Utah Digital Health Service Commission Meeting

Thursday July 12, 2012 10:00 a.m. – 12:00 p.m.
Utah Department of Health, 288 North 1460 West, Rm 114, Salt Lake City, Utah

Minutes

Members Present: Henry Gardner, Doug Hasbrouck (Vice Chair), Jan Root, Nancy Staggers (via Phone) and Brad LeBaron(via Phone)
Members Absent: Mark Munger (Chair), Dennis Moser, Scott Barlow, Natalie Gochnour, Deb LaMarche, Marc Probst and Chet Loftis
Staff Members: Wu Xu and Humaira Shah (UDOH, OPHI)
Guests: Wyatt Packer (HealthInsight), Courtney Dinkins (AUCH), Barry Nangle (UDOH), Sherrie Loewen (Salt Lake Community College), Gred Mead (DTS), Weston Tolman (College of Pharmacy, UofU), Carolyn Steele (Regence), Jamie Steck (Central Utah Clinic), Scott Horne (UHA), Jeffrey Duncan (OPHI), Michelle McOmber (UMA) and Felix Littlefield (Salt Lake Community College)

Introduction and Update:

Doug Hasbrouck started the meeting with introductions and updates from the commissioners. May minutes were approved.

Jan Root gave updates on the Health Information Exchange: UHIN worked with PEHP on House Bill 46. The PHP go-live date is August 1st. Medicaid is writing an administrative rule for implementing HB46 and their go-live date is September 1st. cHIE is currently at 80,000 patient consents through the clinic collection and estimate somewhere around 300,000 plus through the House Bill 46. She reported success with a payer project. Medicaid initiated the long term care (LTC) uses of cHIE: LTC prior authorizations. It was a two year goal of having 72 LTC facilities at the end of 2013. there are now 86. Doug summarized that the cHIE is accelerating its number of data sources, clinics, hospitals, consented population, particularly with Medicaid and PEHP.

Acknowledgement of Outgoing Chair:

Doug commences Brad LeBaron on being a member of the commission for almost 10 years. He has served as the chair the last two years and before that as the vice chair for two years. Brad has left a mark on this institution and provided great leadership and service. In recognition of that the DOH will present him with a Plaque. Brad thanked everyone and looks forward to continuing this service and had a unique experience being chair. He looks forward to working with the commission board.

The Security Subcommittee's Work:

Doug stated the DHSC's mission and said it's important to understand the mission of the commission and then have it as a frame of reference for today's discussion. A lot has been going on in the state with regards to adopting EHR's, exchanges of information, either at institutional level or beginning to be a community level. Attempting to create standards for digital transmission whether that is claims transmission or data exchanges and it's all good but as we increase that activity, the foundation of that working is the confidence that the state is going to manage data properly and that privacy and security controls are in place. The recent data breach in some of the state systems raised concerns: if that type of thing were to become common, a lot of our e-health efforts could be put in jeopardy. The thought for today's agenda was to get a bit of an update from people that are in the field as to what's going on with

HIT security and where are our potential issues that still remain, what should the Digital Health Service commission's role be in helping to promote any solutions or filling gaps, and if there would be any legislative needs, what that might be and what role we might serve in that.

Barry mentioned that there are a series of 3 audits taking place in the state of Utah. The biggest one is the Deloitte & Touche for all state departments through the Governor's Office. They started with DTS and DOH. Greg Mead added that there are two parts to the Deloitte audit. One is going through all departments in the state and looking primarily from a business side of the applications themselves. The second part is IT specific audit, they're looking at IT specific audit technology services and how we do business. Wu Xu said that other two audits were from Hogan and ECFirst focusing on the HIPPA complaints.

Current Landscape of Health IT Security and Activities in Utah:

Wyatt Parker, HealthInsight, HIT Regional Extension Center, said that part of their ONC funding goes to provide tools and support initial education around privacy and security for small physician practices. They have additional funding to help support critical access and rural hospitals. In that role they're currently supporting over 200 provider practices in the state with about 850-900 providers represented in those practices. Additionally they would like to help about 20-22 critical access rural hospitals in the state. They provide a tool kit with tools that have been embedded by OCR who would be the federal auditor in case of a breach in privacy and security. They are basically given the initial guidance on utilizing the tools, but their funding doesn't go much further than that to where the risk analysis can be performed for them. It's providing the tools, getting them started to meet the meaningful use requirements which are conduct or review a security risk analysis and identify security deficiencies and updates necessary. That's their role as a Regional Extension Center. It has worked out well for the practices that they've been working with but he has seen a big gap in their ability to implement a lot of the things that they are being provided as a tool kit. They have recognized that gap and begun preparing to offer a full suite of privacy and security support services to the area of development of security policy and procedures, guidance through the full risk analysis, mock security audits with summary reports and privacy and security training sessions for staff in the small practices.

Michelle McOmber asked when the funding runs out, are you going to make those tools available to offices? Wyatt answered that some of those tools are already available on their website. They plan to make the full tool kit available on the website as part of their general education.

Doug clarified with two additional points: The current focus in terms that is subsidized are primary care practices of a certain size, so specialty practices of that size are not currently eligible for subsidized security services. He asked Wyatt to talk about what that segment is doing.

Wyatt said they've tried to get into all the specialty association newsletters and conferences to make them aware of these tools that are available to them. They've recognized that a small group is actually willing to pay for those services so they began providing those services as a sub-contractor through UHIN to specialty practices in the state.

Michelle McOmber, UMA said that this security issue hasn't been their top priority even though it should be someplace up there but it's a matter of where the board wants to go. This is something that seems like in many physicians' minds that that it's somebody else's problem and in all fairness physicians have so many things that they have to do and that have more to do with them being paid and

being able to treat their patients than this security piece over here. The majority of the physicians don't even have it on their radar. Many physicians are recruited to being employed and she assumed those entities are taking care of that. There's also a majority of physicians that are not in that category. Some don't have the time, they don't have ability to worry about something extra and implementing and keeping up it. It is constantly adding on "little" costs.

Scott Horne, UHA, said that in several ways the hospitals are similar to what Michelle was talking about in that they've got their system hospitals that are handling security issues. UHA has spoken with them on various occasions. UHA also has the independent and small rural hospitals and he thought they do need the extra help. There are about 10 or 11 independent small hospitals that he believed would be the perfect candidates for security services. They're getting credit for ONC to work with 20-22 intermountain facilities and small clinics that feed into those hospitals. It's segmented enough that they could focus their efforts and get quicker results.

Jaime Steck, Central Utah Clinic, said with everything happening with the clinics, including trying to qualify for all of these incentive programs, there are two things that really worry him. One is that it's the secure access of the systems themselves and the secure access of the data. Knowing that Meaningful Use was coming up we knew that Item 15 there was to actually perform that risk assessment. Last fall we hired a company to come in and do just that. With probably about 15 hours of interviewing him and some of his staff. He just turned the consultants loose and told them to go find the problems. Probably about 100 hours later the consultant came back and handed him a large report saying here's what we did and here's the systems we found. All of them are PHI endpoints and what is lacking of security at each of those endpoints.

Jaime said that this initial report came up with about 39 different items varying from high risk to low risk and exposure of things that we needed to look at and do based on that risk assessment from the government standards. Since that time we have been focusing on those high risk items. Now we're working on some of the harder items such as having a system administrator in place making sure that all of the servers are patched and up to date. Right now I'm working on making sure that hard drives on laptops could be encrypted. He continued to say that getting the education out and getting the word out is one of the harder things, and that education is the key. It's a new arena for HealthInsight to provide marketable services.

Doug said I know that SLCC has credential process courses. He asked about their current training and if it encompass this privacy and security piece. Sherrie Loewen, Salt Lake Community College, said we had an HHS grant that using a non credit bearing program that was open access through the ONC. We have now moved through a Department of Labor's grant in the next two years, to a credit bearing one year certificate program, where individuals will have the HIT credentials walking out the door. We're in the process of developing that curriculum.

Weston Tolman, the U of U, said users need education and the focus should be on the education of students, faculty and staff. Focusing on students, so they are exposed and they understand what they're actually dealing with. There's a disconnection to students: PHI seems just numbers but it's actually patient data. To us understanding the implications of the data is important because they are dealing with phones, laptops and tablets. If we can teach them in the beginning what they're dealing with and how to respond and handle it, then it gives us the ability to put out more educated users. We are seeing success rates in the faculty and staff. We've been training them and letting them know what's been going on.

Students have to understand that they're part of the equation and responsible for their data and devices. He then talked about email education on devices like cell phones for teenagers.

Group Discussion:

Doug highlighted three things for the discussion: identify gaps, give suggestions about the gaps, and make suggestions about legislation if needed. In terms of gap identification, we've heard a couple things, one is education awareness and that's probably at a community level, not just small providers. The other gap is a focus on some of the smaller practices that have less resource and we've heard that a piece of that is a subset of education. The third was even if you make the services available with a cost, is there a mechanism to subsidize some of these costs beyond what is currently available.

Wyatt said we have a good base for an article that would be the beginning of some of this awareness to the community, if we could include, we don't have this piece yet, but we have the Phoenix cardiac surgery report on their breach which gives a very good summary of the settlement memo that states the problems that were found. These really would hit home for a lot of these small practices. We could bring in the Medicaid breach elements and then we could go to the offering of tools that are available. Go to the additional support services and list what those options are.

Doug mentioned how he talked to Sharon Donnely prior to this meeting and it sounds like there was a collaboration with the state and UMA about 10 years ago prior to EHR adoption. She also commented that there might be an opportunity to use Medicaid funds for some of this type of education. Michelle said I think we can investigate it but was worried about the cost impact on the state budget with the DOH data breach. Wu mentioned that the provider security education relates to security on cHIE as well. Today's discussion emphasized importance of statewide privacy/security education; and different training programs (i.e. HealthInsight and SLCC) are in place. Shall we focus on coordinating training and propose training strategies? Mark Munger's idea of having a white paper to summarize the landscape and recommendations could be a good start.

Felix Littlefield is the Program Manager for the HIT program at SLCC. He addressed the gap for education. He wanted to make sure that there is a need for IT security education. There are different HIT areas every semester in SLCC. He will examine their course curriculum to include security.

Jan mentioned that there are a number of entities that offer privacy and security certificates and you might just go out and look at those. In some respects if you are going to be an IT person in healthcare you kind of need to know this stuff because you are a covered entity and are theoretically supposed to comply with the entire HIPPA privacy and security.

Felix Littlefield said it seems like HIPPA training comes after a student gets in workforce and it should be a part of the education upfront for a student.

Wrap Up:

Doug summarized the discussion for actions. First, we need a subgroup to work on a draft of white paper and that white paper would identify what we don't know about the current landscape and gaps so we could try to fill that in. Secondly, we begin to make suggestions about where we see gaps. We should start with what we have already in place and what we can gain through some collaborate efforts. SLCC curriculum might be a nice attachment.

Henry mentioned that at the bank they do a lot of compliance requirements and are required to do numerous different compliance trainings. If there are thousands of healthcare employees that have to go through this type of training, can we coordinate to go through the same content, getting the same information, and through similar methods/tools? Participants supported Henry's suggestion.

Meeting adjourned.