

Approved 7/23/2014

MARCH 12, 2014, MINUTES
DATA SECURITY AND PRIVACY COMMITTEE
ILLINOIS HEALTH INFORMATION EXCHANGE AUTHORITY

The Illinois Health Information Exchange Authority (“Authority”), pursuant to notice duly given, held a meeting of the Data Security and Privacy Committee (“DSPC”) on March 12, 2014 at the Thompson Center, 100 West Randolph Street, Room 9-034, Chicago, IL 60601, with telephone conference call capability.

Committee Members Present

David Carvalho
Jay Anderson (phone)
Dr. Carl Gunter (phone)
Pat Merryweather (phone)
Mick Skott (phone)
Harry Rhodes (late arrival)

Welcome and Roll Call

David Carvalho, in place of absent DSPC Chair Dr. Nicholas Panomitos, announced his role as temporary meeting chair. Kerri McBride confirmed the presence of the DSPC members listed above with the exception of Harry Rhodes. The ability of those participating by phone was confirmed. It was confirmed that there was no quorum.

Kerri McBride noted that despite circulation of previous meeting minutes, minutes were absent from the agenda and could not be approved.

Review and Discussion of draft (revised) Security and Privacy Policies

Policy #1: Compliance with Law and Policy

There were no questions or comments offered regarding this policy.

Policy #2: ILHIE Authority Privacy and Security

There were no questions or comments offered regarding this policy.

Policy #3: User Authentication

An updated version of this policy was provided on March 12, 2014.

A committee member voiced concern about the policy’s ATNA compliance requirement and opined that some leeway should exist in the audit log reporting. The committee member suggested a standardized, non-ATNA specific audit.

The “compliance” language in the previous version of the policy has been replaced with “compatibility” language.

The Committee agreed to return to discussion of this policy later in the meeting.

Policy #4: User Authorization

Approved 7/23/2014

There were nominal questions and comments offered regarding this policy.

Policy #5: Access, Use and Disclosure of Protected Health Information

There were no questions or comments offered regarding this policy.

Policy #6: Patient Choice and Meaningful Disclosure

There were no questions or comments offered regarding this policy. This policy was previously approved.

Policy # 7: Information Subject to Special Protection

There were no questions or comments offered regarding this policy.

Policy #8: Emergency access

There were no questions or comments offered regarding this policy.

Policy #9: Individual Access to Data

There were no questions or comments offered regarding this policy.

Policy #10: Individual Amendment of Data

There were no questions or comments offered regarding this policy.

Policy #11: Individual Accounting of Disclosures

There were no questions or comments offered regarding this policy.

Policy #12: Minimum Necessary

There were no questions or comments offered regarding this policy.

Policy #13: ILHIE Workforce, Agents, Contractors and Subcontractors

A commentator noted that this policy is largely duplicative of *Policy #5, Access Use and Disclosure*. The duplicative portion of the policy has been eliminated and the policy now refers back to *Policy #5*.

Policy #14: Complaint Handling and Resolution

There were no questions or comments offered regarding this policy.

Policy #15: Sanctions

There were no questions or comments offered regarding this policy.

Policy # 16: Enforcement

There were no questions or comments offered regarding this policy.

Policy #17: Physical Safeguards

There were no questions or comments offered regarding this policy.

Policy #18: Encryption

There were no questions or comments offered regarding this policy.

Policy #19: Risk Analysis and Management

There were no questions or comments offered regarding this policy.

Approved 7/23/2014

Policy #20: Information Systems and activity Review

There were no questions or comments offered regarding this policy.

Policy #21:

This policy was not included for review.

Policy #22: Contingency Plan

There were no questions or comments offered regarding this policy.

Definitions

No questions or comments were offered.

Return to Policy #3: User Authentication

There was a discussion regarding the decision to use such a high level of specificity in the language for login monitoring, number of accounts, password strength, etc. Login monitoring is something that will continue to evolve in the industry. Some committee members voiced a concern that too much specificity in the policy could force the committee to make policy revisions each time standards for identification of individuals become more secure and password best practices change.

There was a general consensus that the specificity concern is warranted and that additions to the language in the policy are necessary. The language should indicate that there are certain best practice standards that must be met, and the language should permit security audits when necessary. This topic area is likely to change over time.

The DSPC did not determine the exact language that will be added, but commentators suggested the language reflect that industry best practices will be used in regards to login authorization. One possibility is a reference to current best practice standard on the ILHIE website. Due to the evolving nature of the topic, the referenced practice should be suggestive and not mandated.

A committee member voiced concern about the use of less definitive language. Less definitive language could result in an ineffective policy as it would avoid the issues the policy is meant to address. The policy should give some guidance as to what best practices are or no uniformity will exist.

A commentator responded that password protection standards will continue to change so we do not want to tie users down. The ILHIE Authority should get a sense of which portions of the standards are more stable and which are less stable and proceed accordingly. If best practice standards change, the ILHIE Authority should have the ability to review and amend policies when necessary.

There is a login monitor section that dictates the use of particular login protection mechanisms for password guessing. It is a type of best industry practice, but goes beyond best industry practice, listing the practice in more detail. The goal is not to monitor the number of password attempts. The goal is to discourage guessing.

A commentator suggested the use of password guessing protection standards that do not specifically call for standard requirements. The ILHIE Authority should have the ability to change the protections when necessary.

Approved 7/23/2014

The Committee briefly discussed password creation protocols. The primary concern is to reduce and minimize the risk of breach. Different participant users will have different levels of sophistication. It is important to develop a practice that is universally accessible.

The policies will be reviewed on an annual basis at which time changes can be made.

A commentator raised a concern about the language addressing ATNA compatible audit laws. There was a general consensus that the policy language should use ATNA as a standardization reference rather than as the only standard. The policy should state that the format will be standardized and that ATNA is the best example of a standard format.

Return to Policy #4: User Authorization

A commentator raised concern about the ability to allow for backup system administrators.

Next Steps and Wednesday, March 19, 2014 Committee Meeting

The next meeting will occur on March 19, 2014. It is the last scheduled meeting to consider these policies and procedures. Prior to the meeting, a staff member will take a poll to confirm a quorum will be present. If there is a determination that there will be difficulty establishing a quorum, there will be a meeting scheduled prior to the Board meeting on April 2, 2014. Once the DSPC votes on the policies they will be presented to the Board for adoption, and if adopted they will be the policies of the ILHIE going forward.

Public Comment

A member of the public posed a question for the committee regarding policy roll-out to providers that sign-up for the ILHIE. Would policies be presented in some sort of package?

Answer: Participants will be given a link so as not to force them to print all of the policies out. They will also be available on the ILHIE Authority website.

The opt-out forms, notices, etc. were recently received from the marketing department and appear ready to finalize. There will be a dedicated website for all of those forms and these forms once they are adopted.

No further comments were made.

Adjourn

The meeting was adjourned.

MINUTES SUBMITTED BY BRETT STRICKLAND