

Illinois Health Information Exchange Authority
Data Security & Privacy Committee
Meeting Minutes
February 19, 2014

The Data Security & Privacy Committee (“DSPC”) members of the Illinois Health Information Exchange (“ILHIE”) Authority, pursuant to notice duly given, held a meeting at 9:00 am on February 19th, 2014, at the Bilandic Building, 160 N. LaSalle, Room N-505, Chicago, Illinois, with telephone conference call capability.

Roll Call and Introductions

Ms. Kerri McBride, ILHIE Authority General Counsel and Secretary to the Authority Board, called the meeting to order. Ms. McBride introduced Dr. Nicolas Panomitros, Chairman of the DSPC. Roll call was taken and the attendance of the members noted below was confirmed. Ms. McBride welcomed the committee members and members of the general public.

Members Present in Chicago or on the Phone

Dr. Nicholas Panomitros (Chair)
David Carvahlo
Gerald Deloss
Dr. Carl Gunter
Debbie Hayes
Harry Rhodes
Tiefu Shen
Mick Scott

Intentions of the Meeting

Draft policies and procedures governing the privacy and security of the ILHIE were created for the consideration of the DSPC after review of other state policies and other resources. These policies will help ensure the security and privacy of data and will govern the transmission of data through the ILHIE. All the participants of the ILHIE will be required to abide by the security and privacy policies approved by this Committee and the Board of the ILHIE Authority. Ivan Handler, CTO of the ILHIE Authority, was introduced and present to address any technical issues that may arise.

Review and Discussion of Draft Security Policies

Policy 17: Physical Safeguards

The policy includes standard HIPAA requirements for participants and the ILHIE. Mick Scott commented on the lack of workspace security in regards to password controls. He suggested that the password policy already present in another policy be mentioned in this policy.

It was suggested that portable media, similar to a thumb drive, and not just workstations, be required to be encrypted as well. It was suggested to amend proposed Policy and Procedure 6.0 broaden the language to include ‘removable media,’ ‘portable media,’ or any media used in any ILHIE transaction.

The issue of ‘cloud’ storage was discussed. ‘Cloud’ storage, however, is already covered with HIPAA compliance.

Policy 18: Encryption

Encryption standards in the draft policies and procedures are required to be current to industry standards. Including language that addresses evolving standards was suggested. Referencing FISMA/NIST or ‘best practices in industry and government’ was also suggested. The latter was agreed to be added to the draft. Data that is exposed to the ILHIE at rest must be encrypted. Concern over data breaches was discussed.

Policy 19: Risk Analysis & Management

A DSPC member suggested requiring participants to conduct a risk analysis policy review “as needed, no less than annually”. Another member suggested that participants keep written documentation of risk analyses for possible review upon request, with the ILHIE Authority’s right to audit. The ILHIE Authority will accept a participant’s HIPAA risk analysis as long as it includes contemplation of the ILHIE in its analysis.

A template of how to complete a risk analysis was also suggested to allow for an affordable avenue for small physicians. Contacting physicians to see how burdensome these type of analysis are for them was also contemplated.

The ILHIE Authority confirmed that it has its own risk assessment done per contract terms.

Policy 20: Information Systems Activity Review

Section 1.1 allows the ILHIE Authority to conduct compliance audits of participants. Mr. Handler raised the issue of who would carry the cost of the compliance audit. Data was requested on other State exchanges and how they deal with the same issue. Another member brought up the language of 3.3, which offers ILHIE Authority “assist[ance]” in investigating violations. ‘Assistance’ was determined to be intentionally loose to deal with any circumstances that arise. The ILHIE Authority also conducts penetration testing of the ILHIE.

In regards to Sections 2.3 or 2.4, change to the language of vendor-specific practices to open industry standards was suggested, to place emphasis on open access over proprietary. A member commented that compliance with SAML may just be the cost of doing business in the health care industry.

Policy 21: Breach Protocol

It was noted that this policy was approved in November 2013.

Policy 22: Contingency Plan

Discussion of this policy was brief.

Review and Discussion of Draft (Revised) Privacy Policies

Policy 1: Compliance with Law and Policy

Draft – 3/7/14

The DSPC previously reviewed this policy. A redlined draft to show suggested changes was circulated.

A member pointed out that 5.1 ‘Addressable Specifications’ allows for wiggle room and requested that addressable implementation allowance be specifically be limited to certain HIPAA standards.

Policy 2:

No comments.

Policy 6: Patient Choice & Meaningful Disclosure

Previously approved.

Policy 7: Information Subject to Special Protection

No comment.

Policy 8: Emergency Access

No comment.

Policy 9: Individual Access to Data

Members mentioned 1.1 seems prudent.

Policy 10: Individual Amendment of Data

No comment

Policy 11: Individual Accounting of Disclosures

A member mentioned that the HITECH Act does extend patients’ accounting rights, but there is no final regulation on implementation. Ms. McBride responded that, once the final regulation comes, an update to the policy will be required.

Public Comment

The floor was opened for public comment:

Q: Policy 6: Patient Choice & Meaningful Disclosure. What is the legal basis for minors to consent to participation in health information exchanges?

A: The 12 years of age standard was determined to protect minors’ control over data in Illinois health information exchanges in accordance with State Law. Ms. McBride asked that any additional comments on this topic be emailed to her directly.

Q: Will the ILHIE Authority encrypt work stations at rest?

A: All newly-issued laptops will be fully-encrypted.

Next Meeting

The next DSPC meeting will be held on Wednesday, March 12, 2014 and, if necessary, Wednesday, March 19, 2014 for final voting purposes.

Draft - 3/7/14

Adjourn

The meeting was adjourned at 11:14 pm.

Minutes submitted by Jennifer Chow