Hello.

The very slight most restrictive requirements but like everything in life, there are a number of exceptions to this general rule. Since – slide 4 – since we're focused today, I'm entertaining as chair, we are going to start with those confidentiality regulations. You will often find that these regulations prohibit the disclosure of health information in circumstances that it might be permitted under some of the other rules so it's a good starting place because if you can't share information under these regulations, you really don't even need to address the other one.

Slide 5: As I am sure most of you know, the way that this works is that at the federal level, the government has set requirements that state Medicaid and SCHIP safeguard the confidentiality of the data that they hold, and they do that by requiring the states to enact at their own level, laws and regulations or other types of legal requirements that are enforceable to protect this information. So we're going to talk about what the federal regulations require. Many of the states have regulations that pretty much exactly mirror these requirements but also many have regulations that go beyond what is specified at the federal level—so you will find variations from state to state but today, we're just going to talk about the base level requirements of the federal regulations.

The key one is that Medicaid and SCHIP programs must restrict the use or disclosure of information concerning applicants and recipients, to purposes directly related to plan administration.

Slide 6: These regulations apply to this type of information, which includes names and addresses, medical services provided, social and economic conditions, agency evaluation of personal information, medical data including diagnosis and past history, and any information received from verifying income eligibility and amount of medical assistance payments. As you can see, it is a fairly broad range of information and it applies to information that is from applicants for Medicaid and Medicare, Medicaid and SCHIP as well as recipients of these benefits.

Slide 7: Uses and disclosures of Medicaid and SCHIP data are limited to purposes directly related to plan administration, and those purposes include (according to the federal regulations) the following: establishing eligibility, determining the amount of medical assistance, providing services for recipients and conducting or assisting in investigation, prosecution or criminal – civil or criminal proceedings related to the administration of the plan. There are also other restrictions in the regulations.

Access is limited to persons or agencies that are subject to standards of confidentiality comparable to Medicaid or SCHIP programs. The agency must, whenever possible, obtain the permission of the individual or family before responding to a request for information from an outside source. Again, there is an exception to this: when the information is used to verify income, eligibility, or amount of assistance payments, that rule does not apply. There are other restrictions also: the agencies may not publish names or address of applicants or recipients; they must obtain a data exchange agreement to exchange the data, to verify income and eligibility, and there are some others as well.

Slide 9: These restrictions apply to all requests for information, even if it's the source of another governmental body, as long as it's outside of the agency.

Now, as you can see, there might be some challenges in utilizing and complying with these rules and health income information exchange environment and some of the ones that have been brought up during the last couple of years that we've been dealing with this issue. We're going to go into a little bit more detail in this presentation.

The first one is the requirement for individual permission to respond to outside requests for information. Then we'll talk a little bit about the scope of what administering the plan is really about and the requirements that others receiving data be subject to confidentiality standards comparable to Medicaid and SCHIP standards.

I have to say that there is a favorite saying in our office: we have a lot of people who work on Medicaid issues and SCHIP issues and what they often say is when you've seen one state, you've seen one state. So, how these requirements are interpreted right now varies a lot from state to state.

We're now going to cover the way some states have interpreted some of these issues. Obtaining permission. In Massachusetts, they instituted a program where they could share prescription data with emergency departments and they wanted to get that information from the Medicaid agency. They wanted the Medicaid agency [to be] able to provide eligibility and paid prescription history to emergency rooms for treatment upon the emergency room's request. And in order to do that, the user interface that they use in this system captured and was able to capture an oral consent. So they did get the individual's permission to do that and if the person wasn't able to give their consent because they were unconscious or something of that nature, there was an emergency override which allowed the provider to access this information {in case of emergency).

Another challenge was state immunization registries. Slide 12: Many states reported that Medicaid agencies in their states would not share immunization data with the state-run immunization registry because the activity was interpreted as not being directly related to the administration of the Medicaid plan. However, at least one state reported doing exactly the opposite, which was sharing Medicaid with the state department of health that collected and analyzed immunization data; they did that using a data use agreement. This state seemed to be following, this state's action seemed to comport with a CMS guidance from a number of years ago.

Slide 14: (This is kind of like the musician formerly known as Prince); this guidance came out under HICFA, the former name of CMS; it is the Medicaid director's letter and it discusses facilitating collaborations for data sharing between state Medicaid and health agencies. And I've listed a link on this slide for you so that you can go and read the actual letter yourself. It's quite detailed and given our time constraints today, I'm not going to go through as much of this guidance as I had originally planned but when you read it, you'll see that it in general addresses a number of the issues of exchanging health information electronically in the context of the Medicaid agency sharing it with a public health agency. Of importance is that it lists what they

believe are justifications as to why sharing information in this manner relates to, can potentially relate to the administration of the Medicaid or SCHIP program.

So the question probably comes up, well, what weight can you give to this guidance letter? It does provide clarification; it was intended to ensure consistency, it's quite old, it hasn't been reaffirmed, it hasn't been revoked. One option is to seek clarification from CMS whether it still is the agency's position, at least with this respect and whether there's any potential for expanding its guidance in this area.

If you can't share data for a purpose directly related to a plan administration under the Medicaid and SCHIP confidentiality requirements, if you can't overcome that hurdle, then you don't even really need to start considering the HIPAA privacy rule because you're not going to be able to share the data and that's just the bedrock rule right there.

Slide 18: So provided that you're able to get over that initial hurdle, then you'll also have to look at the HIPAA privacy rule requirements.

Slide 19: I'm going to go over these slides fairly quickly because I know that most of you are very familiar with the basic HIPAA requirements and then after we go over those, I'm going to discuss some of the issues that have come up with HIPAA with respect to health information exchanges.

Slide 19: As you know, HIPAA does not cover everybody who handles health information. It does specifically, though, cover health plans and expressly covers Medicaid and SCHIP programs. It covers most health care providers and health care clearinghouses. This term has a very specific meaning under HIPAA and it's not the way the term is used by a lot of lay people.

Slide 20: It covers protected health information, which is information about a person's past, present, or future health, health care payment of – of cumulative health care, (information) that identifies the person and (information that) was created or received by covered health plan or, health care provider.

Slide 21: What information isn't covered? The identified information and information can either be identified through statistical methods or by a safe harbor method under which all listed identifiers have been removed.

Slide 22: In general, HIPAA provides rights for individuals with respect to their protected health information, including the right to get a copy of and amend their own information and to receive a notice of privacy practice and to request limits on disclosures.

Slide 23: It prohibits the use or disclosure of protected health information by a covered entity except what is expressly permitted by the rule or with the individual's authorization.

Slide 24: One of the overarching principles of HIPAA is the minimum necessary rule. It requires covered entities to put forth a reasonable effort to limit the information that they use and disclose to the minimum amount necessary to accomplish the intended purpose.

Slide 25: Recognizing that covered entities regularly share health information with a core group of people for business practices, the privacy rule also allows covered entities to share health information with its business associates without the individual's authorization so long as they have entered into a written agreement limiting the business associate's use and disclosure of information. This can be a memo of understanding; it does not have to be a business associate contract. There are also a number of exceptions under business associates that relate to governmental agencies. For example, if a covered entity is sharing information with another agency that is subject to legal requirements that are equivalent to the HIPAA restrictions, they don't need a memorandum of understanding. There is also a specific rule in the HIPAA privacy rule that deals with agencies which determine eligibility and enrollment to Medicaid and SCHIP plans, for example. And in that case, those government agencies that have those functions do not have to follow the business associate rules either. Now, as a matter of fact, a lot of agencies, even though they're kind of exempt from this requirement, follow it anyways just because having a memorandum of understanding really sets out what the limits are of how the information can be used between the agencies.

Slide 26: This slide explains that the business associate rule is limited to those who perform these functions on behalf of a covered entity and that a covered entity can be a business associate of another covered entity. So there are all sorts of arrangements out there and they can really vary from situation to situation.

Slide 27: We talked about some of the kind of overarching rules of HIPAA. Now we're going to talk a little bit about some of the specific applications and purposes for which health information is exchanged. Of course, the large triumvirate is treatment, payment, health care operations and in general, HIPAA doesn't require an individual's written permission to use or disclose information for these purposes but neither does it prohibit a covered entity from obtaining such permission. That permission is called consent. For those of you who have been involved in this process, you know that the distinction between authorization and consent is often a big sticking point with people. Consent is limited to this purpose, these three purposes, and because—

I'm sorry, Joy, would you say that again?

In this HISPC process, there's been a lot of controversy over the issue of when you use the term consent and when you use the term authorization.

Okay.

They have very specific meanings under HIPAA. But when you start turning into a state law, for example, compared to the meaning in some of the other federal laws, they use different terms for permission. So, what is helpful when you're discussing this, if you get into a discussion with other people about what kind of permission you're going to need to share health information in a health information exchange, you should really be very careful that you say, "we're going to be sharing health information for "x" purpose" and make sure that, you know, like if you're talking about consent, make sure that everybody at the table is talking about [the same thing], for example, we may just mean it for treatment, payment, and health care operations, we don't mean if for other purposes. If they need it for every purpose, that's fine, but you really want to be

careful that everybody understands that the term you're using means the same thing for everybody.

Okay.

Slide 28: There are a number of other purposes for which HIPAA permits use and disclosure without individual authorization.

Slide 29: There are also circumstances under which a patient, an individual must be given an opportunity to either approve or object. Some might apply to a Medicate or SCHIP database because it allows the family or friends or others to receive information directly relevant to the involvement with the individual's care - of payment of that care - without written permission and it also allows exchange of this information for disaster relief.

Slide 30: Authorization, which is written permission, is required for use disclosures not otherwise permitted by the privacy rule and there are specific content requirements for that. There are penalties under the privacy rule. There appears to be a lot of hesitancy to share data in many situations because people are afraid of what their liability might be but as a reality check, I think people should be aware that over 25,000 complaints have been filed and no fines have been imposed to date. That's because there is an official policy at HHS that says that they will try to bring people into compliance before they pursue any penalties. So although there seems to be a large fear of liability, in reality, it doesn't seem that that fear is, at least at the federal level, very well founded.

Slide 32: HIPAA does not interfere with state laws that are more stringent than its standards so that means that operations (inaudible) neither does it interfere with stronger federal laws. So, for example, the Medicaid and Medicare – Medicaid SCHIP provisions that we just went over, which are stronger than HIPAA, remain in place.

Slide 33: For some of the health information exchange, challenges include how is the local health information exchange, often known at the RHIO, treated under HIPAA? What is it? And what are some of the limits on sharing health information in such a health information exchange?

Slide 34: Currently, most health information exchanges are RHIOs—legally independent organizations. They generally are not health plans, health care clearinghouses, or health care providers and, therefore, they're not covered under HIPAA.

Slide 35: This structure has raised a lot of liability issues because people are concerned. Exchanges generally operate through business associate agreements or memos of understanding, at least that's up to the current time.

Another issue, which has been raised by people who want to exchange health data in a health information exchange, is whether the minimum necessary rule applies to treatment. A lot of people know the general rule but it's very important that you read the very detailed requirements of that rule because, although the minimum necessary rule applies to internal uses for treatment, it does not apply to disclosures to requests by health care provider for treatment. With respect to internal uses for treatment, it requires a covered entity to basically have restrictions on who can access data based on how they need the information, such as, role-based access, and it does not

require people to sit down and figure out on a case-by-case basis what information they need to share for any particular patient.

Slide 37: But as a practical rule, again, many stakeholders feel fairly uncomfortable with sharing a whole lot of health information, partially because of ethical guidelines and some of them just because of a fear of information overload. Some health information exchanges are therefore using summary care documents such as the continuity of care record or document, and some are using hospital discharge summaries, which they find to have a lot of helpful information but which is still fairly limited in scope.

Slide 38: The minimum necessary rule and payment are a little different, though, it does apply to uses and disclosures for payment activities. That means that a health information exchange needs to ensure that custom responses for data are limited for payment purposes only to the minimum amount necessary.

Joy, will you accept questions intermediately or would you prefer they wait until the end?

I think they wanted the questions at the end. I'm not sure.

Okay. Okay.

You can always type your question into the Chat so that it's queued up so that you don't forget it and then Joy can address those as well.

One of the areas that's a little bit complicated in the health information exchanges is the disclosure of information for health care operations. A covered entity can use and disclose health care information for its own health care operations purposes without the individual's permission. When you talk about using health care information for health care operations of other parties, it becomes much more complicated. I urge you to read the regulation itself because both entities either had or have a relationship with the individual and the health care operation has to be from a list of specified components such as quality assessment improvement, fraud detection, case management, and some other operation. So the rule essentially says, for some of the health care operations, you can share health information for another person with but only if you had a relationship with that individual. One potential solution, which was created in the revised version of the privacy rule, is the limited Davis Act, which is considered protected health information. It's partially de-identified and it can be used for health care operations purposes without the individual's permission, but it requires a data use agreement, which limits the recipient's use to that information.

Slide 41: One of the larger issues, of course, that lots of health information exchanges have encountered is when is individual permission, often called consent, is required to disclose health information because HIPAA doesn't grant more stringent privacy standards. A lot of the laws that require consent to disclose information remain in place. Those that they include are the requirements for 42 C.F.R. part 2 which is a set of alcohol and drug substance abuse regulations and they require prior written consent to disclose health information even for treatment except in emergency. There are exceptions there and given the time, I'm not going to go into it except to say that SAMHSA ,which is the agency that administers this regulation, is currently reviewing issues of when this information can be shared with entities that provide services such as data

processing and collecting it and potentially what role a health information exchange or RHIO might have.

There are also non-Medicaid state laws such as just some general health privacy laws. Some of them require consent before we can share health information for a number of purposes. Mental health laws or HIV-AIDS laws and other laws that are specific to certain health care conditions.

Slide 45: Some of the health information exchange pilot projects have encountered some of these. (I think I have missed a slide here but I'm not sure.) Some of them have used a general option to participating in the health information exchange to fulfill the state requirement for general consent to share health information. Some have imposed a condition-specific option to share sensitive health information so that they are really trying to share health information—all health information and getting permission to do so from the individual. Some organizations that have tried this and the initial stages, take the following approach: when in doubt, leave it out. And this is an incremental approach that is actually used a lot because it allows the exchange to share general health information and the community will develop trust. They will treat that information and then they put off to a later date how to tackle the tougher issue of involving some of the more sensitive health information. What they're trying to do is kind of get their feet wet and figure out whether and how their systems are working and when they're comfortable they're working well, they'll move on to the next higher level.

Slide 47: Some are currently exploring methods of electronic consent and systems to manage those consents so that we won't be just looking at all of these paper forms and trying to figure out how they operate in an electronic environment. And I'm now going to pass the baton to Walter and we will take questions at the end.

Thanks, Joy, can people hear me okay?

Yes, sure can.

Walter?

Yes?

Just say next slide and I'll the slide forward for you, okay?

Oh, thank you, yes, we're on part 2 and I'm going to switch gears to focus on the security aspects. Joy has presented a very comprehensive background on the privacy policy issues. I'm going to try to focus on security and in the next slide, I'm going to start with really defining what health information exchanges is for purposes of this presentation. Ultimately, it is sort of the consensus-driven definition that is coming out of the consensus conventions stuff project for health IT terms that ONC is working on this year. So this is considered to be a process, it's a process of moving health-related data, clinical or administrative, according to an agreed-upon set of interoperable standards, processes, and activities, across independently operating organizations in a manner that protects the privacy and security of an individual. And the individual's information. So that definition is now becoming sort of the core definition of what we agreed to be an HIE; the key operational term is interoperability or interoperable standards because I think that's what adds the new challenges with respect to security.

Next slide. I think we're going to skip this slide in interest of time. This is just a comparison between the RHIO and HIE and this project's right now underway of helping define and standardize the standard terms that we use.

Next slide. Health information security continues to be a very critical aspect of creating and operating HIEs and most of what has happened in the past with respect to HIPAA, to security and particularly with HIPAA's security, has been related to the internal processes and policies and systems within an organization. HIPAA security really provided that framework but it did not and does not provide any framework for the secure or security of HIEs. It does provide, to a certain extent, some of the foundational components that entities participating in HIE will bring to the table.

Next slide. So, what are some of the unique things that relate to security in HIEs? Well, certainly the bigger challenges come across in these three bullets on the slide are: interoperability of the security systems, risk and liability, and trust. Certainly, there are many other elements, particularly inside interoperability of security systems. We'll talk about all of the aspects of authentication and authorization across systems but ultimately these three seems to be the core, external security issues that are brought uniquely by the external aspects of an information exchange.

Next slide. Here are a few examples (each is related, for example, with the interoperability): is my user identification compatible with your user identification or do my authentication "standards" work with yours? Or do we have comparable access control policies that we can use?

Next slide. Here are some examples of risk and liability issues. What are my additional risks and liabilities when connecting and exchange data via HIE? What are my liabilities if there is a security breach of data that I have used or submitted to an HIE?

And then with respect to trust, really the concept is that HIEs, the more than anything else, require some level of trust between the entities—so what is the minimum level of trust that I should expect in such exchanges and in an HIE agreement and how will multiple chains of trust agreements work in HIE environment? Those are some of the core questions around the three measure issues.

The next slide tries to present the concept that a lot of organizations have put emphasis, time, and effort into protection of internal information resources, data policies, procedures, practices, systems, architecture; it's very strong internally. The key issue is between these two entities—when they exchange information across and, building upon the previous slide, interoperability, security, elements, risk and liability and trust are sort of the core there.

Next slide. This next slide, which is information security, is the core concept; this is basic background, information, security. Ultimately, the overall goal of that information security plan is to safeguard the three bigger components: confidentiality, integrity, and availability of information and systems. And the definitions of those are listed there; we're going to move to the next slide in the interest of time now.

But this one, I do want to spend a few more minutes. I define the five cornerstones of information security with an organization; the first and foremost are security policies and procedures. You know, in many respects, when we talk about information security, we tend to refer to information securities, about 80% policies and procedures and really only about 20% technology because most of the things related to security relate to the establishment of policies and the implementation of procedures and consistent implementation of those.

The second cornerstone is the security architecture: establishing and maintaining the technical and system applications hardware, all the technology that fulfills the purpose of protecting the information and assuring the confidentiality availability and integrity of the data.

The third cornerstone is the assessment and audit, an ongoing process of making sure that security risks are identified and accessed and the proper protections are in place.

Next slide. The fourth cornerstone is accountability and oversight, basically establishing and assigning clear, defined responsibilities, and authority for those responsibilities to monitor the compliance with those security policies and procedures.

And the last, and probably one of the most important ones is training and awareness, making sure that staff internally are aware of the importance of security and empower staff with appropriate skills to meet their work needs.

Next slide. I'm going to talk now about the information security related to Medicaid and SCHIP participation in HIEs. T next slide shows the four major aspects related to this. The first one (which I'm going to try to skip a little more because I think Joy talked quite a bit about it) is the policy references, the federal and state laws and program regulations and requirements that define the security components that need to be in place.

While mentioning a few things about Medicaid and SCHIP architecture with respect to security and its structure, of course, interoperability, and try to focus more about the availability about this interoperatible security standards for HIEs. And also privacy standards.

And then [I'll] mention a few things about, you know, HIE agreements, risk and liability issues. So those are sort of the four areas around security that are key security factors affecting Medicaid and SCHIP participation in HIEs.

The next slide. Again, this elements are referenced already by Joy but I wanted to emphasize here the security aspect. Just like there are a lot of federal and state regulations related to privacy, there are a lot of federal and state laws; for example, HIPAA security is certainly one example but there is the Federal Information Management Security Act or Security Management Act, which applies particularly to federal agency systems but it is very directed to the security protection of resources.

But HIPAA, ultimately, in health care has presented sort of the key security aspects, and the requirements established are the base level of security for protecting internal resources, although one of the challenges has been the scalability, flexibility, and the reasonable and appropriate provisions in the security regulations have certainly allowed for the multiple variety of internal security approaches to be used and has created some of the challenges for interpretability

purposes. And there are certainly no federal regulations established at this point that define security requirements for HIEs.

Now, with respect to state laws, a number of states have actually passed state laws requiring the adoption and use of security standards and certainly they apply to different things. In many states they're applicable to only industries; in some states, [they are] applicable to government assistance specifically. Some of those state laws relate to specific health care industry issues and even specific security issues within those industries like breaches, security breaches and what needs to be done in those situations. So there are state laws that need to be used as reference from a security prospective. The Medicaid and SCHIP program requirements with respect to security - again, there are a number of program requirements that are ultimately reflecting federal and/or state regulations that farther limit the, you know, ability of sharing information with others on Medicaid and certainly Joy referenced a number of those.

Next slide: We'll start with the MMIS and MITA architecture and then security components.

The next slide highlights some of the principles around MITA particularly in the current evolution of the MITA architecture. There are a number of technical and business components that focus on security and privacy; these are examples of the ones that are found in the MITA architecture. Security and privacy must be integrated throughout the architecture. Model architecture ensures that this MITA model architecture ensures the interoperatability within the various system components of the architecture itself.

And then there's also the concept that interoperatability standards are to be established and followed for the ability of MITA to receive data externally in a HIE environment. Ultimately, MITA is also one of the principles to promote the secure data exchange, make sure that it is ordered and promoted.

Next slide: MITA does have a number of security principles and I'm not going to go into the details here but you have them identified there. A number of those are reflected in all of the different interoperatability components that we'll be mentioning in just a few minutes. So I'm going to skip and go to the graphic in the next slide that shows the core components of the security which goes into the architecture security layer. The MITA architecture is layered into a platform application and service layers, and security is embedded, as mentioned earlier, across the whole architecture. Authentication and authorization services, secure transport, and physical and logical security mechanisms are all built into the structure.

Next slide. So, now we ready to finish up; let's talk about the interoperability of security and then go to the next slide.

And the very first thing I want to present is the definition of interoperability. Interestingly enough when ONC (back in 2004-2005) started to gather information, they asked people, What should we do with respect to the nationwide health information network and interoperability? There were over 400 different versions and definitions of the term interoperability but this one, which is now being built inside this national effort to standardize certain health IT definitions, is becoming the most accepted term: the ability of different information technology assistance and software applications to communicate, to exchange data accurately, effectively, and consistently

and to use the information that has been exchanged. So, it's really the ability of those separate systems, software and applications and others to exchange information to communicate, and that information has been exchanged, it's accurate, and it's done effectively and consistently.

Next slide: This goes back to the original picture but tries to highlight the center which is really the interoperability of security policies and systems.

Next slide: This slide and the next few slides show the core requirements, interoperability requirements that have been identified through a number of efforts. This brings together information from HISPC, the health information security and privacy collaborative project information in the industry and information from HIST, the health information technology standards panel and others, and the core security requirements include these.

The first one is an accountability control, making sure that the system can protect the resources in accordance with policies and prove that the systems are being protected.

The second one is identification and authentication controls, making sure that the person or the system that is exchanging or connecting to someone else is who they say they are,

Access control is the ability of the system to control or limit access by an authenticated entity to the information and factions they're authorized to access.

Next slide: Confidentiality controls are making sure that sensitive information is created, stored, communicated, and modified in a way that doesn't allow exposure of that information. Data integrity control is making sure that the data have not changed in an unauthorized way, whether aggressed or as it's being exchanged. Nonrepudiation controls refer to making sure that the entity cannot later refute the fact that they participated in that act so they cannot negate their participation.

Next slide: Interoperability security requirements are patient privacy controls and this relates back to the patient consent aspect of privacy, the controls that a patient can impose or give us consent directive instructions to enforce the protection of data according to those (inaudible). And availability controls are making sure that the information in the systems is available when needed.

Next slide: From this point on, I'm going to try to focus and summarize the work that is being done nationally to define and develop security standards that are interoperable and that the industry can adopt and begin to use to communicate through health information exchanges, whether regional efforts or national efforts.

So this effort has been the central focus of the health information technology standards panel; its purpose has been to harmonize and integrate diverse standards that meet the clinical and business needs for sharing information.

The next slides show actually a very important aspect of this process, unlike what we had with HIPAA which was a set of regulations that define and require us to use specific standards - for example, the transactions and cosubstandards back in the early 2000 - we don't have that with

the interoperability standards. There's no expectation that there will be a federal law that says that we're mandating the use of this in the industry.

There is indeed a standard acceptance process that has been established in which AHIC—instead of AHIC priorities, the AHIC—the American Health Information Community defined a set of priorities and built a series of use cases that are then presented to HITSP, the health information technology standard panel, to define the interoperability specifications. Then they go back to AHIC's recommendations, who then present those to the secretary and the secretary has a kind of two-step process. The Secretary of Health and Human Services first of all accepts those recommendations and then gives a year to do testing and implementation and at the end of that year, the secretary recognizes officially the accepted standards and then there is a implementation process at that point. And the implementation is done through an executive order of the president requiring federal agencies to incorporate those accepted and recognizing them into their systems; the systems are upgraded and changed.

And that affects other components such as SCHIP and others. SCHIP and NHANE are all this elements that now come to play once the secretary has accepted and recognized those standards and they get incorporated into appropriate credentials, certification process and the testing through the Nationwide Health Information Network.

All right, now we can go to the next slide. In the interest of time, I'm going to try to summarize very quickly this one to at least give 15 minutes or so to the question and answer period. These are the actual recommended and now accepted, it should say there, accepted, it's not HISTP final recognized construct, it's really accepted at this point. The first step has been completed now for all of these, the secretary has accepted all these recommendations and they, as you will see in this slide and the next couple of slides, they follow very directly the set of interoperability requirements that we talked earlier and the specific industry needs to establish some standards. Those are, first of all, the secure communication channeling and channel ensuring that there is a mechanism to connect and to securely connect and authenticate or ensure the authenticity and integrity and confidentiality of the transaction itself. Then there are some terms, technical terms that refer to the actual base standard that is being recommended, those sort of coded terms there, IHE ATNA , or ABTAN profile; those are sort of the technical terms, I'm not going to take time to explain those.

Another one is consistent time, making sure that the system clocks and time stamps and the network computers are synchronized. Another one is non-repudiation of origin ensuring that the origin of a document is preserved.

The next slide shows managed sharing of documents, and in parentheses, you see a HITSP TP13 or C19. Those are the names assigned to each of these recommended and now accepted standards by the secretary. Managed sharing of documents ensures the integrity of the document being shared, in other words, document integrity.

Entity identity assertion relates to the ability to correctly authenticate the identity of a user. Managed consent directive is very important and very significant because this is, in many respects, the first time that the nation is defining a way to codify consent and consent decisions and what we call here consent directives of a patient, to incorporate those electronically, and to

be able to manage those through coding electronically. It is really a mechanism to record consent directives electronically using something known as the basic patient privacy consent or BPPC. A standard profile uses HL7 coding for confidentiality codes and consent codes, so this is very, very significant and very important, and we're certainly working towards the goal of making sure that this can be used and implemented quickly.

The next slide concerns access control; it's another one of the elements. So now that we have an ability to know who (this entity or individual) is trying to access the data and have matched that with the consent directives, we now have to manage how the information or the entity or system accesses the system resources and functions in order to use the data or do whatever is needed with respect to the health information.

And then to collect and communicate security audit trails is another component or mechanism to ensure that security policies are being followed and that an audit trail is created properly and maintained. And so, in summary of the last slide, I think I just wanted to highlight, first of all, the interoperability of security systems continue to be a very key factor in the deployment of HIEs. Even though HIPAA security doesn't directly, build on or establish standards for HIE, it does provide a good foundation for Medicaid and SCHIP and all other entities implementing HIPAA security to participate in HIEs. There are some remaining policy and legal limitations that will need to be addressed for Medicaid and SCHIP agencies, certainly to participate in an HIE. Also, very importantly, the Medicaid and SCHIP systems like MMIS and MITA will need to be able to support this new evolving HISP interoperability security and privacy constructs and we really want to kind of put a plug here for Medicaid and SCHIP to become much more engaged in all of the HIST interoperability efforts. I think that's the one way or at least one of the ways to bring specific needs and requirements from the Medicaid and SCHIP perspective.

With that I think I'm going to turn it back to Barbara and perhaps we can take on some questions, so Barbara?

Thank you, Walter and thank you, Joy, I think those were terrific presentations and I'm sure that we have some questions from our audience. We have a little over 10 minutes left for questions so I'm going to ask Nicole to go ahead and let us know if anyone has sent any questions in through the chat box that we would like to address at this point.

You know what, Barbara, actually I was having technical difficulties. I see one from Christopher Sullivan. Go ahead, I'm sorry.

The question is how is it that CCD (continuing care document) is different from any other clinical data for purposes of HIPAA privacy rule?

What raises that issue is Joy's slide number 38 in which a distinction is made.

Oh, slide 37?

Maybe.

Yeah. How do you put this? The continuity and care document has protected health information in it. Like any other health information, if the information is being shared for treatment purposes,

because it's being shared, it's been requested or it's being disclosed for treatment purposes, then that document does not have to meet the minimum necessary standards. But as a practical matter, what I was trying to point out was that many people are not comfortable sharing a lot of information and so they impose what they consider to be almost like their own minimum necessary rule. They use the continuity of care document to share the information that they think is necessary for providing some basic level of care.

Oh.

Does that answer your question?

Actually no, because continuity of care documents can be used in a lot of different exchanges.

Right. But what I would say was if you're using it for treatment, if you're sharing it for treatment purposes, that's what this minimum necessary rule and treatment proposes.

Yeah.

If you're sharing that document beyond the covered entity for treatment, it doesn't have to meet the minimum necessary rule but it probably does because they're already sat down and hammered out what they think are the data elements necessary to treat people.

Yeah. I think that's a very fine distinction in practice but more fundamentally, perhaps I've misunderstood something here but more fundamentally, health information exchanges cannot provide protected information as far as I can tell. They [do] have not legal protections like an electronic health record might. Is that accurate?

They are discoverable by court process, for example, in a messy divorce or in other situations.

Well, you know, if I may jump in, I think one of the perspective issues is there are health information exchanges and then there are health information exchanges. There is the real concept where there is an entity responsible for that HIE, if you will, and that HIE, the HIE itself, is a process. Someone is responsible for that process. If that process is a RHIO, then the RHIO is. in most cases, considered to be a business associate at the level. When the RHIO has direct contact with patients or things like that, from that prospective, a RHIO is more seen as a business associate subject to all of the relationships with the various covert entities.

But I'm not sure that protects them from court order.

Right.

You're talking about a requirement to disclose the data for a court proceeding.

Yes.

And that's handled under different provisions of HIPAA than the minimum necessary rule.

Yeah. But my question was different. Was it handled at all for HIEs?

I'm sorry, I'm still having a hard time understanding what your question is.

The question is, are there any legal protections associated with HIEs yet?

You mean like the RHIO for discoverability of the information that gets exchanged?

Or , I think your question is broader than that, isn't it?

Yes.

And I think you're talking about what a lot of people have called a RHIO, right?

It doesn't make any difference if you call it a RHIO or an HIE.

Well, sometimes –

He is not under the control of a licensed health care professional.

Okay. All right, I understand exactly what you're talking about now.

Okay. Sorry.

What you're saying is very accurate. You're talking about this entity that's either serving as a central data repository for health care providers.

Right.

Storing information that way or is transmitting that information on their behalf.

Right.

And that goes back to my slide 34 ,which is they're legal independent organizations.

Right.

Health care providers so they're not covered under entities under HIPAA and then your next question is, are they covered? Are there legal restrictions imposed by other laws? That's a very big question. It's very hard to tell. There is nothing that clearly covers these organizations directly in both states. There's contract law and there's things like that but are there a specific set of laws that tell RHIOs what they are (or health information exchanges) what they can do and how they have to behave. Generally, the answer is no.

Yeah, indeed.

Now does that answer your question?

Yeah, yeah, yeah.

Okay, I'm glad we got that. I'm sorry I didn't understand.

Okay.

This is Greg Lemis, a real quick follow on on that. Are covered entities not subject to discoverable legal excavation?

They certainly are.

Okay, then I'm not sure why a RHIO would be different.

The RHIO is not going to be any different.

Okay.

For that matter, neither is a PHR. If you're worried about discoverability, people can get access to medical records through all three of those mechanisms unless that information is specifically protected like some of the alcohol and substance abuse information is protected.

All right. Thanks.

So do we want to move on to Chris' question?

Yeah. Yes. Yes, please!

There is Chris' question which is combined with Greg's. I think Chris mentioned later that Greg probably had a really great way to focus on it but Chris' question is, "Can Medicaid information be used for treatment purposes without consent?" That's in HIPAA and just to add Greg's comment, you know, on slide 5, Medicaid—it says Medicaid and SCHIP programs must restrict the use of disclosure information concerning applicants and recipients for purposes directly related to plan administration, please clarify about sharing clinical information within the Medicaid patient and provider arena so it's the question about you know, use of the data for purposes of treatment without consent in a Medicaid arena.

I would like to say that there is a clear answer to this but there isn't. This is a muddy area and it looks like it's interpreted differently in different states. I'm sure that doesn't surprise any of you!

It's not a help, no.

For one thing, I'm reading this, there's a couple of different lines and inquiries here and I'm going to try and answer them a little bit together. The federal Medicaid regulations and generally in many of the state Medicaid regulations make the agency adhere to all of these confidentiality requirements. In some, they also then have those that pass those through to everybody who, including providers, operates underneath them. However, that is not consistent because I have seen at least a couple of states when they had concluded that at least the Medicaid agency and the provider didn't have to obtain patient permission to share Medicaid data because treatment was an essential element of the Medicaid program. So, there . . .you'd think that there should be a very clear answer to that issue but the answers the answers have varied when it's been addressed in a couple of different states. Is anybody on the phone from Massachusetts?

Yes.

Please correct me if I'm wrong, but it was my understanding that in Massachusetts, the Massachusetts attorney general interpreted the Medicaid regs in Massachusetts to require individual consent to share help from the Medicaid agency to a provider for treatment.

That was correct but we have a bunch of state laws and regulations that are very specific to this sharing of medical data in specific circumstances so it's not just from the attorney general.

Right ,but somebody had asked the attorney general in particular in the context of the health information exchange how that would work and . . .

That was MedsInfo, yes. MedsInfo, yes.

So there you have an example of a state where they said that the answer to Greg's question was, yes, you did need consent to share that information. Now, it didn't have to or wasn't a form, a specific consent form, I believe they allowed oral consent but it did have to be obtained.

It would be an area in which clarification would go a long way to help move this process forward.

So what this says is that within Massachusetts from one provider within an organization—one organization to share information to another provider for the same patient—they would need consent from the patient?

No, I think the context in Massachusetts was for the Medicaid agency to share the health information with the treating provider, they needed consent.

That's correct. It was just the state Medicaid agency, it was not all of the health plans.

And it was not from provider to provider.

That's correct, it was just the sharing from Medicaid to MedsInfo.

Now, I'm looking at another state here, from provisions that I had that dealt with participation of that state's Medicaid program for a provider. They have in here that they may not use or disclose any information concerning the consumer for any purpose without the consent of that consumer. So their regulations have passed that requirement on to their providers in general. And I don't think it requires consent for every disclosure but at least once.

I was wondering if we should move to William Golden's question, which is probably just as confusing, potentially as confusing is: How do these regulations pertain to PHRs as opposed to dynamic health information exchange systems? Which is probably another Joy question.

Is it a Medicaid PHR?

There is a proposal on the table because a Blue Cross program has a PHR to offer that mechanism to allow Medicaid to do the same and have a statewide PHR.

And so it would be that the Medicaid agency would be populating the PHR with Medicaid data for the purpose of the individual?

Well, and for that individual health care provider.

Right, but then the individual . . . the way most of these PHRs operate, then the individual has to give the provider the permission to look at that record, right?

Not necessarily. The Blues use a tethered model.

Yes.

Not . . . do not cede the control to the patient.

Oh.

Ah, or the other option would be that when the patients see their doctor, they would have access to the system and also if somebody went to an ER, they would be able to get access to it as well, so there are all sorts of issues about access to the data.

Well, I think that that's pretty complicated because it sounds like Medicaid would be releasing the information not just directly to the patient, which is a much simpler scenario, but in that system where it could be readily accessed—beyond providers—it is also to other payers?

Ah, what do you mean by that?

Well, some PHRs aren't limit to just providing access to the patient and their providers; other entities can get access to that PHR information.

The governance of the data's another matter and that is clearly an issue for discussion but obviously that would require a whole different set of issues.

Well, especially when you're concerning . . . it's one thing to release Medicaid data to the person whose data . . . who is the subject of the data. It's when they start releasing it to everybody else that it becomes very complicated because you have to look at who is receiving it and what the purpose is to determine whether it would be allowable under the confidentiality rights.

The statewide discussions have been trying to create an information system to allow clinical decision making at the time of care. And we were having discussions about a dynamic HIE but the local Blue Cross has an effective PHR for its patients and its provider system at the present time and is offering it free for consideration. On top of that, we also, the home state of Walmart has (inaudible) and they are developing a PHR as well.

Which is the thing you were talking about a minute ago? Which is the state you were talking about a minute ago?

This is Arkansas.

Arkansas.

You know, this is actually one of those topics that have come up as one of the next more in-depth topics, if you will, for technical assistance. I think it is a much larger issue and much more complex issue.

Yeah, because it depends a lot on who's going to be able to access the information, whether the patient has any control over who can access the information.

Who is hosting the information, I mean, there's several factors that –

What they're using it for.

Using it for, exactly.

Yeah. Because you do run into that, you know, administration of the plan requirement.

That's interesting. For Oregon, it's not just that we're doing a health information exchange, we will express that as a PHR under patient control for further dissemination but the question is, within the Medicaid arena, I think we have some rules of which HIPAA's base but then within a larger scope, if we go outside the Medicaid arena, then, as I understand it, we specifically require patient controls to move it farther.

Now is that Oregon's interpretation?

Well, I've got from my legal folks in the HISPC local here that say if within the Medicaid arena, within providers and patients, we can share information.

Right. But is that including the Medicaid agency or is that just provider to patient and provider to provider?

Well, the DMAP or the Medicaid agency is the one that's sponsoring this and has the Medicaid transformation grant, so we expect to get MMIS at least encounter information as a framework for medical history on this. So, I'm going to have to go back to the drawing board and do a little bit of looking to see whether that is an authorized source of information versus the current Medicaid providers which have electronic information available to aggregate and present back out.

I was just curious as to how that was being interpreted there because as I said, it looks like it's being interpreted differently in different states. I don't know that there's just one right answer.

Yeah, and I think I'm okay . . . because there's a whole issue here and ours is a health record bank: how do you populate the information because if you do opt in, there's going to be a successful as the PHRs are out in the real world which it's not.

Yeah.

So if we do an opt in for basic medical information, excluding specially protected information, at least to populate the initial data or the initial health record bank, where can we go from there? What level of consent is required? And these are the issues.

Are you getting authorization to create the record in the health record bank from the individual on the first instance or are you just doing this for everybody?

We have not done it yet. And this is what we'll take and drive policy within our steering committee, which also includes the legal folks and patients. But I'm hoping that we can populate it and then notify the patient that they can opt out but at least put up a flora of clinical information, non-specially protected, non-behavioral HIV, addictions, etc., including filtering diagnoses and diagnosis and drugs which would be related dual purpose, even if they are dual purpose but related to specially and sensitive information.

Now, it's my understanding that Oregon has that PHR health record bank model that puts the patient in charge of how that information is dispersed, isn't that right?

That's correct, and whether it's opt in or opt out is part of the reality of what we all have to face. How do we populate this thing to start with and then once we do populate it, who can access it?

Those are kind of distinct issues.

They are. I look at them at two separate axes of perhaps an X, Y graph: the amount of data to put in is, and then how much you can actually access the information that's in there and how we approach both of those. So we're about ready to have fun.

Who's controlling this databank?

Who is controlling it?

Yeah.

It's under the Medicaid agency, DMAP, Division of Medical Assistance Programs of the state.

And it's for the entire state population?

It is not.

Oh, just Medicaid.

Yeah, it is looking to be able to move forward into that and be a template from that but we are very specifically scoped to the Medicaid population, Medicaid providers, and Medicaid plans.

Gotcha.

Which does, I think, make it a doable first step.

If the individual is put in control of how the information is shared with others, that probably eases some other concerns, too.

Yeah, I think, if we move out into the wider world, that's going to be an absolute that there are no equivocation as to where we opt in and opt out. But our key is, how do we bootstrap this and put information in so that it's sufficient; the first three telephones are useless for the general

populations so we have to get a sufficient amount of information in there to be available and accessible to attract the attention of providers.

It's not clear to me why that's an issue if it's only within the Medicaid agency and for Medicaid patients because there are no strictures on what Medicaid can do internally for their own operational purposes.

Well, when you're speaking Medicaid, do you mean the state Medicaid agency?

Yes.

Does that include the health plans and the providers within the Medicaid community?

I would think so.

Okay, well, by being within that scope, we at least have some leeway to essentially run within, I would say, HIPAA as a floor but now – then we get into the trust issue in terms of can we actually administer this access and give the patient a control as to what degree? We're doing some groundbreaking work on this and it will be interesting as we go.

This is Barbara Massoudi. I think we're going to need to wrap up at this point. I want to make sure that we're able to just give a couple of closing comments before we're kicked off the system. Thank you, everyone, for attending. I again apologize for the problems with the technology. We will have that resolved. We will be sending out the slides as well the links for the tape recording of this session to all of those participants and answers to the questions, especially those that we did not have a chance to get to, so everybody should be receiving that. We will be sure to give those unanswered questions careful thought and careful responses and we will share those with everyone.

The next session that we have planned will be sometime early in April. We're still finalizing the date for that and it will be on the topic of data and other standards that apply to Medicaid and SCHIP agencies in the health information exchange arena. And we will have two engaging speakers joining us for that presentation. I encourage everyone to go ahead and sign up for the list if you haven't already done so. You will receive a notification of that session as well as all of the future sessions that we'll have planned for you over the course of the year or so.

Thank you very much. I appreciate your attendance and have a nice rest of the day.