

**Ohio Health Information Security and Privacy Collaborative (HISPC)  
Implementation Working Group Meeting Agenda**

January 3, 2007

1:00 PM to 3:00 PM

Attending: Kate Cauley, Bill Mitchin, Doug Alt, Sandra Solano-McGuire, Ayeshia Ellington, Ernie Boyd, Philip Powers

By telephone: Jeff Kapp, Margie White, Megan Smith, Denny McLean, Kim Keiser

Kate reviewed the agenda and asked for commentary on the minutes. The minutes were accepted as written. Kate reviewed the need to identify the assumptions that we are making as we begin to write the implementation plan. She asked for reports on homework assignments from Kim, Margie and Phillip. Kim reported that she had not heard anything from Bridget but that she understood that the state budget includes a provision that the Third Frontier Network will be extended to every county seat in Ohio. Margie continues to work on the analysis of Steering Committee membership and the state agencies that will need to be involved with any health information exchange efforts on the state level. Philip reported on Broadband Ohio and suggested muniwireless.com as a resource.

Sandra reported that in the auditor's report on Medicaid the recommendation from that report was to have state RHIO activity administered by the State CIO. Sandra also reported that in the Medicaid Transformation grant the Office of Health Plans continues to describe a patient summary like the CCR and administrative tools for RHIOs. Kate reflected that most of our discussion to date (see solution 1 b.) is for a state authority with more of a consortium focus. The group then moved into a continuation of the discussion related to implementation for the state level solutions identified in the Interim Report of Solutions.

*6 b. Increased human oversight, evaluation of data integrity and enforcement of security protections are all recommended.*

Our primary assumption is that there will be a state group that will assure standardization and interoperability among RHIOs. An additional assumption for this solution and its implementation is that all systems will be HIPAA compliant including a full audit trail. A third assumption for this solution and its implementation is that all systems in the state would be interoperable to facilitate health information exchange. Given these assumptions:

Sandra suggested that the critical dimensions of implementing this solution should focus on the evaluation of how standards are being met, how data accuracy and integrity will be determined and how complaints will be handled. In other words, who is responsible for enforcement? Will there be legislative/regulatory oversight, and will the state level body have the authority for enforcement, or will market and quality functions drive the necessity to meet state level standards once they are in operation for the majority of stakeholders? As we discussed the importance of this monitoring function, Denny clarified the need to distinguish between two levels for data accuracy and integrity—one, at the point of direct input from the provider and two, within a data repository maintained

either regionally or statewide. Kate offered as an example, that with the shared community health record, HIE<sup>TM</sup> housed in a regional central data repository, maintained by the HealthLink RHIO, there are data sharing agreements between the RHIO and provider organizations that specify that members are responsible for the accuracy of the data input, and at the level of the central repository regular audits are conducting for monitoring purposes. The group agreed there would have to be business rules specified to address these issues, and that common practices across the state should be in place. The group then discussed multiple possibilities for how and where data would be maintained as this would have an impact on monitoring and enforcement processes. Rather than specific recommendations since at this point much of these issues are under discussion across the state, the group decided to stay generic in suggestions for implementation and listed examples of functioning models from which to draw including: the UHIN model where the data all stays in cyberspace; systems that plan to use a statewide system as a library card catalogue directing the inquirer about where in the state to find specific information; and systems like the two functioning RHIOs in Ohio where data is maintained centrally in the largest politically feasible geographic region—with HIE<sup>TM</sup> as a share community health record where data is input and accessed by multiple providers who share a common record for each patient, and with HealthBridge where a central data repository of laboratory results is accessed by multiple providers. The group reviewed the nature of the various discussions related to this issue—the Roadmap calls for regional data hubs “reporting to some kind of state level RHIO, the State Attorney General’s recent report had a recommendation for a state level RHIO, Medicaid has outlined in their Transformation Proposal a kind of data consortium of local, regional or state-wide data systems with an expectation of facilitating health information exchange. Overall the solutions and implementation working groups have discussed to date following the real time evolution of HIT and HIE in the state which includes multiple RHIOs and the need for some state level coordination, monitoring, oversight, etc. Doug reported on the state committee that is working to develop an administrative rule on securing sensitive information. As these rules are developed they will state regulatory authority and apply to all state agencies, and not necessarily have any specific provisions for personal health information.

To summarize the discussion Kate reiterated that we recommend a state level coordinating group to audit interoperability, data integrity and that it would implement multiple levels of enforcement and evaluation. We need specificity about security rules for both data input and management of data repositories on both the state and local levels. When articulating these plans we need to include examples of what exists and best practices. Following the work of the group developing criteria for standardizing HIE will be important, for example.

*5 a. Current laws and practices that govern the paper release of treatment related information, should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*

The overall assumption guiding discussion on this solution and its implementation is that the technology can handle whatever is needed to provide appropriate privacy and security. An additional assumption articulated is that currently information related to diagnoses and medications are routinely exchanged for purposes of treatment, payment

and operations as specified by HIPAA and demonstrated in state business practices—i.e. claims date. However, this is not the kind of sensitive data addressed in this solution and discussion of its implementation. Rather we are talking here about information that might be classified as the providers notes, text from psychological reports or assessments, treatment planning, and the like.

Sandra suggested that standard rules for the state need to include methods to implement and store those permissions. Not only are there typically no data fields for documenting that permissions have been given, to whom and for how long, there are not pathways to coordinate and monitor this information potentially across multiple providers. Kate suggested a detailed review of what currently happens in the paper based system would provide direction about how to proceed with standards for electronic systems for authorization and access. The group concluded specific business rules within the context of existing law is critical to insure both comprehensive and accurate information and careful privacy and security protections. Following the research on the legal requirements on authorization and authentication, the identification and implementation of algorithms will be the easy part.

*5 b. The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, should be used as the standard for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.*

Kate reviewed the spirit of previous discussions including the assumption that data are already being exchanged by payers, pharmacies and others on medications and diagnoses that are critical to provide quality care. The group agreed that any pertinent information such as that specified in the CCR should be exchanged for treatment and payment regardless of whether the state barriers in practice variations apply. Bill Mitchin reported that during the Variations group discussion it was apparent that the primary focus needed to be treatment and having the right information available at the point of care. Jeff confirmed that there are no legal state provisions preventing the exchange of data for mental health, substance abuse and other disease diagnosis as specified by HIPAA. Sandra reminded the group that standard business practices in areas such as the routine use and exchange of data using the 837 included information about diagnosis and medications for mental health, substance abused and disease conditions. Additionally, discussion focused on the fact that standard privacy releases also specific exchange of data in all areas of health and mental health care for purposes of treatment payment and operations. It was pointed out however, that providers do not all implement these kinds of privacy and security measures uniformly, and many are reluctant to share this kind of data for fear of breaking HIPAA and/or state rules. This emphasized the group's call for statewide standards of business practices and a state level coordinating/monitoring function to enforce implementation.

*5 c. A federal and state approved emergency release should be adopted that patients routinely provide at the outset of treatment for exchange of information related to mental health, substance abuse and other "sensitive diseases" in case of an emergency.*

The group agreed that this "break the glass" provision was unnecessary given solution 5b.

An additional meeting is scheduled for January 25, 2007 from 2 to 4 PM. This will allow more time for the specifics of the implementation for the various solutions and will also then be able to include data gathered from the statewide meeting January 16 which will review recommendations from the Roadmap and what kinds of responsibilities for HIE will be managed/monitored at the state and local/regional levels

Next steps include follow up on previous assignments.

**Next Meeting date is Wednesday January 10, 2007, 1:00-3:00PM**

Meeting adjourned at 2:30.