

**MINUTES OF THE AUGUST 13, 2012 MEETING
OF THE DATA SECURITY AND PRIVACY COMMITTEE OF THE
ILLINOIS HEALTH INFORMATION EXCHANGE AUTHORITY**

The Data Security and Privacy Committee (“Committee”) of the Board of Directors (“Board”) of the Illinois Health Information Exchange Authority (“Authority”), pursuant to notice duly given, held a meeting at 2:00 p.m. on August 13, 2012, at the offices of the Illinois Office of Health Information Technology (“OHIT”), 100 West Randolph Road, Suite 2-201, in Chicago, Illinois and at the offices of the Illinois Department of Healthcare and Family Services, 201 South Grand Avenue E., 3rd Floor, in Springfield, Illinois, and with webinar participation capabilities.

<p><u>Appointed Committee Members Present in person:</u></p> <ol style="list-style-type: none"> 1. Leah Bartelt 2. Elissa J. Bassler 3. David Carvalho 4. Carl Gunter 5. Pat Merryweather 6. Nicholas Panomitros, Chair 7. Harry Rhodes 8. William Spence 	<p><u>OHIT Staff Present:</u> Mark Chudzinski; Krysta Heaney; Cory Verblen</p> <p><u>Invited Guest:</u> Sonia Desai Bhagwakar</p>
<p><u>Appointed Committee Members Present electronically:</u></p> <ol style="list-style-type: none"> 1. David Holland 2. Tiefu Shen 	

Call to Order

Mark Chudzinski, Secretary of the Authority and General Counsel of OHIT called to order the meeting of the Committee. Prior to calling roll, the most recent meetings of the Committee were summarized. Over 35 stakeholders have provided testimony to the Committee on July 17, 2012 and July 27, 2012. All of the submitted testimony has been posted publically on the ILHIE website; a copy of the Committee website page was distributed.

The next scheduled meetings of the Committee are Thursday, September 6, 2012 and Friday, September 7, 2012, if necessary, to finalize the Committee’s privacy, security, and consent management recommendations for submission to the Board on September 19, 2012.

An overview of the documents distributed to the Committee prior to the meeting was provided: 1) summary results of submitted Committee member responses to the Policy Decision Ballot (“Ballot”) and 2) a tool summarizing the submitted public testimony grouped according to the questions on the Ballot.

Roll Call

Mr. Chudzinski welcomed the appointed Committee members present in person and electronically, and confirmed the presence of the Committee members noted above. There were no objections from the members of the Committee to the participation by electronic means of David Holland and Tiefu Shen who had advised the Secretary in advance of their attendance by electronic means necessitated by business or employment purposes.

Deliberations Regarding ILHIE Privacy and Security Policy Questions

Dr. Panomitros, Chair of the Committee, suggested the Committee review the results of the Committee's responses to the Ballot. After hearing the input and testimony from stakeholders, the Committee should begin to review the various arguments provided and strive to develop a Committee consensus on the privacy, security, and consent management policies that will be in the best interest of the State.

A concern was raised about the Ballot noting it asks questions that cannot be answered in isolation. By themselves, the tradeoffs between questions are not clear in the Ballot and the results should be reviewed with this in mind. It was further explained that the Ballot reflects the current legal and regulatory environment in Illinois.

The Committee discussed Ballot question #1: *"Federal HIPAA allows providers to disclose patient data without patient consent it for purpose of treatment, payment, or healthcare operations (a/k/a/"T-P-O"); the major exceptions are: psychotherapy notes; substance abuse data; use of data for marketing purposes. Illinois should follow Federal HIPAA policy; ILHIE rules should not be more restrictive than HIPAA."* The question is intended to determine if there is support for "no consent".

Based on results of the Ballot there appeared to be a degree of agreement to Ballot question #4, *"The consent of patients to have their provider use the ILHIE should be implied, but the patient should be provided the opportunity to object ("opt-out")."* There appeared to be some consensus that patients should have an opportunity to consent (opt-out) to having data available to providers using the Illinois Health Information Exchange ("ILHIE"). One of the Committee's tasks is to determine in what situations it is sufficient to be only as restrictive as HIPAA and when to be more restrictive than HIPAA. In some cases, we want to scale back from HIPAA, in others we want to extend HIPAA.

Based on responses from the survey and Committee discussion, the majority of the Committee believes HIPAA is not sufficient for participation in the HIE. A minority suggested the consent requirements for participation should not be more restrictive than the HIPAA policy, but voiced support for the exceptions specified within HIPAA.

There was general consensus that there are some discrepancies between Illinois law and HIPAA on how particular categories of information are treated, and that these differences should not be preserved. Harmonization with HIPAA does not preclude consent for HIE (disclosure).

One of the Committee's tasks was described as determining whether to require consent for data exchanged using an HIE for treatment purposes. It was added that the Committee should also

determine whether the treatment exception under HIPAA should also be extended within the HIE environment to also include payment and operation purposes. A concern was raised that if the HIPAA rules were extended generally there would be nothing holding providers to gain consent prior to participating in an HIE.

It was brought to the Committee's attention that in addition to the categories of data discussed, there are other sharing rules not mentioned in HIPAA, like research, that the Committee should also address.

The main arguments presented were summarized. In general, being more restrictive than HIPAA is not ideal from an administrative standpoint but there are specific areas where there may be exceptions. It was further explained HIPAA should serve as baseline; there are instances where we want to be no more restrictive than HIPAA and in some cases more restrictive than HIPAA.

Ballot questions #2: *“For purposes of the ILHIE, Illinois law should be amended to harmonize with HIPAA and more clearly allow transmittal to the ILHIE for T-P-O of: 1) General medical PHI; 2) Mental health PHI; 3) Substance abuse PHI; 4) Genetic testing PHI; 5) HIV/AIDS PHI.”*

If, for example, for general medical PHI Illinois law should be harmonize with HIPAA it will allow transmittal of general medical PHI within the HIE, not covering the particular types of data mentioned in the question, without consent; therefore, no opt-in, no opt-out, no consent required. There was a discussion about what the default policy of data “inclusion” should be. There was a discussion that these particular types of data should not be treated any differently. It was noted that there is not an inconsistency between wanting certain types of data to be treated the same and allowing patients to have the right to opt-out of particular types of data being included within the system.

The Committee reviewed the ILHIE technical infrastructure. It was explained that the State is not purchasing hardware on which to house data. The State has entered into a contract with Intersystem Corporation, a cloud vendor, for them to provide the HIE service. There is no centralized database currently planned for the State-level HIE; the State-level HIE is federated. However, it was noted that one of the Regional HIEs has a central repository, MetroChicago HIE. The data that would stay at the State level is the data for the directories, for example, the provider directory; the electronic health records (“EHRs”) will move in and out of the HIE.

It was further noted that testimony provided indicated that it was not privacy and security issues that drove the choice of pursuing a federated model but issues of competitive advantage from the provider perspective. A key difference between the virtual and centralized models is that if a provider decided to drop out of the virtual model there would be no data in the system but if the system was centralized the data would remain. It was added it would depend on whether the provider had the right to retrieve their data upon leaving the system.

It was stated that the architecture models are not as different as they sound – if you have a system in which you can query data on responses it is not that different than storing data in a central repository. An issue to be considered, possibly by another committee, is whether

provider participation should be mandatory. It was noted that patients will not benefit if providers do not participate in the HIE.

It was brought to the Committee's attention one of the documents that was circulated on the amount of data obtained under opt-out and opt-in participation models stating that it has some interesting data on page two about participation rates under opt-in. The document provides information on the Massachusetts' system that has an opt-in system and has 90% patient participation. They explain the high participation rate as having come from a robust education campaign about the benefits of EHRs and participation in HIE so patients were very well informed and there was arguable strong provider encouragement to get patients to participate in HIE. This example demonstrates that an opt-in system does not necessarily mean a complete dearth of patient data and it also demonstrates that there really are not that many patients that would refuse the opt-in. It was noted that it also demonstrates the need to have put in place a very robust education campaign to get the high participation rates. The Massachusetts system only involved three communities thus the model may not be as scalable to the Illinois.

Another possibly for how the consent model could be operationalized was presented for consideration. You could have an opt-out for the system but then when you go to an individual providers the patient would need to opt-in to have that provider collect the data. The system would be neither opt-in or opt-out but a combination of both. Upon listening to the testimony provided by the AIDS organizations, there may be reasonable situations where not all information needs to be shared. Under the 2-stage consent model a patient could be in the system but for an individual provider if they ask if they could get that patients' information that patient could tell them they prefer not.

OHIT has identified four states that have what is known as a 2-stage HIE model. For example in New York all of the information goes into the HIE but the provider may not pull that information out of the HIE without patient consent. The Swiss cheese analogy does not apply, because all the data goes in to the HIE it is only a question that when the patient sees a provider that provider needs to get their permission to get the data. One disadvantage with the 2-stage model is the logistic issues with referrals where the provider has not yet seen the patient and wants to pull information in advance of the visit.

The 2-stage model is also in Rhode Island Minnesota and New Mexico. In New York, the American Civil Liberties Union ("ACLU") sued the state of New York and published a negative report that the act of putting information into the HIE constitutes a disclosure and the ACLU views that the HIE is contrary to New York law. Both Minnesota and New Mexico have statutes that specifically provide for a 2-stage model; in Minnesota consent is needed for pulling information out and in New Mexico consent is needed only for special categories for information, so TPO can still apply.

A issue was raised that a clinician would be concerned if one of his patients indicated that he did not have permission to access the patient's record stating that it raises a red flag and introduces risk. It was noted that this is not that dissimilar from the current system where the patient may not choose to fully disclose all of the information from another provider. Dr. Gunter further explained that the goal of the 2-stage consent is that someone might choose to opt-out of the

system entirely if they do not have the provider-level opt-in option. Allowing opt-in at the provider level is a mechanism to come up with a practical way that balances the need for the system to have the information required for it to be effective with patients feeling confident that the data in the HIE will be shared in a way that the patient finds acceptable.

A concern was raised that the patient may not have the clinical expertise to determine what information is relevant to their care, noting that there is significant patient risk to not sharing all information with the treating clinician. It was stated that the largest risk to any clinician having access to any data in the HIE is that the patient may choose not to participate in the system at all if their data can be accessed without their permission.

It is important to note that there is a lot of information in a patient's medical record that physicians could have access to that may or may not be relevant to care; the patient may feel that the provider does not need to see all the details of a sensitive event from the past. It was recommended that the consent conversation is one that if had at the physician-patient level, where the provider pulls up the EHR and it is obvious that it appears to be incomplete record, the provider can then inform the patient that there are certain conditions that although the patient may not think are relevant, may be significant to their treatment and the provider would like to request the patient provides consent to view their entire record.

To OHIT's knowledge all of the 2-stage HIEs are operating in an all-data-in or all-data-out approach. In other words, all of the information is in the patient's record and that because of current technical limitations it is not really possible to segregate specific items of information. For example, a patient cannot simply indicate that they want to sequester only their HIV/AIDS information; effectively, if a patient wants to sequester some items in their record the entire record will be sequestered.

The Committee discussed and agreed that there are significant limitations to the current technology's ability to allow for the granular sequestration of patient records. Because a great deal of data in the patient record is textual data as opposed to data in discrete data elements it is extremely difficult for a computer to make determination as to what data to exclude and not exclude. This limitation has resulted in certain Regional HIEs not including any textual data fields/elements because of fear that data that the patient would not want revealed is inadvertently disclosed to providers. It was asked how providers currently handled this issue in a paper system. It was explained that in a lot of the data systems manual intervention is necessary. It was stated that the 2-stage all-data-in or all-data-out is a pretty practical approach until there is a better way to perform segmentation.

A hypothetical example of how the 2-stage all-data-in or all-data-out approach would be implemented given that Illinois law concerning certain categories of health information are harmonized with HIPAA was provided.

A patient, after Illinois law has been harmonized with HIPAA, is given the option to opt-out of the HIE and does not opt-out. The patient's record includes information about his positive HIV status. The patient goes to the podiatrist where they are asked if the podiatrist can access their medical record; the patient says no, access is declined. The patient goes to another provider and again declines to share his medical record. The

treating provider explains the benefits and potential risks of not sharing the data at which point the patient grants consent and the provider may access the record, including the HIV information.

It was noted that there is some of the information that would be available through the HIE the treating provider will gather directly from the patient when the patient completes the medical history. It was explained however, this information is based only on the information that the patient has chosen to share with you at that point. It was further explained that one of the benefits of the HIE is to move away from depending only on the patient to remember all the details of their previous care encounters; it doesn't mean that you don't ask patients any more, it just means that the patient doesn't have to be responsible for everything. A Committee member shared his experience serving on the Health Information Technology Standards ("HITSP") Committee, the electronic clip board combined what the patient's medical history with: 1) the patient's pharmacy benefits history so it includes all medications with the current dosage and spellings and 2) the patient's insurance providers' claims information so the provider is aware of the patient's procedures and the admission details. It was mentioned there are good examples, like from the Memphis Exchange where money and lives were saved because the electronic record was available when the patient could not remember something.

An issue was raised that the interests of public health and research may not be fully realized with the 2-stage model. In the federated model where the HIE queries records, when would the consent for public health purpose be collected. It was explained that public health would be one of two the exceptions where the HIE could send the information could send the information to public health without additional consent. The same would be true for break the glass as well assuming the break the glass exception is passed in Illinois.

It was explained there is a technical problem with the system the State is implementing. The ILHIE queries on the basis of patient name, it is designed around the idea of helping individual patients with their care. The kind of public health system envisioned may need some additional features such as the ability to query for data without names and this has not yet been discussed yet. It was stated that the data does need to be identifiable, for example with communicable disease like TB where you need to know the patient name so that the intervention can occur. It was also mentioned that it is also important to avoid duplicating counts of infection and disease. Further clarification was provided that it is not an "either-or", there are some situation where you need an identifier and some where you do not for example, in situations of mandated reporting of certain conditions where there is an obligation of the public health department to follow up you need the identifier, however when you are conducting surveillance and looking at trends of flu, you do not need the identifier.

The Committee suggested charging OHIT with the responsibility to develop plans to address the issues of segmentation and permitted uses for public health and research. It was mentioned it can be difficult to go back to the General Assembly and request additional data at a later point. The Committee asked if there was a proposal from OHIT on the engineering side of how to address public health reporting. The plan is that one of the four initial use cases is the implementation of the Public Health Node, currently operational, that will eventually be hosted on the ILHIE. Using the Public Health Node, information flowing through the ILHIE, at appropriate points in time, would be passed along to the Illinois Department of Public Health,

and when appropriate also shared with Local Health Departments and the Centers for Disease Control.

It was asked whether the State would require records to pass through the ILHIE. It was noted that Indiana has a system where information is sent to a central repository where data can then be surveyed for public health purposes. However, the ILHIE system is an on-demand system; you only get an opportunity to pass through to public health whatever is being passed at any given moment through the system. This approach helps address some of the security concerns but hampers the ability of public health to collect data. An example was offered of a patient diagnosed with an STD [non-reportable], that information will sit with the provider who made the diagnosis until that patient's record is queried by another provider. It was asked if the ILHIE would be able to, at some frequency query all of the data from all providers. It was explained that the gateways that are sending this information would then need to support receiving those types of queries. Currently, the systems only support a query again a name, an individual person, the provider's system will create a persistent document that is transferred through the HIE. A query for a specific data element, for example of query for all cases of disease 'X', is a very different kind of query than for a name.

It was noted that initially the Public Health Note will replace the mandatory reporting system that currently exists from separate interfaces to one interface. In the future, there will be syndromic surveillance function but it too requires the data passing through the system. It was further explained that complicating the issue is when data is exchanged through a Regional HIE where 95% of transactions stay within the regional, data will reach the state level HIE with less frequency. It was also noted that when the provider has an internal HIE or a patient receives care within a health system, data will also reach the state-level HIE with less frequency; in this scenario, in only very limited situations, for example an out-of-town ER, would data pass through the ILHIE and to the Node, for non-reportable conditions.

It was noted that although from a public health perspective a repository would be an ideal state the planned ILHIE infrastructure supports more advanced and timely public health reporting than is currently available. With EHRs and the HIE, if the Illinois Department of Public Health were to impose a reporting obligation on Illinois providers, there would be a more favorable response from provider who would no longer need to rely on manual processes.

It was noted that the Intersystem vendor product is capable of being technically configured as a repository or an on-demand system; the State is pursuing an on-demand approach. An important operational issue to consider in this type of system reconfiguration in a query model the system is optimized by making requests on demand. So suppose you have 25,000 patients in a given month then you only expect a tiny portion of those records to be requested. However, if you are talking about this public health query function this represents an entirely different demand on the system.

The Committee discussed Ballot question #5: *"A patient's decision to opt-out should be signed by [the] patient (i.e., written not just oral)."* A clarification of the question was provided. Under Illinois law it is sufficient to document in the record the collection of consent; the question is intended to indicate where patient choice should be documented. Committee members were

informed of federal law, e.g. the E-Sign laws and the Uniform Electronic Transactions Act, allowing for electronic signatures as the means for affirmatively collecting and documenting patient choice; implementing electronic signatures would be consistent with federal law.

The Committee discussed the potential impact various consent approaches may have on provider and patient training and education. The advantage of pursuing a “no-consent” approach is “avoiding” the complexity of how specific providers pose the option to “opt-out”. The Committee recommended there would be standardized guidelines, promoted by OHIT, to provide uniformity across providers to create consistency in how patients are informed of their consent options.

Data from Massachusetts suggests, to a significant degree, consistent training can positively impact patient participation rates. The Nebraska HIE was used as an example to demonstrate a possible solution to assure consistent provider to patient messaging, routine provider audits. There was consensus that “opt-out” does not eliminate training obligations however, it is advisable to avoid things that require significant training obligations since it will likely increase cost and introduce inconsistencies among providers. Committee members were informed of annual provider obligations to provider HIPAA staff training; a recommendation was put forth to incorporate HIE patient preference collection into the HIPAA training program.

The Committee discussed Ballot question #22: *“Security Compliance Standards: imposed by ILHIE on sub-State HIEs.”* The Committee discussed the potential trade-offs between imposing standards and allowing sub-state HIEs to implement potentially inconsistent standards. If security standards are not imposed, a violation would cause a loss of confidence in the whole system. A strong centralized governance and security compliance structure ensure consistency and encourages trust in the system. There was consensus among the Committee that ILHIE should impose security standards.

The Committee discussed Ballot question #6: *“An opportunity to opt-out is insufficient; providers should obtain affirmative written patient consent to use the ILHIE for all patient data (“opt-in”).”*

The majority of Committee members disagreed that an opportunity to “opt-out” is insufficient. An argument was presented in support of “opt-in”. One of the benefits of “opt-in” is to introduce consistent consent approach across data types. Currently Illinois has state laws more restrictive than HIPAA that require affirmative consent to share. Even with strong support for amendments to current Illinois law, if changes are not successful, Illinois HIEs will be operating in a dual system where certain types of data are treated differently. In this legal and regulatory environment, the State will encounter the same problem currently faced by Regional HIE MCHIE where an entire set of data, e.g. behavioral health data, is excluded from the HIE. Requiring an “opt-in” would “require” providers to treat all data shared through an HIE consistently; the need to segregate certain types of information is eliminated. It was mentioned that a blanket “opt-in” does not achieve the ability of patients to control sensitive information.

A concern was expressed about the “opt-in” model is the potential for low participation rates. Additionally, “opt-in” places an additional burden on the provider and may introduce consent

fatigue on the patient. The Committee discussed the benefits of the proposed 2 stage HIE consent model noting that allowing patient to “opt-out” of the system and “opt-in” for individuals providers would provides some of the benefits of each approach.

The Committee discussed existing technologies to support granular sequestrations. It was brought to the Committee’s attention that while there are vendors that “advertise” that they can perform sequestration there is no scientific testing that supports this ability and whether it is successful. To date, scientific studies show that records can be reconstructed based on information remaining in a record that has had some amount of information sequestered. There are some HIEs that offer patient configurability that gets mapped to a specific list of drugs for example; however, whether this effectively protects patient privacy is not yet clear. There was consensus that there are current technology limitations to implementing granular data sequestration.

However, the adoption of policy proposal should be based on a desire to drive the development of products to cater to patient preferences. Initially an all-data-in or all-data-out approach allows for data exchange through ILHIE to begin while types of data segmentation can be advanced in stages over time to benefit those that may chose to not participate due to the inability of the system to support granular patient consent.

The Committee worked through scenarios under the 2-stage HIE consent model. There was consensus that the 2-stage models offers protections to those concerns about sharing sensitive patient data by “opting-out” will allowing for 1) the sharing of patient data under current and future legal and privacy environments and 2) sharing of data with Public Health and for emergency situations (“break-the-glass”). To have effective point-of treatment patient choice patient information needs to go the HIE.

The Committee considered whether the provider or the HIE is responsible for data sequestration. With an “opt-in” at the provider level, is it the responsibly of the provider to sequester patient data or does it all go to the ILHIE and the ILHIE performs the sequestration? The Committee was informed of an Office of the National Coordinator (ONC) project to create labels and that would allow a HIE identify what information to disclose and which to not.

The Committee discussed consent requirement at the provider level to query the ILHIE. In this scenario, by default (“opt-out” for HIE participation) a patient’s information is included and if a provider wants to query that patient’s information they need a consent. Requiring consent to query is a form of access control and addresses some of the security concerns regarding who has access to pull and view patient information available through the HIE (permitted users). There was a concern that implementing an “opt-in” for query was more stringent than HIPAA for sharing of general PHI and whether exchange is only as robust as Direct. Requiring “opt-in” consent at the point of treatment although would introduce more stringent requirements for general PHI it would allow access to the full data set available in the HIE, not only that data provided through the provider-to-provider exchange enabled through Direct. It was noted that audit controls and audit trails, would allow for system monitoring of inappropriately access records. A concern was expressed about the ability of manual subsequent review to effectively prevent security breaches.

The Committee further discussed the process of collecting patient preferences. The Committee was informed that neither the State nor Regional HIEs currently have the functionality included to record patient preferences. Although it is easier to segment data based on recipient versus the categories of information, neither is implementable at the moment.

The Committee reviewed the proposed 2-stage HIE consent model. Assuming Illinois law is harmonized with HIPAA as previously discussed by the Committee, 1) by default patient data is included in the HIE, 2) patients are offered an opportunity to “opt-out” of re-disclosure by the HIE to subsequent providers, “opt-out” would apply to all data until data sequestration techniques are sophisticated to support granular patient, 2a) patients can grant subsequent providers one time overrides to view data available in HIE, the subsequent consent does not void previous “opt-out”.

The proposed 2-stage HIE consent model with opt-out will achieve desired patient participation (although does not address provider participation), allows info to flow to public health and be available in emergency situations, while allowing for protection for those that are concerned about sharing of sensitive PHI. Additionally, for those that would later decide to share their information they would be able to receive the benefits of the exchange. The majority of the Committee agreed with the proposal. A minority would prefer an opt-in at the point of treatment to address privacy concerns.

The Committee decided to meet again prior to the next currently scheduled September 6, 2012 meeting. The Committee agreed to meet on Friday, August 17 from 2:30-5:00pm.

Public Comment

There were no comments offered from the general public.

Adjournment

The meeting was adjourned at 4:45 p.m.

Submitted by:

Krysta Heaney