined in the Electronic Health Records (EHR) Taskforce report and supported in the HISPC-Illinois State Implementation Plan forward in the areas of privacy and security. "Solution 8," of the "State Implementation Plan – Illinois" provides for the "lead state agency/organization" to have expertise in privacy and security to guide state activities.

- Consistent with the spirit of that implementation solution, HISPC-Illinois II will set up an expert work group to prepare draft privacy and security policies and recommendations for consideration by the governance structure of a state-level health information exchange (HIE). Another work group will prepare a uniform patient EHR/HIE consent form for possible use by the state-level HIE, clinicians, health care facilities and other providers.


# HISPC-Illinois II Structure




# Privacy & Security Work Group

Develop draft privacy and security policies and recommendations for consideration by the ILHIN Board of Directors.

- Develop an outline of privacy and security issues to be included in the "Draft Policies and Recommendations document."
- Prepare a draft of the "Draft Policies and Recommendations document" for review by stakeholders.
- Finalize the "Draft Policies and Recommendations document."


# Definitions of Privacy, Confidentiality and Security

- **Privacy** – an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.
- **Confidentiality** – refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.
- **Security** – refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.[1]

[1] Extracted from "Privacy and Confidentiality in the Nationwide Health Information Network," National Committee on Vital and Health Statistics, June 2006, http://www.ncvhs.hhs.gov/060622lt.htm.


# Definition of Privacy and Security Policies

- **Policies** describe how the organization plans to protect the [organization's] tangible and intangible information assets. Policies include generalized requirements approved at the [organization's] executive level that indicate a course of action to personnel who must make decisions.[2]

[2] Extracted from "Managing Information Privacy & Security in Healthcare: A Primer on Health Information Security," By Greer Stevenson, part of the *HIMSS Privacy and Security Toolkit,* Healthcare Information and Management Systems Society, April 2007, page 5, http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D03_Security_Primer.pdf


# Work Plan

- **First Meeting**
  - Review the work group task.
  - Discuss approach to achieve the work group task.
  - Discuss and adopt a consensus outline of the privacy and security issues to be included in the "Draft Policies and Recommendations" document.
  - Discuss work assignments for next meeting – select author(s) to prepare draft policy paper for each outline dot point.
  - Set meeting schedule
- **Second Meeting**
  - Review draft policy papers.
  - Discuss work assignments for next meeting – revising policy papers to address work group comments.


# Work Plan Continued

- **Third Meeting**
  - Discuss and approve a draft of the "Draft Policies and Recommendations" document for review by stakeholders.
- **Fourth Meeting**
  - Discuss stakeholder comments on the draft "Draft Policies and Recommendations" document
  - Discuss work assignments to make revisions to address concerns or questions.
- **Fifth and Final Meeting**
  - Discuss and finalize the "Draft Policies and Recommendations" document.


# Policy Outline[3]

1. Philosophy for the Protection of Information
2. Patient Rights with Respect to Information Security
3. Protection of Caregiver Information
4. The Privileges and Obligations of Researchers
5. The Rights of Society
6. Collection of Information
7. Retention and Destruction
8. Information Security Program

[3] Extracted from "Developing Policies, Procedures, and Practices - Introduction ," By Ted Cooper, MD, part of the *HIMSS Privacy and Security Toolkit,* Healthcare Information and Management Systems Society, January 2007, page 2, http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D37_Introduction_to_P-Ps.pdf


# Policy Outline Continued[3]

9. Accountability and Responsibilities
10. Access to Information
11. Classification of Information
12. Records of Access
13. Disaster Recovery/Business Resumption Plans
14. Information Security Awareness Training
15. Monitoring and Auditing

[3] Extracted from "Developing Policies, Procedures, and Practices - Introduction ," By Ted Cooper, MD, part of the *HIMSS Privacy and Security Toolkit,* Healthcare Information and Management Systems Society, January 2007, page 2, http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D37_Introduction_to_P-Ps.pdf


# Issues to Consider

What should or should not be included in Illinois' Privacy and Security Policies


# Policies to Reflect Functionality

**The state-level health HIE is to serve as the bridge between the Nationwide Health Information Network (NHIN) and Illinois regional health information organizations and health care providers.**

- To participate in the NHIN, the state-level HIE will be required to adhere to adopted standards.
- Illinois policies will have to be developed to reflect or prevent a conflict with those standards.


# NHIN Requirements[4]

- Secure operation in all activities related to the NHIN
- Protect the confidentiality of personally identifiable health information as it is used by those who participate in the NHIN
- Reconcile patient and provider identities without creating national indices of patients
- Provide local registries that may be used, when authorizations permit, to find health information about patients
- Support the transfer of information from one provider or care delivery organization in support of collaborative care
- Support secondary uses of data while protecting the identity of patients to the degree required by law and public policy

[4] Extracted from Gartner, "Summary of the NHIN Prototype Architecture Contracts - A Report for the Office of the National Coordinator for Health IT," May 31, 2007, page 25, http://www.hhs.gov/healthit/healthnetwork/resources/summary_report_on_nhin_Prototype_architectures.pdf


# Policies to Address Public Trust

The state-level HIE privacy and security policies need to provide assurances to the public that personal health information will not be misused or abused.

- Numerous organizations have developed recommendations on how best to protect health information
- Recommendations from some of those organizations follows


# NCVHS NHIN Privacy & Security Selected Recommendations[5]

- The method by which personal health information is stored by health care providers should be left to the health care providers. (R-1)
- Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN. (R-2)
- Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN. (R-3)
- If individuals are given the right to control access to the specific content of their health records via the NHIN, the right should be limited, such as by being based on the age of the information, the nature of the condition or treatment, or the type of provider. (R-7)
- Role-based access should be employed as a means to limit the personal health information accessible via the NHIN and its components. (R-8)

[5] National Committee on Vital and Health Statistics, "Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network," June 22, 2006 Letter to the Secretary of the U.S. Department of Health and Human Services, http://www.ncvhs.hhs.gov/060622lt.htm


# Connecting for Health's Common Framework

## Core Principles for a Networked Environment

- Connecting for Health's nine specific recommendations to ensure privacy

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

- For explanations of the core principles go to: http://www.connectingforhealth.org./commonframework/docs/P1_CFH_Architecture.pdf [This link is included in the Resource page of the HISPC-IL Web site.]


# Policies on Connecting with the State-level HIE

The state-level HIE serves as a link between entities with health information and entities who have a legitimate need for that information. This means the state-level HIE must address privacy and security concerns involving linking entities as well as those relating to its own systems. Formal agreements or contracts provide the mechanism to require connecting entities to adhere to privacy and security standards.

- The privacy and security policies need to provide the framework for these agreements or contracts. Among other elements, the policies need to address:
  - Compliance with state and federal law
  - Sanctions for breaching privacy and security provisions


## Summary of Connecting for Health's "Model Contract for Health Information Exchange" Key Provisions [6]

- Each HIE participant must comply with healthcare privacy, confidentiality, security, and use standards.
- Each HIE participant must comply with state and local privacy, security, and use laws.
- Each HIE participant shall report to the other serious breaches of confidentiality.

[6] Rhodes, Harry B.. "Privacy and Security Challenges in HIEs: Unique Factors Add New Complexities to Familiar Issues." *Journal of AHIMA* 77, no.7 (July/August 2006): 70-71,74.
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031662.hcsp?dDocN&dDocName=bok1_031662


## Summary of Connecting for Health's "Model Contract for Health Information Exchange" Key Provisions [6]

- Established limitations will be placed on the use and disclosure of protected health information.
- Protected health information will be secured by appropriate administrative, physical, and technical safeguards.
- Each HIE participant shall report to the other any use of protected health information outside the established terms and conditions.

[6] Rhodes, Harry B.. "Privacy and Security Challenges in HIEs: Unique Factors Add New Complexities to Familiar Issues." *Journal of AHIMA* 77, no.7 (July/August 2006): 70-71,74.
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031662.hcsp?dDocN&dDocName=bok1_031662


# Work Group Resources

- Copies of or a link to most of the reference documents referenced in work group materials can be found in the Resources page in the HISPC-Illinois II Web site: http://www.idph.state.il.us/hispc2/resources.htm

- If you have any questions, please contact Jeff W. Johnson, HISPC-Illinois Project Director at 217-558-3403 or by e-mail at Jeff.W.Johnson2@illinois.gov