Model Contract Language for Health Information Exchange

March 15, 2007

I'm Brian Dixon, with the AHRQ National Resource Center for Health IT. I want to welcome you to this afternoon's conference. At this time, I want to turn things over to our moderator, Susan Christiansen from the Agency for Health Care Research and Quality. Susan will introduce our panel and get things started today.

Greetings. Welcome to the AHRQ National Resource Center web teleconference, the Connecting for Health Model Contract for Health Information Exchange. I'm Susan Christiansen. I am a senior advisor at AHRQ, and I will be your moderator.

Before we start, I would like to say that if you would like to access the model contract and the related topic list, you can go to WWW.CONNECTINGFORHEALTH.ORG and click on the Common Framework link. Scroll down a bit, and you'll see a box marked "M-2." Click on that, and it will take you to the page where you can download the document. I would recommend saving it for reading later.

Now I would like to say how excited we are that Gerry Hinkley and Allen Briskin, of Davis Wright Tremaine, the authors of this contract, will be talking to you today. They will cover the basic principles embodied in the model contract, and then they will get into tactical issues with using it, based on their experience working with clients. We have allowed time at the end for your questions, so please jot them down as you're listening and you'll be able to ask them as you're listening, or e-mail them, and they will be placed in a queue.

Jerry and Allen contribute generously of their time to a variety of organizations, working to support broader secure electronic health data exchange. In addition to the work they've done with Connecting for Health, they work with the E-Health initiative in tracking state legislation, and Jerry is a contributor to the National Alliance for Health Information Technologies CPOE Implementation Guide. That's enough from me. So let's get to the subject you dialed into discuss. Jerry and Allen?

This is Jerry Hinkley speaking. Since we were asked to do this presentation, Allen and I have been working with a variety of clients to enable Health Information Exchange and to address the legal issues that arise in that context. One of the issues that comes up repeatedly and it's something that HIE is confronting, is how to document the contractual relationship among the participants.

As Susan mentioned, Allen and I have the opportunity and really the good fortune to be included in the Connecting for Health Common Framework project. And while we generally are credited with being the authors of a model contract for HIE participation, it's the work of a large group of individuals who are part of the policy subcommittee of Connecting for Health, and we would be remiss if we did not thank all of them for the time they put into making this the most useful and robust product that we think it is.

A challenge that we're facing now, and really how we've redistricted the talk a little bit from just describing the contracts to turn it into more of a process presentation is that the Common Framework model agreement needs to be viewed as a starting point but not an ending point. And understanding that our goal was to do what we call the "60/40 solution." And that really was aimed at a team of policy issues, providing alternates for solutions and policy decisions that needed to be made that would be embodied in the contract and leaving open the local HIE issues that would be unique to any particular HIE.

There's an underlying assumption for the model, and that is that there would be in existence a national framework of policies that need to be in place for national exchange to occur, and course that isn't in place yet. So what that means is that the model is useful because it identifies those issues, but it doesn't provide particularly extensive guidance on how regional HIEs could address them. And so what we're going to do today is to outline some of those policy decisions that need to be addressed at the local level in the absence of national standards, and talk a little bit about the process from getting to policy-making to actually implementing contractual language.

I think a footnote to this is that the job of the business people in developing an HIE and their legal advisors is that they aren't separate jobs. It's the same job. Policy decisions need to be made with due regard for legal considerations, and then the document needs to be created or documents that implement those policy decisions so that there is an enforceable and readily understood mechanism for the exchange. Allen?

As we're adapting the model contract to present-day use, use without the national network in place, I thought it would be helpful to go through some of the definitions and make some suggestions for how those terms could be changed a bit to avoid confusing people and make the discussion most helpful.

In the model contract and in the following slides we talk about participants, which are the sources and recipients of health information on an institutional organizational basis. So it's the hospitals, the physician practice, the laboratory corporation, et cetera. Next is the authorized user, and that's the individual who uses the network on behalf of a participant. Next, we have temporarily dropped the term sub-network organization or SNO, which appears in the model contract, and what we're using instead, HIE network. This is either the organization or framework network that brings together the participants to facilitate Health Information Exchange. It's important to note that it doesn't necessarily need to be a separate entity, and so as people are working in a setting where there isn't a separate real or HIE entity, I would still say the concept here of the network is important. And when we look at the model contract and look at some functions that are assigned to the SNO to say those are still important roles that need to be fulfilled by someone.

I think the point to stress here is that we adopted the term sub-network organization with the thought that there was a going to be a network, which would be at a national level, and the use of that term has proved in some situations to be a bit confusing, and so we've adopted a more generic term to describe HIE in whatever context it arises.

The final bit of terminology to discuss at this point is participation agreement. In the model contract it was referred to as a registration agreement, but as we work with more people we're finding that participation agreement is a more helpful term. And this is the document that links the various participants in the HIE network to each other. It provides for the creation and use of a shared technology for information exchange and secures all the participants' agreement to follow common policy and procedures that promote this process, and describes consequences for failure to follow those policies and procedures. We're finding that's particularly important as a way of building trust among the participants, needing to have some assurance that if the other participant doesn't act with respect to the network or the information the way that participant should, that there will be consequences that I can take some comfort from.

Early decision-making can be helpful if it first focuses on the documentation involved and looking at the structure of those materials. The model talks about a participation and registration agreement that has a significant amount of substance spun off into separate manuals, operating manuals that address specific privacy and security rules and other operational matters.

We think it can be helpful to make some early decisions about what terms and conditions are going to be going into which document as a way of organizing thoughts, organizing decision-making processes, and pushing off certain decisions for later as a way of organizing an agenda through which people can work in an orderly way and make the decisions that they need to work.

The other point that I think needs to be made is that when we're talking about a participation agreement as the agreement that pulls everybody together, we don't want to exclude the possibility but there will be separate agreements that parties have to enter into in order to participate fully, and I think the simplest and the most direct example would be an agreement to acquire technology rights in order to participate in the network. The model contract was described as one of the alternatives that describes a mechanism by which parties would be obligated to enter into those separate agreements.

Just as a practical note, in sitting down with developing HIEs, one of the things we found useful is to take the detailed table of contents from the model and really go through topic by topic from the table of contents and say -- and make an assignment of that topic, that, yes, this is something that should be contained in your participation agreement, or because of our own circumstances this needs to be in the manual or needs to be separately contracted for, and then what we do is we take that table of contents and actually make assignment responsibility for follow up and development of initial work product in those areas to bring it back, and so that you will ultimately hopefully cover all of the issues that are called out in the model, but you'd need to do it in a way that is going to be useful and practical in your own context.

Jerry describes the purpose of the model is providing a 60/40 solution. When we sit down to work with groups organizing their participation agreements, we find that the model, which we can put in front, provides the 60 percent. The additional 40 consists of making several lists of significant policy decisions, which we've described on this slide. They're the policies that address privacy and security, user identity -- excuse me, user authentication, and responsibility, risk management, insurance, indemnification, business associate responsibility, and governance issues, including a mechanism for amending the participation agreement and the related operating manuals.

And there are others that will come up in the context of doing your assignments that are delegated out of the table of contents. But what we wanted to do today in the interest of time and to try to be as concise as we can is we're going to focus on these five issues in more detail during this presentation.

One of the challenges that we're facing now is that we had contemplated while we were developing the model, but now that we're in the field it is becoming as significant really as anything else, is developing the process for decision-making so that you create a timeline for decision making, you identify deliverables, and you assign responsibility.

What we found is that it is better to divide responsibility along subject matter. And we encourage the joining of the business individuals and their counsels on each of these topics, and must stress we think that these -- generally speaking, these are business decisions that have legal consequences, and so it really isn't appropriate to send your lawyers in to work up the agreement and then bring it back to the business people, because there are a lot of practical considerations.

There are goals that the business leaders in these organizations have for these programs, and they need to be at the table to express those. And really a principle reason for that is to save time, because we've learn that we run through it once with one group, typically a legal group, and then we start again. And those of us who are on tight timeframes, and I'm assuming everyone on this call is in that context, you need to understand that there are pressing items and how to try to address those up front.

We believe it's key to make sure that all the right people are in the room at the right time so that you try to reach consensus at as early a time as possible, and then also that individual participants don't feel that by their absence either by not being included or excluding themselves at the beginning that they gain some kind of leverage over the process by coming in later. And so inclusiveness and decision-making in the group of decision-makers is really key.

We also find that it's not very helpful for a group to meet with blank pieces of paper. And one of the things that we'll point to later are the policy guidance that are in -- guides that are contained in the Connecting for Health documentation that provide some great starting points for decision making. And it's much better to start a conversation around a straw man, which is not to [inaudible] the initial draft, but something for people to talk about rather than concepts to throw around in a more abstract way.

And, as I said, we believe that it's important to convene consensus bodies by subject matter. We also believe that a group subsidiary to HIEs governing body ought to take responsibility for pulling together the work product from the various subgroups to reconcile that [inaudible] facts, when that's necessary in order to achieve reconciliation, and then to create a work product that is presumably ready for governing body adoption at the time that it's presented because of all of the stakeholders have had an opportunity

to, for their views to be heard for consensus to be developed, and for concise written descriptions of the decision-making to be presented.

As I mentioned, there are policy documents within the Common Framework that I suggest are mandatory reading. They are really a remarkable compilation of a variety of credible sources on the topics that are addressed. They're numbered P-1 through P-8, for policy, one through eight. P-1 sets up the architecture that is envisioned by Connecting for Health. I want to underscore that that architecture is a suggested architecture and that the issues that are raised, if your community or your HIE is looking at some more consolidated federated model or a record locator model, that doesn't mean that P-2 through 8 are not useful. They're extremely useful. And the model contract, we believe, is also adaptable because the technology solution is clearly optional in the model contract, and you're not locked into that.

This is just a screen shot, and obviously you can't read it, but I want to just show you how we laid this out. In the left-hand column we have indicated -- this is in the context of the specific policy that is to be addressed, and we have included policy language that could be adopted by a policy-making group, and then in the middle column we translate that into what would be a contractual vision, now coming to be called the legal language of, I guess, differentiated from the illegal language.

And then finally in the right-hand column we've included comments that were made by the policy subcommittee about how these provisions should be dealt with. I think a point here is -- and we've heard this from a variety of places, is that they print out the model, and that it's an 80-page document and it's too scary. What I would tell you is that if you use the model document as a tool, you can end up with a 12-page document, which we have in situations, so that it doesn't mean that by adopting the model as an approach that you somehow are going to end up with this unwieldy, oversized contract. Keep in mind that the model is in column form, and the terms if you X them out, get down to a rather manageable amount of verbiage.

It also incorporates many alternative provisions. You never have all of them. You may have only one of five, which also shortens the final product.

On the slide we're just listing the resources that are cited throughout the Common Framework, and although I think this is good suggestion reading, it's not as compulsory as reading the policy provisions, but for those of us who can't get enough of privacy, these are places to go if you're not familiar with them that will enrich your understanding of the issues and how they've been handled in other context. And we look, of course, at the bottom that as baseline for these policy-making decisions are HIPAA and also state laws that deal with exchanges of information and privacy.

So this is -- I tip my hat to Vicky Estrin at the Mid-South Alliance in Memphis for the content of this slide. And I asked her recently, "So really, Vicky, how did you get started?" They had really, because of the involvement of Mark Frisse on the policy subcommittee, co-chair of that body, Mark very graciously said, "All right. We'll try it in Memphis and see how it goes." And I think in the end they say it went well. But they did add some local color to the process, which I think is pretty valuable. And Vicky describes that as a cheat sheet, some basic initial policy-making decisions, not etched in stone, but at least a starting point for all of the work groups, there are kind of the core 30,000 decisions that an HIE needs to make in order to get started and also to guide the work of various consensus groups that are dealing with specific issues. And I'd look for them on this slide. One is, "What information is going to be included, initially, potentially in a pilot, and then long-term." Who will have access to this information? Under what circumstances will access be granted, and for what purposes? And lastly, how is accountability going to be built into the system? Who is going to do auditing and who is going to enable auditing?

Then you need to come back and say, "Oh, here's what we want to do. Does our selected technology solution enable that?" And what they learned in the Memphis situation is that they had to adjust some of their decisions because the technology approached things in a slightly different way, and they were able to get comfortable with how that worked. And then finally a reference that you create a cheat sheet for

this. This is kind of your Ten Commandments or Six Commandments, however many there are, that approved at the very top level as an initial matter to guide the work that follows.

So we want to drill down on a few of these particular policy decisions and those of you who've heard the lecture in the past know that I believe that 2007 is the year of privacy and security, and unless we get it this year, we're going to have some real roadblocks to getting networks up and running. And so we put this one first.

The concerns about privacy and security are justified and they are significant. The concerns about misusing data, that there could be commercial, governmental, criminal use of information, criminal prosecutory use of information that is not intended. There's concern about when security breaches could take place and how they're going to be handled. There are significant conversations about the quality of data and how useful it is and how reliable it will be, and then the concern about, well, what happens when there are breaches where data is used inappropriately. And these go back to that very famous [inaudible] article about what privacy is, and privacy is supposed to be the right to be let alone and -- according the to that author. And how do you build that into a system that accomplishes what HIE is intended to accomplish without violating rights that I think most of us would say are closely held and to be guarded?

The goal through the privacy decision-making is to create an architecture, a schema, a system that leads together all of the issues around privacy and security and identify solutions and mechanisms for addressing those. And what I just described is one bullet point on one slide that is an enormous amount of work, and I'm hopeful that as the communities start developing and sharing this kind of information; that it's going to get easier down the road. But it's still pretty hard, because it still requires -- in the every situation once a policy decision is made, that may be the one liner about, well, individuals will choose whether their information is accessible to the network. That's a pretty simple statement. But, how do you implement that, and what is the appropriate way to do that?

There are decisions that need to be made, and one of the things we're discovering is that there are profound regional and local differences of opinion about these issues. There is at least at this juncture, I'm not perceiving any national consensus on this topic. At some point hopefully one will evolve, but these are hard conversations. People hold their views dearly, sometimes misguidedly, but nevertheless, we need to respect those points of view and figure out how to reconcile them and actually turn it into a system that generates the level of trust that will make you or me or somebody you're talking to about HIE say, "Oh, yeah, I'll be in that because I feel like this is the right thing for me to do."

And lastly -- let me -- underscoring again the importance of integrating privacy and security within the privacy and security architecture of leaving in applicable laws and regulations. And one of the things that is yet another pressing item but an important one is the work product from the RTI contract from ONC, and how significant that work is. I heard a brief report at the (INAUDIBLE) meeting -- those of you who weren't there in on that call -- about what they're learning. And in what is coming out in general is validating what we're seeing in the field. There is in many cases a misunderstanding of what HIPAA requires or doesn't require, similarly, what state laws requires and doesn't require, and then finally, an appreciation that privacy and security in the context of Health Information Exchange will in most cases start with state and federal law as a baseline, but that's not the answer, and I think generally speaking we're finding that HIE needs to speak to a higher level of concern than with state and federal laws were intended to address when they were enacted.

This is a list drawn from the Common Framework which are the basic principles around private and secure architecture. And I'm hopeful by now that most of you have familiarized yourself with these, and I won't spend a lot of time on it, but we'll talk a little bit about how some of these can be implemented through open policies and transparency describing clearly what the exchange is about; what information is going to be collected; how is it going to be used; the rights of the individual to participate and to control; the importance of the integrity -- maintaining and securing the integrity and quality of the data; appropriate security, safeguards and controls; accountability and oversight; and finally remedies of what is often

called the consequences of a participant who has agreed to follow the rules, what those consequences are when they don't follow the rules.

So in the suggested privacy policy that is within the Common Framework, there are ten discussions with proposed policies in each case. And don't misunderstand us here, we're not espousing these but we do believe consistent with your thought that the discussion has to start somewhere, that these are a useful place to start the discussion.

The first two we won't drill down on too much. They certainly are worthy of your time though. One is the compliance with law and policy, and the second is how a notification of privacy practices should be carried out. The third one, number 300, really talks about patient participation and control over their information. And the principals included there are that the individuals should have a choice not to have information included. And it should be a clear understanding of what the effect of what that choice might be. There should be a mechanism for changing your mind. There should be a clear mechanism for documenting the decision so that it can be referred back to later, and the actuality of the the content of that decision-making needs to be documented. And there needs to be a reasonable way for patient choice to be expressed. And finally, an assurance to individuals who are participating that their decision to be in or not be in a HIE will not affect their ability to receive care or to receive insurance coverage or other unintended consequences.

The fourth policy, 400, focuses on how information could be used. Again, we focus on the baseline of HIPAA and state laws, but keeping in mind that they're being viewed often as merely that, a baseline, a starting point. Consistent with the cheat sheet that I described earlier, what can information be used for? How are we going to ensure that participants comply with the policies. And a common theme through the mechanism devised by the Common Framework is that ultimately the participant who is the source of the content would have the ability to control whether that content is transmitted in any particular situation, whether it's on a case-by-case basis or other basis where that could be instilled in the system; that there needs to be an accounting for disclosure so there's an understanding of when and to whom information was shared. There needs to be a way to audit through the creation of logs or other mechanisms that throughout the system there needs to be a uniform way to authenticate who is a source of information and who is an authorized user on the system, and Allen's going to spend a little bit more time on that in a couple minutes.

And then lastly, an important principle that individuals should have access to their own information so that they can be assured that the information is correct to them.

The next two policies, the five and six, talk about information that may suggest no special protections like HIV/AIDS status, mental health information, other kinds of information that is either protected by statute or may be excluded as a policy matter for the exchange. Six is a hot topic, and that is minimum necessary, and the implications of that concept that is clearly a part of HIPAA where minimum necessary exchange is mandated for all permitted exchanges of information other than treatment where minimum necessary doesn't apply. But the way HIPAA treats minimum necessary, again, it's a starting point. It isn't where your HIE may end up.

Policy seven focuses on a participant's own workforce and their agents and their contractors and how participants need to be responsible for those who are authorized users of the system. And this policy decision-making process would encompass who is going to have access to the system. How are they going to be educated and trained so that they understand what their rights are with respect to access but also what their obligations are; that there is a mechanism for disciplining users and the participant when an authorized user fails to follow the processes, and that there'd be a mechanism to report non-compliance through the network so that affected participants and patients know that there has been a violation of a policy.

The last three, eight has to do with the minimum of data, nine has to do with adhering to and trying to comply with specific patient requests. And the last one, ten, addresses potential measures for mitigating

breach of policy and/or improper use of data, and time doesn't permit us to go into those in as much detail as we would like, but I, again, refer you to the documents that we've referenced to get more information on that. Now I want to turn it to Allen to talk about user authentication.

Thanks. When we start talking about using authentication and responsibility, we're asking ourselves the question, how do we establish adequate trust so that a participant, a data provider, feels comfortable releasing? I do recommend -- I know I may be repetitive on this point, but I do recommend reading P-5 in the Common Framework material that provides what I think is a very good discussion of the essential concepts involved in the direction that we found is particularly important to answer these questions as a part of the trust-building process.

The key concepts are, again, who is this party who is asking for information? And in order to develop appropriate mechanisms for sharing information, we found that an identifier for each individual is critical, and that must be unique. So for example, when John Smith quits and Jane Smith takes it, we don't have a second Jane Smith; that a critical part of having valid identifiers is that they are unique and they're not reused.

The next question to be answered is, "How is a personal question information authenticated; and secondly, where does that authentication take place?" It can happen at the HIE network level. That's a responsibility that the network can assume from the participants, or it can be authorized -- excuse me, implemented at the participant level.

In the model contract, the approach is taken that authentication is going to be done at the participant level; that each participant is given responsibility for certifying and credentialing its authorized users and assuring that they are who they say they are and that they are going to be aware of the rules for Health Information Exchange, and so there's consequences if they don't follow those rules.

I think what -- let me just let me interject. We have received actually some relatively significant pushback on that, where the network, and particularly the technology vendor, want control over authentication because of their perceived risk of delegating that liability and responsibility to a participant, so that seems to be quite a debatable concept at this point.

The theory behind this, having authentication at the participation level, was there would be fewer parties that you as a participant as a data provider would have to trust. You wouldn't have to worry. How do I trust the few hundred people who have access to a terminal and get information but rather I'll trust the several institutions that have agreed to par participate in the network and trust them to administer the process appropriately. The first fact that Jerry mentioned actually here saying that to establish appropriate levels, they want even fewer parties' responsible, maybe even one party, and in that case, the vendor takes the place of the network we have described in the slides.

Right. And the issue that we debated in that context is the timeliness of that action. Because if someone needs to be disabled from the network the participant is going to know first, and how quickly can that decision to disable be implemented so that the integrity of the exchange with respect that particular individual is assured.

And then once you decide, once you determine, once you authenticate, once we determine that the personal question, the information is the person that he or she says he is, the question then is, "What information do they have access to." And here I have to identify and apologize for a typo in the materials that -- among the types of authorization and the two most frequent ones -- the two we see most frequently are ones that are role based. In other words, a request by a physician allows certain information to come there. A request from a claims processor allows a limited and different set of information to pass through. In other cases the authorization can be request-based, where if the request is from a short menu types of information, it can be generated more or less automatically, based upon their authentication. Other requests, if they not on the menu, are authorized, if they are, based on a specific inquiry and intervention by a decision-maker.

If authorization failed, a situation where we can't determine whether or not the individual is authorized to receive the information -- Or if the information is the right information.

Yes. We then have to ask the question whether or not the individual's going to be allowed to do what's called "break the glass," which is short circuit the process and get information without going through -- without being authorized or without having the information as the appropriate one, the appropriate set of information. This is a difficult issue for a great many organizations.

I think one of the key questions to ask is, if we look at where a provider is before we have Health Information Exchange to ask if that provider's materially harmed by not allowing access to the information, or is it so critical that we need to have this mechanism. We found a lot of pushback against the notion of breaking the glass.

Right. But you're already starting with no information about an individual. Running the risk of having information about the wrong individual doesn't necessarily serve that argument though. One of your commentators noted that we had a typo on Slide 18, and under the word role-based is not referenced to what I had for breakfast but actually it's r-o-l-e, so if you'd make that correction if you have a printout. We apologize for that error.

Moving from one hot topic to another, and this is one we've spend a lot of time on and actually a lot of conversation with people who feel very strongly about these issues. The first has to do with insurance and whether or not the risks inherent in the operation of an HIE can be mitigated through appropriate layering of insurance. And when we had this conversation about a year ago, we really had difficulty identifying insurers that felt capable of assessing the underwriting risks and making coverage offerings. That over the last 12 months has changes, and a number of larger insurers are focusing, both on the cyber liability issue that attend HIE, that is the technology failures, as well as professional errors and omissions that might be exacerbated by the connectivity that wouldn't -- having an error that isn't communicated to anybody else has limited implications, and one that is in the medical record that communicated as part of a continuity of care or other record to a recipient caregiver would have broader implementations, and although I'm not entirely comfortable with the pricing that's coming out on some of these things. I think that's part of any early underwriting experience, but I believe the good news here is that the underwriters are starting to get this and are coming forward with some practical solutions to fill the gaps and protect, not only the HIE network itself but also those who provide content and those who utilize that content, potentially to a patient's detriment.

Kind of hand-in-hand with HIE coverage then is the layering and collaboration with participant coverage. And that is deserving of some attention, because even if you have compatible coverages, you need to make certain that if there is a claim that you aren't spending time on the coverage dispute as opposed to spending time addressing the core liabilities and taking care of remediating in that regard. Allen, did you want to comment on the indemnification issue?

Just briefly. It's one that often gets people into knots as they're working their way through the documentation; one to propose a couple of ideas for simplifying the approach here. First, here's one of those where I think it is particularly helpful to have one's lawyers in the room. But also under guidance that the primary objective of these participation agreements is to create a network to which people can trust each other enough to provide Health Information Exchange and not necessarily to win and to hoist off onto someone else responsibility for something they -- for their own responsibility that they'd rather avoid.

And so I think to first focus people before we start negotiating really heavily on the indemnification language, it's worth taking a step back and saying, "What does the applicable law say already?" That this does vary from state to state. But a common and basic rule, one that you find iterated in terms among many of the states is that you're essentially, in absence of a agreement otherwise, responsible to correct -

- responsible for the harm that you create, responsible for your own actions, not responsible for the actions of others. And I think that's a good working place from which to start here.

Certainly one can start making decisions about shifting responsibility for potential loss that can arise. A couple of examples could be malpractice, breaches of the agreement, or breach of the privacy and security, but would encourage people to think in the greater terms about shifting that responsibility if it makes the network operate better in that way. And not simply with the objective of winning, and pushing as much of my responsibility off on someone else.

I think in some of the conversations we have on this topic, there is a concern, I think justifiably, well, it wasn't my fault. It wasn't my negligence. But I'm dimed into a lawsuit and I have defense costs, and how am I going to deal with that, which could be a substantial amount of money. And if you're asking that question and you have your HIE hat on, you're probably struggling with how do we make this economically sustainable anyway without the risk that the further lawsuit is going to bring us down, not because we're liable but because of the cost of defending ourselves, and that's really how -- that's how an underwritten product is going to provide comfort in that regard.

Similarly, some of this debate, and this isn't finger pointing, but its shared our pain at least, comes from a misunderstanding of the rules of negligence and that people's behavior in the context of information exchange has to relate to a standards of practice. If you don't meet that standard of practice then you could be found to be negligent. But a lot of the conversations has to do with a concern about absolute or strict liability if someone is hurt because of activity running through the network, that everyone along the chain is going to be responsible and then we -- someone inevitably says, and I don't want to be responsible for so-and-so's error. And that's something that I think we're not going to solve it in 2007 or for a while, and we're going to learn from circumstances that occur that we're not even imagining now as these things become operational.

And so, starting an informed dialogue on what these issues are and what the potential risks are and how a claim might be handled in the context of HIE, it needs to at least start in that conversation and needs to continue and develop. And I wish we had the pill for you. We could just say here's the answer. But I would love to know it but we're not there yet I don't think. Allen, do you want to talk a little bit about Bas?

Yes. We found that often the process of developing a participation agreement does require a very brief HIPAA primer, which is to go back and remind ourselves that a separate entity doesn't need a business associate agreement with every party to whom it discloses protected health information. And for example, covered entities don't need a business associate agreement to share information for treatment, payment, or health-care operations purposes. I want to underline that fact that often people think that business associates -- that we need to create this web of business associate agreements in order to run information exchange, and the answer is that we don't. Business associate agreements are required for entities that are going to receive or use PHI on the covered entities' behalf, and we think that's helpful, first, because it reduces the number of agreements that people see that they need. And secondly, offer suggestions for how the HIE network, either the arrangement or separate entity, that entity, can streamline the process, be it working as an attorney in fact for the covered entities or otherwise to create those arrangements and enforce those arrangements and provide that additional service to the covered entity.

I think one other point. The question keeps popping up, is the HIE a covered entity? And the answer to that is, it is if it is. Generally speaking, I think it's unlikely that most HIEs are going to be covered entities. So then the question is, are they a business associate? And you need to ask, well are they going to get access to PHI? In a vendor solution HIE the vendor may be the business associate but the HIE, the network itself, may not be a business associate, and so chart out those relationships, I think is key, and it seems to be a waste a little bit too much time scratching our heads about business associate relationships and responsibility. Allen, did you want to touch at all on streamlining -- ways to streamline in the BA context?

Well, certainly one way of streamlining is to have the HIE network act as the party it goes out and obtains the business associate agreement. The covered entities can empower the network to function as their attorney in fact to create those agreements. It simplifies the process because the business associate signs one form of agreement that applies to everybody, rather than having to having the covered entities manage the process and negotiate their own specific forms.

Okay. I think that it's very stressing here that a goal of successful HIE, at least in our view, is to streamline the contracting processes wherever possible because it takes time, and if everyone insists on their own business associate agreement because it's near and dear to them, that is going to get in the way of the exchange. And so what we really encourage is some open-mindedness about existing procedures within institutions about how they will treat the business associates that they will end up being involved with in the context of HIE and looking at their willingness to participate in mechanisms which delegates to the HIE the ability to enable the execution of these contracts without the covered entity having to sign each one but merely receiving information about who their business associate is. And then similarly, the HIE taking on some of the early enforcement obligation so that covered entities are assured that they will be able to enforce the provisions of the business associate agreement in the context of an HIE.

And this topic could be its own separate seminar, because the issues are quite complicated, and maybe we'll figure out a way to get one of those put on in the future. But I think once HIEs develop sophisticated streamline business associate contracting mechanisms and they start to become the norm, that that will remove a risk I think for success to HIE networks that they get bogged down in these kinds of details that consume resources that the network doesn't have to give to a topic such as this.

Allen, we're getting close to time, so you might want to address just how briefly technology licensing can be accomplished through this mechanism.

Well, we first want to identify the network's role with respect to the technology itself. The network can be a vendor of technology. You see that in some situations. In other cases it can facilitate the supplying of the technology by arrangements with vendors, or in a third setting it can lead the participants on there own to get whatever technology they need in order to facilitate the exchange.

The legal relationships that need to be addressed in the contracts are going to be driven by the roles that people play and the particular technology solutions that are selected. This can be something where it may be helpful when wrestling with all of the problems that we've been talking about so far is to put this off into another document, if nothing else, just to take it off the table and recognize that these are issues that may be dealt with in a different group, a different sub-group in the overall group that's pulling together participation agreements.

The counter balance is that if you add an agreement you add time and process, and so make those decisions carefully, because every time you have a new separate statement of agreement, it adds additional complexity to your process, and try to think creatively about how you can accomplish the goal of segregating provisions that relate to technology usage in a manual or in something that is adopted by implications through the execution of the participation agreement and doesn't require execution of a separate instrument.

Structural considerations, now we actually are coming to repeating ourselves. Leaders in the process should give thought to the principles that may help them achieve consensus. When we talk about managing the resources and negotiating participation agreements, we're talking in part about the structure of agreements but also for parties to recognize the multilateral nature of the agreement; that the agreement between the network and one participant affects the legal rights and responsibilities of the other participants in the network and that our goal here should be developing a process that works and facilitates participation among all the parties and not necessarily to have one person or one party win and get a particularly advantageous arrangement. In particular, on this slide I've tried this many times, and it's difficult to come with the terminology, but part of it is to look at the advantages and disadvantages of the

traditional relationships and the way they work with each other regularly and ask, “Is this the way we want to do this now?” As I said, this is about -- this agreement needs to be a result of consensus and cooperation more than the gaining of advantage. Finally, on this slide I wanted to note that part of what we found facilitates negotiation of these documents greatly is to have a very powerful management committee or other assemblage of stakeholders that are broadly representative and represent the various constituencies’ perspectives as the initial drafts are being developed.

And as an operating committee this isn’t the CEOs. This is the folks who are going to be on the ground in the institutions and taking responsibility for implementing their own participation.

But they can play a big role early on in the process before operations begin to assure that the contracts -- the contracts have terms that are going to be workable for all the parties involved.

Which goes back to one of our original points, which is, this isn’t legal homework. This is a document that participants need to live with. It contains operational terms, and the people obligated to carry those out need to be involved in the decision-making all along.

And then next, acknowledging that no matter what we do, changes are going to have to be made, whether to the agreement or to the operating manual. We suggested a mechanism, and the model contract describes one variance of it by which we have this management committee, which is broadly represented (INAUDIBLE), in other words, a group of people trust and have confidence in that approves changes. Those changes then can be made unilaterally. Changes required by law would be made automatically. In other words, each participant would be agreeing to participate in the network in accordance with whatever the law says is required; that they wouldn’t have the opportunity to negotiate their terms when the law changes. Next, [inaudible] changes would be coming if the management committee could impose, take effect if needed. Again, without having to go out to other parties and negotiate everything and gather everybody’s signatures.

Then we come to the question of material changes, when you really do want to make a change that will materially affect the rights and responsibilities. How is that done? How is the management committee empowered to do that? We found that putting super-majority requirements on management committees helped gain a significant amount of trust, which is a two-thirds voting requirement, and then offering parties the opportunity to opt out by training their participation if they find that notwithstanding the fact it’s management -- that it’s going to representative of management committee in whom they would hope we both have trust approve the change but the participants still finds it needs to terminate and get out. As a practical matter, we think that needs to be moderated by having a long lead time for termination, in large measure to protect the stability of the network. And also having that long lead time for termination allows the management committee time to revisit the issue and say, “Well, we thought this change would make sense. It’s had a destructive affect on the network. Perhaps we want to take a different course.”

Okay. Why don’t we wrap up this up by talking briefly about pilots. It seems to be the first topic we get to with most of the exchanges.

Actually the pilot offers you the opportunity to deal with making a lot of these decisions with fewer elements on the table, fewer participants, a smaller range of information that’s going to be exchanged, a less than complete array of technology perhaps, and by constricting those variables, making some of the questions easier to answer. So one can make the initial policy decisions sooner, such as the access question we described, on the slide what, who, when, and what for, and coming up with more simplified documentation and able to put something small into practice and learn from that and build on that for developing the full-scale network.

Right. And what we’re learning is that pilots oftentimes will get disparate group of participants who agree to work on something that they can get their arms around to get comfortable with each other and also to put off, at least for a short time, the ultimate decision-making on some key issues like how often opt out might work or how other elements of the exchange might work that the various participants may not be

entirely comfortable with until there is some level of exchange taking place so they see how something is going to work in their own community.

Just to repeat what Susan said at the outset. Here is the link for Connecting for Health, also links for the AHRQ user form, and some other resources that you might find useful. And then I want to conclude with an admonition that we're delighted to bring this information to you for that purpose, but we encourage you when you get to legal questions to consult with your own advisor. And with that, thanks for your attention. I know we have some time for Q & A, and I'll turn it back to Susan.

The slides will be able on the AHRQ website that was just put up there, which is HEALTHIT.AHRQ.GOV.

We've had quite a few questions. A lot of questions around the privacy issues. But let me start out with that the pilot, you mentioned that pilots are useful for SEP. How would a Health Information Exchange minimize the ways in getting a pilot up and running that may affect implementing their more robust figure system that they're aiming for, or is that going to cause an additional delay?

We're actually dealing with that right now. I think we feel that the industry wants pilots, but the concern is that you spend a lot of time negotiating a pilot agreement and then you turn around and have to do the user agreements. And what we're suggesting is, based on the one situation we're advising right now on this topic is that, during the pilot, the user agreement be finalized, and that it spring into effect at the end of the pilot without requiring the pilot participants to re-execute that agreement and to allow the pilot participants to terminate their participation.

So it's a, I don't want to keep going as opposed to all of us need to regroup to decide if we're going to keep going. And that is essentially a mechanism to force decision-making during the pilot phase. What we learned is just human nature, people put off making tough decisions until they absolutely have to make them, and so we want to make certain that those decisions are made during the pilot phase and aren't delayed for some period might consume weeks or months between completion of a pilot and implementation of a more robust system.

Going back to your discussion about each community making some choices about how they're going to allow access and who's going to be able to obtain what information for what purpose, the question is, don't you think if everyone has different access rules this creates problems nationally? What if on the Interstate Highway System -- you said the roadways change from state to state.

From my perspective, that's an inherent problem. Since there is no national network now, what communities and organizations are finding is that they have a need or a desire to implement this now and do their own program and leave the later integration with the national network for later when that national network appears. And what I would think now is that parties ought to do the best job they can at setting something up. Try not to build barriers into connecting to a larger, say, national network. But not allow that possibility in itself an obstacle now.

That's a laudable goal. In the absence -- the question went on that, if the Interstate Highway System used a roadway changed from state to state, what would that mean? Well, in the absence of general dictates, and I think many of us have different thoughts about whether or not that's a good idea at this point or not, but not getting there. The communities are going to benefit from having their regional exchanges, and so focusing on the local benefits and not, having your head in the sand about where things are going.

Now I'm optimistic that this National Government Association, E- Health Alliance may be helpful in creating some uniform state legislation. I know that there's quite a bit of interest at the state level now in working cooperatively. There's an initiative that Mike Hekin (PH) has started for Florida to try to create or to get guidance from the Commission on Uniform State Laws.

So, I'm expecting that there are going to be leadership in this regard, but it's not going to be immediate, and so I think what Allen said is the right answer. Do the best you can and don't create a mechanism that locks you into a solution, at least as best you can, that limits your flexibility when rules start to become more common place.

And then I'll alert just to the fact that out there may explain why I spend as much time as I did talking about the flexible process for making changes later, knowing that other things are going to come down the road, some of which we don't anticipate now. Others, we don't know what they are, even if we anticipate them. An important part of setting up an HIE would be the ability for that organization to change, to address these developments as they occur without having to go back to square one with everybody and start negotiating.

Thank you. I think that's consistent with what we're finding in the national privacy and security contracts that you referenced earlier, is do what you can now with an eye towards what can be done, and that's getting into another question that someone asked, which is, "How does this Common Framework approach relate to the HCIS," and I think we've pretty much answered that question.

The other question we have is, Please explain how a Health Information Exchange would not be a covered entity or at least a business associate. If the goal of the Health Information Exchange is for exchanging electronic PHI for treatment, how does the Health Information Exchange escape becoming at least a business associate by providing information in support of treatment payment for operations?

Well that's a great question. An HIE is a covered entity if it is one. It would need to be either a payer or provider of services or a clearinghouse, and you can't make yourself a covered entity if you aren't one.

If a covered entity is asking a third party to carry out a function for the covered entity that will enable the third party to have access to PHI, then under HIPAA, the covered entity is obligated to have a business associate agreement with that individual or that third party. And so that really dictates kind of what the basic rules are for participants. And then the question is well, in your situation, based on your own technology solution will the HIE have access to PHI such that a participant would be legally obligated to have a business associate agreement with them?

I think that a common misunderstanding is that somehow it's -- well why don't you have a business associate agreement anyway? And really from a practical standpoint trying to minimize the proliferation of contracts, we're really trying to have our group focused on the times when you have someone who is your associate and therefore you need an agreement in place with that entity. And if someone isn't a business associate then questioning the need to have a business associate arrangement to protect PHI when that third party doesn't have access to PHI to begin with.

But maybe the shortest alternative answer is that -- or better answer -- no, just shorter. The HIE will avoid being a business associate first if it's not itself a covered entity; or secondly, if it doesn't receive or transmit the health information itself. It's not acting as a repository; it's not acting as a conduit it won't be a business associate agreement. Some technological solutions have information being exchanged without that information going through the possession or control of the HIE.

Right. It's going to be a -- the vendor's going to be a business associate in all cases; right? It's highly unlikely that the actual technology provider is not going to be. But an enabler of that technology, an enabler of a network that's not necessarily how to carry out business associate's functions in order to do the job that is envisioned for it.

Okay. Brian, let's go to AZ.

Hi. I was just typing the question. My question is getting to liability, and that is whether you can share any experience or information about industry standards for vendors accepting liability for technology failure, which results in a breach or ill harm to an individual, as opposed to the HIE organization?

Exactly. Vendors don't want to and -- but we -- on behalf of clients, we have been successful in -- usually they tell you to deal with this either with some kind of limitation on liability, but rarely with an exclusion of liability. But we've been successful in arguing that with the technology itself causes injury, that the technology supplier needs to be responsible for that, and they need product liability insurance to cover that. And so it comes down really to a question of leverage.

We're working with a very small rural exchange that will involve, at the very most, nine providers, and including a very small hospital, and they pick the technology solutions they really like. And their vendor has basically said, "We're not going to" -- "It's gleaning that liability, and you're waiving any responsibility that we have to your participants for that."

They did not insist upon being indemnified by third-party claims, and so they still are responsible to injured patients if their technology is found to have caused the injury. But within the network, they required disclaimer of that, and because of really the lack of clout on behalf of the network, they don't have a choice, and they're looking to insure against it themselves at this point.

Yeah, I'm sorry, I lost one part. I thought I heard a contradiction in there, which was the technology vendor is responsible for taking responsibility if their technology does something because of data that ends up causing ill harm or there's some sort of technology failure. But then I thought you said that the participants -- I lost something there in what you were saying.

All right. Well there's two kinds of liability there. There's a liability to an injured patient, and there's a liability to the network if the network is ultimately found to have some responsibility for a technology failure. And so your vendor is, generally speaking, going to push back on indemnifying the network against that liability and will want to impose some kind of limit of liability and that's a conversation that you need to have with them. The position I take on behalf of providers buying these systems is that there shouldn't be a cap on liability that relates to patient injury caused by technology. But that is the subject for contracts.

Between the vendor and the purchaser, the licensee, the licensee is not in a position to waive the rights of injured patients who may have a claim against the vendor. So what the vendor would ask for in that context is an indemnification from the licensee, from the network that if, in fact, the claim is made and they have to defend themselves and ultimately if there are damages to be paid, that they want to be indemnified by the network, and that's shifting responsibility to the network, and that would, assuming the network is solvent and can live up to that, remove that risk from the vendor. Whether that's the right answer, personally speaking for myself, I don't think it's the right answer but it is a matter of contractual negotiation, and what oftentimes we find clients that have entered into licenses kind of as a routine matter where they've waived all kinds of things they didn't know they were waiving, and they've had some unintended consequences regarding third-party liability. And so certainly, Amy, your question is certainly right on point. It's something to pay close attention to, and your address is really a matter of contract with your vendor to try to achieve what you as a licensee believes is the right result.

One point that may be helpful is that it may be a question that you want to raise with the vendor while they're responding to your proposal while they're bidding for the work rather than after they've been awarding the contract.

And that's a whole other presentation as well on procurement. We strongly believe that your license -- that the purchaser's license, the licenses ought to be included in the RFP, and that the responding vendors should react to that license so that their positions with respect to indemnification, service maintenance, all the kinds of things that are going to become important when you're under contract are discussed before you select the vendor and not after you've selected your vendor.

I have one here that says the presenters clearly speak from experience with lots of organizations, but I don't have a clear sense of how many of these Health Information Exchanges have actually been implemented. Can you speak to how much implementation traction this model has achieved at this point?

It's working in Mendocino; right?

Yeah.

That's the one I know of.

The Mid- South Alliance.

Mid-south; right. They're operating, obviously Indianapolis is operating, but if you go and look on the eHI website and probably on the AHRQs website, you'll see the communities that are up and running. If you look at the eHI surveys, it sounds like there's a lot more exchange happening then at least I'm personally aware of. But I think that in part the response and we've had more participants on this call than we've ever had on this topic. And we've spoken on this numerous times. And so it seems to me that communities are getting to the point where they really are saying, "Gee, it's time to go. We've made our technology selections and we're moving forward. We figured out a way to be sustainable, and now we have to document the user participation," and people are focusing on that, which leads me to believe that we're on the verge of a number of organizations that will be going live soon. But I'm really not an authority on whose -- I would tell you that the clients we're working with are generally in a very relatively -- I was going to say very, but a relatively preliminary stage toward implementation.

We have another question about the pilots. Have you created a minimum set of recommendations such as a subset of the documents? You had mentioned just taking specific or a smaller set of questions to address through your pilot. Do you have a model for that?

We've developed pilot agreements for various clients. The format of them is to try keep them as simple as possible and to really make them relate to a small number of participants dealing with a limited data set of exchanging under circumstances that are highly scrutinized and that have an end point and that everyone in the pilot commits to stay through the end point. And during that time, preliminary decisions are made about patient choice, about use, access, user authentication. But because of the manageable size of the pilot, they're more of a work in progress that requires a fair amount of baby sitting through it. So our average pilot agreement is, what, three or four pages?

That's right.

Right. And it really -- the big documents that attached to it is the pilot project description that goes through operationally how the pilot is going to work. And the agreement essentially says we're going to participate in the project as described in the pilot description, and then those descriptions tend to become kind of more robust over time as pilot planning gets more mature.

Okay. I think maybe one more question, and then we'll have to close. With all the depth of knowledge that you have on this subject, will you be participating in comments to CCHIT when the RHIO and HIN [PH] network certification starts in the fall with an environmental scan of what is out there and being used?

Well I'm involved in CCHIT, and I'm on the process advisory group, and so personally I'll expect to play a role in that. And I think CCHIT needs to be commended for the level of transparency that they've brought to this process of kind of inventing themselves and running it the way they do. Not just us, but just everyone who's thinking about these issues hard will enrich the CCHIT process by responding when they send out documentation for public comment.

I apologize to all the many, many people who submitted additional questions. We're supposed to end at 3:00. The e-mail addresses of our speakers are up on the website. I can't thank you both enough for the time you've taken to do this, and I know the long preparation to give us such a thorough overview of the work that you've been doing.

For all of you, I want to remind you that we have another web conference coming up on March 28th, "The Socio-Technical Aspects of Health Information Technology." Information and registration is available through the HEALTHIT.AHRQ website that's on the screen. And now I turn this back over to Brian.

Thanks, Susan, and I also want to thank the entire panel again for you participation today, and for everyone else for dialing in. I opened the poll a few minutes ago. I encourage you to provide us feed back. We take a look at this feedback. We share it with AHRQ. We pass it along to the presenters. So I know that all of those stake holders would appreciate your time in answering a couple questions before you log off today. And if you have any questions, please feel free to either e-mail us at the Resource Center or the presenters who were kind enough to put up their e-mail addresses on the screen. And for those of you who aren't familiar with the Resource Center's address, that is, the NRC-HEALTHIT@AHRQ.HHS.GOV. So again, thank you everyone, and have a great day.