Electronic Standards for Privacy Consent Directives
Technical Assistance for Medicaid and SCHIP for Health IT and HIE Webinar
8/27/08

This is the Technical Assistance for Medicaid and SCHIP for Health IT and HIE Webinar. We are at about 50% of those who registered. We will wait about one minute and then we will begin with today's session. Good afternoon. We are going to go ahead and get started. My name is Walter Suarez. Jonathan Coleman is our moderator, and he is having some trouble joining us at the moment. We are going to go ahead and get started.

Can you hear me now?

Jonathan, you are in. Go ahead.

I do apologize for the technical difficulty at the beginning. Welcome to the webinar on electronic standards for privacy. I just want to mention my name is Jonathan Coleman. I am the facilitator for this Medicaid and SCHIP technical assistance webinar. This [webinar] will focus on managing directives and electronic standards. We are having some logistics issues. As a reminder, this webinar will be recorded and all participants will be on mute. If you wish to unmute, please raise your hand. Please send your questions to all panelists. That's where we can supply summarize the question and vocally relay them. Also, e-mail Nicole if you would like a copy of today's presentation. The RTI team is currently in the process of posting all the presentations. Once again, the URL for the website is posted on the screen (www.healthit.ahrq.gov/Medicaid-schip) . If you have not already, you can register for the project listserv to receive announcements about program updates and upcoming webinars. The URL is on the screen and there are instructions for joining the list serve in the body of the message.

At this point I would like to introduce our speakers for today. Walter Suarez is president and CEO for the Institute for HIPAA/HIT Education and Research. He provides consulting services to health care providers, organizations, public health agencies, and vendors in the areas of health IT adoption, health IT exchange information, data standards, privacy and security standards and also HIPAA standards with regard to transactions and that national program identifier. Our other presenter is John Moehrke He specializes in durability, security, and privacy. He is primarily involved in the international standard effort related to business. He is co-chair for security and privacy at HITSP, as is Walter. He is a representative for numerous national and international standards organizations. At the end of the presentation there will be ample time for questions and answers. Once again, if you could use the raise-hand feature to ask a question. Then we will proceed with the question. With that brief introduction I would like to turn the presentation over to Walter. Walter, thank you very much.

Thank you, Jonathan. Well, what we want to do during this webinar is basically four things. We want to review some of the core privacy concepts that are applicable to what has been the development of interoperable standards would for patients' privacy and consent directives. We want to introduce you all and discuss the history of the health IT

standards panel construct that was developed. It is called managed consent directives to establish national harmonized interoperable standards that can be used to electronically capture, maintain, and report privacy consent directives given by patients or consumers. Then we want to review some of the ways this construct can be and has been implemented through the work of HITSP as well as discuss the applicability of the constructs to Medicaid programs. Next slide.

So some basic concepts that we want to discuss and cover. What is privacy and what is security? These concepts are very integrally related. We think of privacy of the formation as an individual's (or organization's) right to determine whether, what, when, by whom, and for what purpose their health information is going to be collected, access, used, or disclosed. It is the ability of the consumer to determine the inspectors. Security is broadly defined as the set of administrative, physical, and technical actions that are used to protect the confidentiality, availability, and integrity of health information. In that respect we really insure the privacy of the health information. Next slide.

Many of you have seen or heard talks about this basic concept around security, computer integrity that is related to what we are doing with respect to privacy. The confidentiality concept focuses on the property that data or information is not made available or disclosed to unauthorized persons or processes. Integrity relates to the property that data or information will not or has not been altered or destroyed in a manner that is not appropriately authorized. Availability relates to the property that data or information is accessible or usable upon demand by an authorized person.

The next slide. Let's cover a few of the underlying realities. We at the HITSP used these and looked at them when framing and developing this interoperable standard for privacy consent directives. We are very familiar with the fact that medical records and medical health information are among the most sensitive information that a person has. It is indeed an industry and a field that is very much information driven, health care that is. It deals with everything about the health care system which relates to and involves the information. Certainly information itself, the information is used and the information in health care is much more complex than what is used and handled in other industries. More complex in many ways, not just in terms of the amount of information, but the type of information and the frequency by which information is collected. Certainly health information is central to the relationship between a doctor and his or her patient. Privacy and security of health information are core elements in that relationship. Next slide.

We are also familiar with the fact that health care is a very complex system. But there are many actors involved in the health care process, certainly starting with the patient and provider involving all these other entities and individuals within those entities, employers, government, public health researchers. There are various types of information: clinical, medical, financial. There are various processes that relate from collecting and creating information when a patient comes to a doctor and the doctor is taking notes or making notations in the medical record to maintaining and then accessing and using and disclosing that information. There are also different purposes for which information is collected, created, and disclosed. There are payment and operation

purposes and a whole array of other purposes including public health research, legal, and others. There are many places where health information resides—physical as well as a virtual, if you will. There are a lack of common elements, critical infrastructure such as identifiers and some other standards, vocabulary and others. We have more and more of those coming up, including identifiers for providers, for example. But we still lack the unique identifier of an individual, the consumer, patient. And we have a number of vocabulary standards, for example. We do have more than one. And so there is that type of complexity around standards and identifiers. Next slide.

There are also many laws that affect how the privacy of health information is maintained. Federal laws started with HIPAA but involve many other laws, the Privacy Act, mental health records, public health information laws. There are state laws and in many regards we are continuing to create a patchwork of different types and different levels of protection. A few of them address health, privacy, and security in a comprehensive fashion. Then there are different policies and practices used by entities to collect and use and disclose health information that have been created and are used by those organizations. Many of these policies and practices go way above and beyond what the federal and state laws require. That adds to the complexity of this structure under which we work to develop this standard. Next slide.

Then there is increasing complexity. There is the standard use of electronic health records and the increased involvement of electronic communication to exchange information between the different actors, patients, health care providers, and others. There are an increasing number of electronic networks, regional, local, state, and then the Nationwide Health Information Network, which add new dimensions to the protection of health information. Then there is, of course, the evolving of personal health records that are also adding yet another perspective to the privacy of health information. All of them related to the way electronically we collect and capture and use privacy consent directives. Next slide.

Current practices, we all know that HIPAA has generally defined the floor for uses and disclosures of health information. We probably are all familiar with the fact that HIPAA in legal terms did not require consent for many uses or discloses. All of those related to treatment, payment, or operation do not require consent under HIPAA. HIPAA refers to the use of an authorization that is required for very specific uses and disclosures. But HIPAA, certainly when it was established, did not take into account several of the new emerging issues, including electronic consent, the expectation and the concept of granularity of consumer controls. How deep and how specific can consumers control various aspects of their health the formation? The electronic health information exchanges that are emerging and evolving across the country and the existence of personal health records—all of those are elements that the HIPAA did not cover specifically. And as I heard earlier, there are a number of other federal laws that define the use and disclosure requirements for specific types of data for specific types or purposes. There are also program-specific privacy protection requirements (such as within Medicare and Medicaid). Many state laws establish additional requirements for when privacy consent is needed. Some require consent even for treatment, payment and

operations, Still most are silent about electronic consent, granularity, electronic health information exchanges, personal health records Next slide.

Now, most consumer privacy, as we are familiar with, is still conducted via paper forms. General consumer privacy consent forms are usually offered at the initial point of care (whenever that type of form is required). Then there are additional patient consent or authorization forms that are used for specific health information that is required at specific point of care or points of time during the care and for specific disclosure purposes. There are no standard paper consent forms nationally or even within many states. Each organization/program has its own form, and some states are beginning to establish a standard form. And then essentially each organization and program has developed and establishes and uses its own form for patient consent. Most of the current requirements focus on use and disclosure. When I say disclosure, I am including (within the frame of disclosures) the term access to health information. Very few of them really deal with or refer to the collection portion of health information regulating what and when and how they can be collected. As most of you know, HIPAA referred to privacy in the context of uses and disclosures, not really in terms of collection. They give the responsibility or expectation that the entity that is requesting some data from somebody will be requesting the data, the minimal amount of data that is needed. Next slide.

There are two issues I want to mention very briefly here that affect how we use privacy and certainly how the electronic privacy consent directives standard can be used. One is jurisdictional portability, what I call entered jurisdictional portability. This refers to the fact that consumer privacy consent laws and requirements, and consumer privacy desires and directives in one jurisdiction may not be legally applicable/enforceable in another jurisdiction. So you have consent operating in each organization based on its own policies and procedures that have been created based upon the consent requirements within that state jurisdiction. The differences in consent policy can make it seem risky to exchange data with another provider in another jurisdiction. You can see the picture, just a simple example going from Minnesota to Wisconsin. That provider is receiving vast data in Wisconsin from a provider in medicine that certainly has and uses a different set of policies and procedures that have been created and built based on the jurisdictional requirements. So that type of portability does not exist in our system yet. Next slide.

The other issue is cross-validation. Now, as we move more into electronic assistance and people's ability to create consent at different points, there is the challenge of cross-validating and verifying conflicting consent. So what is the most recent or latest consent the patient has given? Is that the latest or most recent overriding? Specific data for specific purposes. And then ultimately, where can I find it, if I am looking for the various consensuses so that I can do validation verification. Where can I find all of them so that that can happen? Next slide.

Based on this concept, we really came to add a new paradigm. We offered consumers and the health care industry an interoperable standards-based electronic mechanism to collect, capture, maintain, report, transfer, and then act upon consumer consent directives. That

type of flexibility is needed in an environment like the one in which we operate. Next slide.

Let's define what a privacy consent directive is. A consent directive is a record of a consumer's privacy policy, in accordance with governing jurisdictional and organization privacy policies. What we consider a consent directive is a record of a consumers' privacy policy. Privacy policy means a decision of a customer regarding one or more elements on the protection of their health information in accordance with a governing jurisdiction and organizational privacy policy that would then grant or withhold consent to any of these factors: one or more of the identified entities within that specific role, to perform one or more types of activities related to that information (collect, access, use, change, amend, delete); on an instance or type of health information or for a general or specific purpose, such as treatment, payment, operations, research, public health, quality measures, health status evaluation by third parties, or marketing; under certain specific circumstances in some cases (there is the situation of what happens when a person is unconscious and cannot provide those privacy consent directives);for a specified amount of time (the fact that they are ineffective and there is an expiration date); and in certain contexts (as emergency situations). All those are factors that a consensus character refers to. Next slide.

So what are the characteristics? Some of the key characteristics we looked at when we were seeing the development of this standard? Well, these are some of the key factors. We look at consumer-friendly mechanisms, finding ways to allow customers to manage their consents directives electronically in what would be a simple, reliable, secure, and effective manner. We want the consent and consent directives to go from general and overall types of consent to a much more granular type of consent directive, such as for specific data, specific people, specific purposes. Codifiable means basically that consent directives can be defined within the context of a set of standard codes, electronic codes that express carefully what the directive is. These would be machine readable and machine actionable, meaning that it would not require human intervention in order to process. It will allow systems to execute and operationalize as the ultimate expectation, which is either grant or withhold access, use, and disclosure possibilities. They would also be portable and transferable. I mentioned already the concept that we want this type of consumer concerns directive to be able to be transferred and imported into other systems. The expectation is that the consumer consent directives can be electronically transferred to another system. Next slide.

Other key characteristics are: be flexible and adaptable. Be able to turn on or off certain elements based on based on differing levels of jurisdictional requirements. Be valid and verifiable and auditable so that one system can make sure that the system is there for auditing and purposes or record-keeping purposes. And be unambiguous and complete. Certainly this is one of the features of consumer consent directives, being able identify and operationalize the appropriate one when there might be conflicting consent directives. Next slide.

So I am going to turn the podium here to Walter who will then cover the details and specifics on the standards.

Good afternoon. This is John Moehrke. Walter has done a terrific job as far as the kinds of information. I am going to pick up and give you some background on what HITSP is and what we have come up with. HITSP is a volunteer-driven consensus-based organization that comes out of the Department of Health and Human Services. It brings together a wide variety of stakeholders. We have consumers, doctors, nurses, hospital representatives. We have those who develop the health IT systems as well as those that are using the systems. We also have representation from government agencies and those who were writing the standards. Next slide please.

So at HITSP, we take these use cases that we receive. We are trying to harmonize the standards necessary to have made those cases. We take the use cases from AHIC and analyze them as far as what would be necessary from and interoperability only perspective which, you know, does cause some aides to and we are dealing with things like privacies that are very policy based. We look at the technology that would come under a reasonable set of policies. You said it, Walter, describing that reasonable set of policies that we start with. What we create is a couple of different things. One is this interoperability specification, which shows how you orchestrate the underlying standard to carry out this high-level use case. Underneath that interoperability specification we have these things we call constructs, which are the components that we orchestrate within that interoperability specification. And those components really are pointing at specific standards that we expect to be reusable. We expect to be able to provide clarity and interoperability if used with the additional guidance that HITSP provides. As this indicates, we have looked at these cases from AHIC and we tried to gather together the likely standards that would potentially fill the particular reuse we are looking for. While we are doing that, we are assessing whether there are any gaps. We are assessing whether there is overlap with existing contracts that we have already created or whether there are overlapping standards themselves or to different standards or organizations that have done a similar set of work. We will make recommendations where we see gaps that need to be filled. We will make these recommendations down to the standard organization. And indeed, we have some focus often both HL7 and also to two different standards organizations, one very focused on health care and one that is up in the general I T space. So we are actually rather broad and where we will pull standards from. In that and we end up making recommendations. We end up raising these packets. The standards get selected. They go through an approval and readiness process. The end result is that they go out for of public comment through this testing system. Next slide please.

So the security, privacy, and infrastructure committee is the committee that Walter and I co-chair. Glen Marshall is the third cochair. Our goal is to identify, evaluate, and recommend security, privacy, and in fresh directional construct to address the needs of the AHIC use cases. It is important to recognize that we are focusing on the three different things all at the same time. The topic of this presentation is really just that topic in the middle, but clearly it does work across all aspects. So we identify the needs. We do an analysis. Within the HITSP that is called a Tier 2 criteria. There is a fixed set of

attributes that we all look toward within our standards. We are all maturing in a similar way. We produce these contracts. Next slide.

When we are done with that work, the construct is integrated into the interoperability specification which is recommended to the AHIC. Next slide please.

It so that make components, security is the balance such as secure communication. The basics of security that is rather classically known in IT. Privacy are [sic] those elements that we specify under consent reporting or consent management. Then we also have some infrastructure components for managing and sharing documents, four points to point delivery of documents, or for delivering orders or even the authorization request the papers. The next slide please.

So the space in which HITSP works is not only just interoperability, but the use cases that we get are really these interorganizational use cases. Really we look of the classic system today and you have these intraorganizational networks today that deal with specific work flows within an ambulatory clinic or specific were close within a hospital or within an IBN. What HITSP is doing is it is within a step back at this inter organizational exchange. How can we satisfy these larger views cases that really required more to multiple organizations to participate in order to get a particular task done? Next slide.

One of the things that we do as a security, privacy, and infrastructure, we keep in mind not just the things that are supposed to be done, the appropriate actions and people and systems—but also as security and privacy professionals, we are very concerned about the misuse. We also keep in mind some of these other scenarios and try to apprehend them, if you will, tried to handle these misuses as well to make sure that the good guys have what they need. We make sure that the bad guys don't get what they want. Next slide please. This is listing of the current list of constructs, our documents, or components that we have described. And the highlighted one is managed consumer privacy consent directives. We referred to it as the transaction package number 30. That is not all that important. What is important to note is that it is really one of the cost charges that the community has produced among many. We are going to be focusing purely and on that particular cost at this time. Next slide please.

So the consent directive is really asking how we can, within a health information exchange, develop the privacy policies and implement them using the role-based access control or the mechanism that is supported by the system that is there. We are trying to enable the patients to be aware of the privacy policies or consents but also have the opportunity to select a modest a set of these privacy consents, the ones that they want to acknowledge. Next slide please.

So the concept is, how would you, within this interorganizational environment, relate information that a patient has been acknowledged to consent or that the consent is needed yet for those kinds of things? That what we are dealing with. How do you manage the consent in this kind of environment? What we did was look across existing standards. This is one of the areas that we found rather full of accounts. The one standard that we

chose was this basic paper: patient privacy consent standard, which is a rather simplistic profile. Hence the title, basic. That is also indicative of the immaturity of the standards underlying it. One of the things that we did absolutely in parallel with the selection of this particular profile is we imported upon and the standards, organizations, the need to fill these gaps, and the need to make the consent of management system or rich, have the ability to deal with the kinds of variability amongst patients and a must providers, the policy language in a way that can be much more dynamic, much more complete. But we selected this one. It works quite well with that document exchange model that was also chosen on how to manage and exchange medical data. It supports a couple of different environments which I can get into a little bit later. It does indeed leverage the experience that the patient has today as well. Next slide please.

So within this managed consent directive, there are even a set of underlying standards and underneath a sick patient privacy consent that we think is important to expose as well. And we did find that an HL7 standard around the data can send that message and confidentiality code and some consent-related vocabulary and even some role-based action vocabulary as well. Some of these things can be rolled up in order to describe what is being a balanced by the patient. The consent is captured within a CDA document, which is essentially an XML document. Therefore, it is processable by computers yet also this level to a patient or to a provider. It supports an environment that is kind of evolving from the environment's a day where a patient might get a piece of paper that has the policy written out on it and they are acknowledging that policy. You can then scan that particular document using a flatbed scanner and use this particular document type tests to save and image of that signed piece of paper. As of now in an interorganizational environment, somebody in a different organization can actually see the signed piece of paper. They can read it, see what was acknowledged by the patients. So you have this high level interoperability that we have enabled through the support of a scanned document in PDF form. Yes, there is enough information about the policy that was acknowledged that make this machine processable as well. So the system that is over there and another organization can tell that it was a particular policy as opposed to other policies that they may have chosen from. Next slide please.

So not only this can record patient consent, but this can record eight patients choosing to revoke consent. They can choose to acknowledge a policy that says, “I don't want to share my data” or there are some broad conditions like spouse is not allowed access. But this set of policies at a very coarse level can be added to fight within the health information exchange. The patient can have one or more of those active at a time. It is also supported in environments that are not just in a document-sharing mode, but also supportable when that document needs to be placed on possibly a CD-ROM or delivered in a point-to-point fashion. Next slide please.

Along with these consent documents are clearly political documents being shared. It is important that every technical document being shared is described in the data. What kind of the document is this? Is this a document that contains only payor type information? Is this a package that contains general episode summaries or is this a document that possibly contains something that needs to be protected at a sensitive topic level? So what we have

is a set of confidentiality codes that would be applied to the data of all of the chemical documents. In this way we can see that the policy that they may have chosen has allowed specific clauses of documents to be accessed by specific roles of individuals. And we will build that as we go on. Next slide please.

So the next thing that we brought into this construct is a setup permissions that are being defined. You see a snippet here of the list of professions that are currently available. And these provisions can be a part of that policy to set a particular role users would have access to reviewing progress notes. They have that permission. Because this is a standard, when I describe that permission locally within my organization and I convey it as a description of the other organizations, because I have used a standardized vocabulary, the other organizations will understand that that permission has been granted. Next slide please.

I am going to move from the wording to more of a graphical description. I am really just restating a lot of what has been said. What you see here is an environment where you have often the left-hand side all of the documents that have been registered for a particular patient. It is the medical records department equivalent. There is a place where documents are. And the consent that is represented here by the document that has been signed is a dating factor to gaining access. Indeed, when you gain access to the study, it does not mean a full part bonds access but it means that there are certain types of data that are available to certain types of users. There are some aspects here. The next thing we also recognize is that there are cases where patients have chosen, no, I don't want to enable that. They can explicitly authorize an opt-out policy which, of course, would stop that particular action. The next slide please.
One of the things I do with HITSP is a deal with different policy sets. There are other policy sets. So what this says is, I have captured a new consent that has a particular time period to it, and the fact that there is a consent for the next seven days means that the surgery units would be given access to the document. That has been the episode described. So these also can have time durations to them whether it be for a simple office visit, a 24-hour access maybe, or something longer term as well. Next slide please.

Another dimension to this is that we are not just simply capturing a single policy. We have enabled but the ability to have multiple policies. Indeed, you can have a policy that offers normal access to normal people. You can have another policy at the top that says research institutes. No, we are not going to give you access. And there may be yet a third policy has shown down at the bottom that gives a very, very specific access to a particular episode of data to a specific researcher. It does have that ability to have multiple policies, policies specific to enterprises, individuals, and the like. The next slide please.

And again, another view of this is so far all of the consent policies I have shown have been policies that make the consumption of documents or use of documents. The underlying standard we are pointing at is global, but there are other policies that would really date the publication. Quite possibly you may need to have a consent specific to

allowing your facility tub publish a document. That is what this is showing. Next slide please.

Over the last couple of slides you have seen a yellowish egg graphic. I'm sure you are wondering what it is. It is simply a graphical representation of role-based access control. It happens to come from a standard. What it is kind of saying, there are classes of data that would have accessibility based upon the classes of individuals using the system. For example, the blue ring around the outside is a cause of data that is rather broad because it is available to the administrative staff. It might be the billing address. It might be the insurance number. It is those kinds of broadly available implementations. There is another broad category, the information that is being allowed access to become a potential use in emergencies. You can see that this emergency slip is rather thin. It does not need to be that. It is just being presented so that then you see the larger set of clinical data that is accessible to the direct care team. And then you see these little smaller areas that are episodic data or data that is specific to a particular type of case such as the health team data. And then we also recognize that there are a lot of little red diamonds within patient records. These are the pieces of information that the patient only shares with a specific, named individual. They really don't want that detect go anywhere else. Maybe it is with their general practitioner, maybe their gynecologist. Who knows? We recognize that is important. If you like to see it set up on a table, this is the effect the same information shown on a table view as opposed to a picture view. Next slide please.

So I was referring back to before, confidentiality code, data on all of the clinical documents or the documents being shared. And this is related very much with the role-based access control. Within role-based access control you identify a particular type of data that would be accessible to a particular role of the individual. So how did you know in a document-sharing environment, especially across an enterprise environment, how do you know what type of data is in a document? Well, it is because the metadata that describes the document informs you as to what kind of data is in there. So in here you see there is a decade that is being shared. In this case maybe it is a red diamonds type of document where an explicit consent must be captured. This is a policy. It is not one we demand, but it is certainly something we enable. You can see some other documents that are much more typical, the clinical document that is being put in. It has a little hint of blue because clearly the billing department needs to be able to bill for this and the like. Next slide please.

We have been talking about consent. Really, consent is managed within a couple of different environments. The first one is where you are publishing these documents at some time in the past and that they are being pulled sometimes when they are needed. There are other environments where you need to send the consent from one place directly to another. Don't let your intermediary see it and then we also recognize that the CD-ROMs are really a very good exchange model. Patients can carry them with them. Couriers can carry them. We need to be able to support all of these different environments, and we have done that through a simple set of common infrastructural components. And indeed -- one more quick, I think. You can see that within the HITSP

environment we recognized there is the sharing Internet point-to-point environment and this interchange of media environment. Next slide please.

So what I have kind of laid out is what we currently have delivered within HITSP. You can see that there are some gaps that really need to be filled. We really need to be able to support better coating for confidentiality, more complex policies, more extensions, how to deal with the other environments outside of the document sharing. We need to better enable patient access. How do you deal with the fact that a lab result is a direct indicator that a patient has got a dramatic problem? Well, that must be discussed with their general practitioner before the patient is allowed to see it. How do we deal with that? How do we deal with topics of low sensitivity? How do we deal with topics of high sensitivity? How do we deal with topics where the patient himself is the one reporting the data? We need to come from a consent perspective, support inclusion an exception and obligation and be able to capture this in a way in which the patient understands what they are requesting and that the system has the ability to enforce those dynamic policies. Next slide please. At this point I will hand it back to Walter.

Thanks. Can you hear me?

Yes.

All right. So how does all of this relate back to Medicaid and did the SCHIP program? A couple of points that I think it to be made as we transition into the applicability to Medicaid and SCHIP, this work that HITSP has done with respect to this construct as well as the Security construct has been already accepted by the Secretary. It is in the process of moving into the next stage of a deduction which is, the Secretary of Health and Human Services recognizing that construct and requiring its use across the systems of federal agencies. And so that is already moving along. I think that is an important aspect to consider for the future. There are a number of policy level elements that need to be considered. Of course from the technical perspective, which is what we are trying to focus on today, this relates to the architecture. That is what I wanted to spend a couple more minutes here on.

So the next slide, if you consider really the architecture there are a number of overarching statements and expectations within this new architecture. Basically, among the technical principles there is the fact that security and privacy are being integrated throughout the whole architecture itself. And the architecture insures interoperability within its various components as well as externally with the entities that are trading in these changing information with Medicaid agencies. One has to remember that the original architecture models were developed before HITSP was in place. They had already been looking at the interoperability expectations, that there would be interoperable standards to develop and establish and then to be followed by this architecture. Certainly it will be promoted. Now MITA is also adhering to the federal standards.. And so the expectation is that those standards are the ones being developed by HITSP. With respect to privacy and security HITSP has already been developing interoperable standards in that field, specifically the privacy one, the one be presented today. Next slide.

Within the architecture, the service-oriented architecture that was developed, there are several places that deal with this type of a common-sense directive. At the top left of the screen you will see the of the authentication management utilities service. At the bottom you see the privacy guard and filters orders. That is one place where this electronic consents directive will come into play. At the bottom of the screen, then the Security component's the last item in that, you can see the privacy monitor and access control. There is a place where privacy concern is directed specifically with link. Again, one has to think that the privacy consent directive is one element within the whole security and privacy infrastructure and would certainly includes all these other elements depicted in this diagram from the architecture. So it relates all the access of administration processes that access control.

The next slide also shows how within the architecture the different layers, the three different players that are being established so that at the application and platform level, there are security components. Privacy is really imbedded within that type of security structure where there is going to be the expectation that the privacy consent directives will drive and define how many of these different elements. All these access systems will operate.

The next slide shows also how within the service-oriented architecture that has been established is the type of standards. All these terms on the screen relate to the various standards that are being incorporated within the architecture. All those types of standards are certainly the kind of standard that HITSP is looking at. When that you do not see here—because part of the transition here was that of this was developed prior to HITSP—is the MMPC. We moved into the next stage of adoption and implementation of HITSP privacy consent directives standards. Next slide.

I think this brings us to the end of our presentation. Certainly we see that in an era of increased health IT implementation the definition of interoperable standards for capturing and communicating privacy consent directives is at the core. Those standards that are being developed certainly have to meet some of those requirements I mentioned earlier, including the flexibility to respond to many coexisting jurisdictional policies and program requirements. Since we don't have a national, single, uniform way to look at it, certainly they must be flexible to respond to all of those areas HITSP has been presented and certainly establish the necessary basic privacy interoperable standards. Even though, as Jon pointed out, there are a number of gaps that we are working on with the core set of standards. The architecture is certainly intended and expected to support and use this national interoperable standard. It now is, I think, the time when we will begin to move into the application testing of these kind of standards within the various architecture's including certainly Medicaid. Since there are still a number of caps we need to work on a number of areas for improvement, I think that is where we wanted to point to your participation where you can certainly help, and not just address the caps, but also bring specific requirements that the programs need and have when dealing with privacy. So we are calling upon you to consider participation in to the harmonization efforts. Next slide.

I've just pointed to some of the other ways we can also begin to incorporate this information into your work. HITSP interoperable specifications will be part of the requirements that you would expect from vendors. We ask for certification being the Consumer Health Information Technology. They take the HITSP standard and work on incorporating them into the certification process. So that will be part of that. And then leveraging health information exchange to promote the specific HITSP specifications so that others will benefit as well from the use of the same standards. And if there is a HITSP standard, we could be using now and in shaping those standards. Next slide.

Here is some contact information about how to join the organization. It is free. This is a very open process. Certainly we encourage and welcome you all to the organization. Next slide. So I'm going to return it to Glenn who will be facilitating the question and answer, and we'll conclude the call.

Thank you. That was an excellent presentation. At this point we have a few minutes left. We would like to receive questions for our presenters. If you wish to ask a question you can use the raise hand feature in your chat window and then notified the host and your line will be opened. Alternatively, if you wish you can post your question to the whole panel using the chat window, we will relay that question. So Nicole, do we have any questions queued up on the phone at this time?

We will be glad to relate that. We have one question regarded how you can get a copy of the presentation materials. I'll post that information to the chat window. It is also at the beginning of the slides. We will post all the presentation materials, the audio portion, and the transcript to the project. I will post the linked to that to the chat window now.

Thank you. It looks like Kathy would like to be unmuted, and I can't unmute you.

This is Kathy. I am policy analyst. My question is, since this construct will be becoming mandatory in the future, how do we get ready now to incorporate this construct in our process? You put a couple names on the screen there. I think that is something that could really be helpful to us, but who would be contacts to help us with this process?

This is John Moehrke. I can take a swing at that. The concept is relating directly to a profile where the actual technical details are listed as to exactly what the underlying HL7 standards are needed, how it is supported through Adobe PDF if you are going to do a scanning of an image. I think you are asking the higher level question. You know, from a health information exchange it is important to gather together a team that is going to look at building up the policies that are going to relate to how privacy is maintained within that health information exchange. And this was very much the administrative tasks of looking at international criteria, national criteria, state criteria, and building the policies around that. I think Walter can fill in more details.

Thank you.

Yes, I think, you know, there are a number of steps. One thing we should mention is that the contract document itself (you know, we just did a presentation here today on the contract). We have a detailed description document. That document is available from but the HITSP web site, the web site that was on the screen. I won't repeat it. You can link up to the construct document. Certainly working with of that technology, you are looking at ways on how to incorporate and begin using some of these -- it's going to be critical. And the other part is really beginning to join and participate in the process. The process that we use at HITSP helps all those participants test and experiment with the construction during the timeframe to try to understand the ability to make it mainstream. So that is also another way that you can, you know, begin to move forward now.

Okay. Thank you.

I have one or two more quick points. From a high-level perspective HITSP, we also published a technical note called the Technical 900. It is a high-level document that goes through, how do I build a privately protected environment. There is a note as well that really has a higher view of the environment. The specific contract. The other thing is when you talk to your technology partners, leverage this new vocabulary that HL7 is defining. PP30. When you say PP30 you're unambiguously explaining to your vendor or your organization a specific standard. Take advantage of the fact that HITSP has looked at the existing possibilities and has chosen a particular way to do it.

Thank you.

We do have one more question. The question is, beyond technology, is there any place where the process is being looked at with respects the have tech captured consent from the patient? An organization would be allowed to perform this function.

John, Walter, any thoughts?

I guess I can state that one place I know that there is some work going on is within the different health information exchanges that are being piloted right now. They all see there is a need for capturing a patient consent in a way that has not been done before. Specifically, I have looked at the shared environment that the HITSP leader is in charge of. He is doing rather interesting work with Web interfaces. I think one of the concerns that comes up is that the technology is not necessarily from the barrier, but trying to get a patient to truly feel that they are making a commitment to a policy I think those social issues are an area that we are going to have to get through as well.

Thank you. Walter, is there anything you would like to add?

No.

Great. Do we have any other questions either verbally or through the chat feature? We have time for maybe one more question. Okay. I don't see any right now. If you like we can move on to the closing slide. If there are any additional questions on this topic, you

can contact me or our presenters today, and we will be glad to give you any information you need on HITSP or consent directive constructs. There was a link posted to all participants that will direct you to the PP30 document. Any comments or recommendations for future sessions you can send to this e-mail address, which is on this slide. I believe there is also a final slide, which you can also use to get further information on the project itself and there is also a toll-free number. If there are no other questions at this point, I would like to think AHRQ for hosting this session. In particular, thank you to our presenters for the excellent presentation today. Absolutely to all the attendees and for those who ask such excellent questions. If there are no other closing remarks I will send it back over.

I would like to thank everyone for attending. I believe that wraps up the end of this webinar. Everyone have a wonderful day, and thank you again. Goodbye.

[event concluded]