Utah Digital Health Service Commission Meeting

Thursday September 6, 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: Scott Barlow, Henry Gardner, Doug Hasbrouck (Vice Chair), Chet Loftis, Dennis Moser (via Phone), Mark Munger (Chair), Jan Root, and Nancy Staggers
Members Absent: Natalie Gochnour, Deb LaMarche, Brad LeBaron and Marc Probst
Staff Members: Humaira Shah and Wu Xu(UDOH, OHIDS)
Guests: Patricia Carroll (UTN), Courtney Dinkins (AUCH), Charlene Frail-McGeever (UDOH), Felix Littlefield (Salt Lake Community College), Michelle McOmber (UMA), Craig Nelson (LDS Bussiness College), Wyatt Packer (HealthInsight), Deepthi Rajeev (HealthInsight), Robert Rolfs (UDOH), Aimy Sawaya (AUCH), Jerry Smith (UOU), and Weston Tolman (College of Pharmacy, UofU)

Introduction and Update:

Mark Munger thanked all the commissioners for attending the meeting and asked everyone to introduce themselves. He also thanked Doug for chairing the July meeting. He welcomed the guests from different avenues of the states to talk about their educational initiatives. He asked for an update on the security audits that are taking place in the state of Utah. Wu Xu reported that the consultants finished risk assessment for the DOH and now were working with other state agencies. They used the NIST security framework and made recommendations in improvement in each area. Six specific initiatives were suggested to DOH.

Mark asked for a motion of approval for the minutes, they are seconded and approved.

Meaningful Use Stage 2 Core Objectives for Security Analysis:

Wyatt Packer explained that the Stage 1 Meaningful Use (MU) has the requirement around privacy and security of protected health information. The objectives and measures of Stages 1 and 2 include addressing the encryption, security of data stored in certified EHR technology. The MU 2 core objectives also include security analysis - conduct or review security analysis and incorporate in risk management process. Wyatt discussed compliance with 42CFR Part 2 with state mental health privacy requirements and said confidentiality laws are outside the scope of the rule making relative to Meaningful Use. There are no changes relative to meaningful use until 2014. Most of the changes, beginning in 2014, are relative to new requirements, new measures and an increase in thresholds for existing measures.

Commission's White Paper on HIT Security:

Telehealth: Patricia Carroll presented that Utah Tele-health network is based on a membership with different health care institutions throughout the state. We have unrelated sites so security is of utmost importance to us. We have a shared information and security policy in place. We also have a Business Associate Agreement in place with everyone. We work in coordination with the University of Utah IT security team. We require all of our team members to do the yearly HIPPA training, with particular attention to train new sites, which is to look at the telemedicine considerations with privacy. We run into the problem of sharing data and that's often done with faxing and emailing and we do use the U of U's PHI encrypted emailing system for that. We have a specific consent form and a waiver form that providers can use for such technologies as Skype and Face Time. Jerry Smith from the U of U Hospital IT, commented that encryption is a good fix for security standards. Patricia continued to say that there

are physicians who want to use iPads and such technology so we are really moving forward with that. We are also looking at social media applications. Utah Telehealth Network being a part of the U of U hospital, we follow all of the policies from the hospital for both security and patient confidentiality. More and more providers and patients are utilizing mobile devices. We have no idea where the info is stored and on what servers; so we deem it not secure.

Higher Education/University of Utah: Nancy Staggers presented that the privacy and security are really regarded as a worldwide requirement for any informatics specialist but however it usually is just a bullet point without details. The topic of security is considered fundamental to informatics at the entry level. The topic will vary according to the educational institution because that's academic freedom. She then mentioned how HIPPA programs are a part of every single educational and service organization. Academic institutes develop an educational module that would include hopefully the latest things. Nancy pointed out that there's another dimension and that is privacy and security with research, where had a gap in the past. Research's privacy and security are an issue even though the IRB talks about de-identified data. It is pretty easy for a researcher to accidently have PHI, even though you are not supposed to, and use cloud computing as a drop box, which might be a potential gap in security. There is little educational material publically available in informatics education, the professional training, and even at the entry levels, because that is considered intellectual property, it belongs to the institution or the instructor. Another potential gap is that people who are in formal educational programs have a better shot at getting the latest scoop. People who are practitioners and out of school for a long time are where the gap might be, so we'll be dependent on each organization adherence to policies and knowing about the latest meaningful use.

LDS Business College: Henry Gardner introduced Craig Nelson, VP for LDS Business College. Craig presented that they focus in three main areas: business, technology and health professions. What they try to do is focus in the core of those three programs but then try to see where the overlapping areas are. He said, "Today I've heard a security concern about the health practitioner but also the business training of health management. So in essence we have to have an aligning of those three circles: Technology, the business approach of the management of the system, and then the practitioner itself. We really want to revamp our programs such as technology and health programs. Our bottom line is this if you need something as an industry; we are going to respond to it.

Salt Lake Community College: Felix Littlefield addressed that they are in the process of starting a certificate for health information technology. One of the components will be tackling some of these security topics from the very beginning. Mobile and physical security is in line with some of the healthcare IT certificates. There will be direct modules that will not just be knowledge but can apply security facts as well. Furthermore, we want to be in line with the other institutions. The idea is to make the certificate and the training to meet in the industry's need.

Learning from the Banking Industry: Henry discussed the five HIPPA compliance activities organizations must undertake today. He emphasized training workforce members including management. He shared the compliance management at the banking industry. In the banking industry we have a lot of moving parts, complexities and security and privacy. There are several employees, groups and banking structures, branches and departments. There are so many different job areas and each one has its own different area of compliance, security and specialty. We're extremely regulated. He handed out a job family-and-compliance training grid and explained how they have a tracking mechanism and it shows what classes you are suppose to take or what job group your are in, as well as shows your status.

Southern Utah University: Dennis Moser presented his meetings with the deans and department heads in their business management, computer science and nursing programs. The nursing program was pretty much what I expected with the privacy, security and patient confidentiality. HIPPA and all of that are covered. Nursing programs also get a double dose of it when they do their training programs throughout the facilities and they have requirements at the facility level that the students have to go through. The second thing that I discussed was the computer information systems program. These are primarily technical type programs and privacy and security are covered in quite a bit of detail in all the different degrees and course work within that program. In the school of business (degrees relating to management, marketing, economics and finance), it was a little bit different response that there really wasn't any significant privacy or security requirements in any of the coursework. The exception to the security education was in the accounting information systems program. There was a required class that had quite significant content on privacy and control and that class is an elective for the business classes. I think a lot of this mirrors what both Nancy and Henry have talked about in that the nursing type's programs and health programs, which students get a big dose of. I think a lot of the people that over see our IT programs systems have the security in place. He talked about how some controls and systems weren't in place and thought that that was where the data breach occurred.

Discussion: Jan shared her notes on the speech from Michael (Mac) McMillan's, National Chair for HIMSS Privacy and Security Policy Task Force, at the UHIMSS meeting on August 17, 2012. Healthcare is going through the evolution that banking went through. The majority of breaches are mobile devices. Stolen unrestricted laptops are still the leaders in health data breach. But mobile devices breaches are getting up there. Furthermore, more cyber incidents occur in healthcare than in any other industry. On the black market a medical identity is worth fifty bucks. Average spending for IT security in other industries is 6-12% and in healthcare is less than 3%, unless you've had a major breach. If it's a major breach then they get up with industry standards, even though that hasn't happened for most companies.

Mark expressed his major concern as the smaller group practices that are not completely aware of the privacy and security that they're under. The intention here for the white paper is (1) to try to give all of us in the commission short talking points that we can do to give to practitioner groups around the state to give to the legislature and to other enterprises, and (2) to protect those small physician groups from as much as we possibly can. Further, I appreciate what came from the University of Utah group. We need to get this message out to the practitioners. Also, regulations and statues updates might be necessary. We've identified several gaps. I'd like to get some thoughts about basic agreements that may be in place that are important for physician groups to worry about as they look at cloud computing or they look at these types of things. We're going to try to have this ready by November.

E-Prescribing Task Force:

Mark mentioned that they had a meeting of the Utah electronic prescribing task force; it was a subset that was deemed from the health commission a few years ago to look at just electronic prescribing. We talked about a communication issue between clinics and pharmacies. That is specifically that physicians told UHIN that they don't have a way to communicate with the pharmacies when they are actually doing the e-prescribing, so pharmacies don't really realize that there are a number of e-prescribing prescriptions coming into their site. Therefore, pharmacies are not responding and then the patients don't get their prescriptions. We're going to communicate with the UMA and REC for possible solutions. Utah has 30% of wired prescribers, with 22.6% of them e-prescribing utilizers. There were three things that we set out for this task force; the first one was increase capacity of e-prescribing. We're starting to supplement and support the implementation of the DEA from rural to handle identity proofing. Also, the vendors are now starting to step up to the plate. He continued to say that the state of Utah through DOPL is not going to

step up to do identity proofing. The last one is a financial barrier through Surescripts, which is not an issue anymore. ONC has sunset their state e-prescribing community of practice. We put this forward to the group of people that were at the meeting, including Jan, Wyatt, Francesca Lanier, Wu and myself. We all unanimously agree that this probably should come to an end and so should this task force. This was put forth through this commission so I need a motion and a vote to actually sunset this e-prescribing task force.

Motion made and seconded, the motion passed.

Utah HIT Governance Consortium:
Dr. Rolfs mentioned that the HIT governance consortium was set up originally by Dr. Sundwall as a way to coordinate the various projects funded under the HITECH act. As that progressed we realized there's a lot of duplication of coordinating functions between that group and this group. The commission has a larger body of people who are involved and so issues come up that need some sort of community action that would benefit from being brought here. We decided to sunset the consortium as a separate entity and have it meet with this group. The commission can have a standing item on your agenda for each meeting. Individual ARRA projects can come to this group reporting how things are going. Projects can raise issues and identify anything they would like to be identified. The commission accepted this proposal.

Other Business:
Mark accepted Jan's suggestion to look at the cHIE enrolment across the state in the November meeting. The commission can explore whether we need to rethink the way we're actually enrolling potential patients and communities into the cHIE.

Meeting adjourned.