

THINC RHIO, Inc.

Taconic Health Information Network and Community

*Privacy and Consumer Affairs Committee Meeting
December 18, 2008, 2pm-3pm*

A meeting of the Privacy and Consumer Committee of the THINC RHIO, Inc. (THINC), a New York not-for-profit corporation (the "Corporation"), was held on December 18, 2008.

Committee members present: Art Levin, Paul Kaye, Steve Sarg, Norma Johnson

Non-Committee members present: Susan Stuard, Dianne Koval, Helen Pfister

Not present: Susan Wilson, Tim Cleary, John Blair, III, Asha Upadhyay

I. APPROVAL OF NOVEMBER 2008 MEETING MINUTES

A motion was made, seconded to approve the November 2008 meeting minutes.

II. RECRUITMENT OF COMMITTEE MEMBERS

Susan Stuard gave an update on the Committee recruitment and noted that inquiries have gone out to another hospital and physician practice to see if they might like to add someone to the committee.

III. REGULATORY ISSUES

Susan Stuard briefly discussed: Two regulatory issues: Mass Code 201 and the new privacy and security framework for health information exchange (HIE) just issued by the Office for Civil Rights at the U.S Department of Health and Human Services.

The Mass Code 201 CMR 17.00 sets forth the standards for the protection of personal information of residents of the Commonwealth. It is unclear if it would apply to RHIOs in New York State that see patients from Massachusetts. THINC will need to ask NYSDOH-Statewide Collaborative Process to review and determine if the RHIO Policies and Procedures v.1 are in keeping with the Mass Code 201.

The Office of Civil Rights (OCR) has issued eight guidance documents for HIE. They are: 1) Correction Principle 2) Openness and Transparency Principle; 3) Individual Choice Principle; 4) Collection, Use and Disclosure Limitation Principle; 5) Safeguards; 6) Accountability; 7) HIPAA Privacy Rules Rights of Access and HIT; 8) Personal Health Records and the HIPAA Privacy Rule. These guidance documents were issued on Monday, December 15th. Susan Stuard noted that she had not yet had time to thorough review the guidance documents but suspected that the New York State Department of Health has taken a more restrictive interpretation of privacy than the Feds. Pending further review, the Mass Code 201 and OCR Guidance will be topics for discussion at a future committee meeting.

III. DISCUSSION OF DRAFT SECURITY BREACH POLICY

Art Levin and Susan Stuard drafted a first version of the security breach policy which was circulated to the committee for review. Susan Stuard noted that the committee may go through several rounds of revisions before this policy is finalized. She also noted that all the policies will be reviewed together at the end of the development to check for consistency.

The committee discussed how breach might be handled differently if it were a one-to-one transaction versus a many-to-many HIE-type transaction. An example of a one-to-one transaction is when a physician send an order for a test to a laboratory and the laboratory sends the test result back to the physician.

Breach, in a one to one transaction, would be handled under existing New York State laws (e.g., The NYS Information Security Breach Act) and would not trigger the THINC security breach policy. THINC's security breach policy will govern many to many transactions, where patient consent is required.

Art Levin outlined key components in the policy, such as the commitment to have a transparent and explicit breach policy. First is to establish a process to determine if a breach occurred and the nature and magnitude of the breach. The second is the investigation of the breach to determine the factors that led to the breach, and the third is to have a process in place to provide timely notification to those consumers whose personal health information has been compromised. Norma Johnson said that the notification and the investigation could happen at the same time. It was suggested that the ordering be removed. Susan Stuard asked the committee if the statement about the participation of organizations was clear enough. She said that it is important that the policy be clear and concise and easily understood by the consumer reading it. The committee agreed that this was a clearly defined policy but subject to other revisions based on additional discussion.

Security Breach- Notification and Remediation

Bullet 1: Timely notification and notification in writing – The Committee asked if a patient would be notified if lab test result was mistakenly viewed? Art said this policy would apply only when protected health information (PHI) is actually breached. In regards to the timeliness of notification, Susan Stuard noted that THINC's interpretation and other organizations of timeliness may be different. The committee considered whether a set time should be defined in the policy. Art Levin noted, and the committee concurred, that we can leave the words timely notification for now and adjust later if needed.

Bullet 2: Notify government agencies - no comments.

Bullet 3: Notifying participating organizations – no comments.

Bullet 4: Notification under existing law by law enforcement agencies – no comments.

Bullet 5: THINC investigates the breach/root cause analysis – Helen Pfister said that in regards to SCP says that the investigation has to happen in the shortest time possible without reasonable delay. This should be added to the THINC policy.

Bullet 6: Remedial plan in the event of the breach – Helen Pfister said that this encompasses two items and should be separated to 1) identify the cause of the breach and 2) remedial plan. Dianne Koval asked if a provider's office breached the information, how would this be handled in terms of notification? The patient would be notified that the user breached the information at this practice, and this is the plan of action being taken towards that individual. This would be a physician level issue rather than a RHIO issue. Art Levin said THINC will seek to define the site of breach issue further.

Bullet 7: Organizations notify THINC within 48 hours of breach at their facility- no comments.

Security Breach - Enforcement and Sanction

Four sanctions at minimum should be applied: 1) Suspending/temporarily restricting specific users' access to health information; 2) Requiring user to undergo additional training in use of health information; 3) Terminating access of user to the health information exchange; 4) Terminating participating organization's access to health information exchange. If an organization applies the sanctions, a written report of the sanctions is required to be furnished to the RHIO within 24 hours.

What happens if a person opens a record accidentally? This could be a breach but it was not malicious. Art Levin will find out where the Statewide Collaborative Process stands on accidental access.

IV. REVIEW OF AUTHORIZATION – will be discussed at the next meeting

V. QUESTIONS and NEW BUSINESS

There being no further business for discussion, the meeting was adjourned.