

Health IT Joint Committee Collaboration

A Joint Policy and Standards Public Advisory Body on Health Information Technology
to the National Coordinator for Health IT



Joint Health IT Policy and Standards Committee Application Program Interface Task Force Final Transcript February 22, 2016

Presentation

Operator

All lines are now bridged.

Michelle Consolazio, MPH – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology

Thank you, good morning everyone this is Michelle Consolazio with the Office of the National Coordinator. This is a Joint meeting of the Health IT Policy and Health IT Standards Committee's API Task Force. This is a public call and there will be time for public comment at the end of today's call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Josh Mandel?

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Hello.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Josh. Meg Marshall?

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Hello, hi.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Meg. Aaron Miri?

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Hello.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Aaron. Aaron Seib? David Yak?

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, David. Drew Schiller is not able to join. Ivor Horn? Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Leslie. Linda Sanches?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Hello, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Linda. Rajiv Kumar? Richard Loomis? Robert Jarrin? And from ONC do we have Rose-Marie and Lucia?

Rose-Marie Nsahlai – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Here, hi, Michelle.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Anyone else from ONC on the line? Okay, with that I'll turn it over to you Josh and Meg.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Hi, great, thanks Michelle, this is Meg. So, I'm going to do a quick review of the agenda, I'm not sure that we have a ton of opening remarks. I know that we have a fairly light group today but we have quite a few important topics to discuss. We have just two more meetings I think before our draft

recommendations and then after which we'll have one additional one additional one before finalizing according to our current timeframe. So, lots of work to do, lots of great discussion to be had.

And first of all want to thank our OCR folks for joining us today. Throughout the hearings and I think some follow-up discussions topics around data ownership, patient access rights, HIPAA Security Rules as they relate to identity proofing and authentication came up and thought that it would be best to set aside some time for OCR to present their thoughts around how all of this should work. They've recently published some guidance that will be applicable to us.

So, certainly want to thank them and make sure that our primary focus for the call today is to make sure that we can listen to that presentation and have the ability to ask questions and other discussion. And then after that, if there is time, depending on the time that we have, we do have...we did not make it through all of the slides in our last meeting to review key themes that we heard from the panelists who were there so we would like to finish discussing those slides.

We need to figure out if there is more information that we need to gather so there will be hopefully identifying additional action items that we need to do, what other next steps that we need to have as we continue to march forward with framing our recommendations. So, with that I'd like to go ahead and get started, but Josh, do you have any other comments to add?

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

No, I think that's a great overview, thank you, Meg and looking forward to jumping in.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

All right, well, thanks, Michelle, I assume that we've got our OCR folks on the line and everything is all set to go?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Yes, hi, this is Linda Sanches, do you want us to just get started?

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Please, yes.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Okay. Well, I brought along two of my colleagues who are experts in different parts of the issues that were raised in the hearings and the discussions, first Marissa Gordon-Nguyen is going to talk with you about the guidance we put out around access. I will be speaking about recent guidance we created for health App developers which was circulated to you I believe last week, and then Nick Heesters is going to talk about the Security Rule and how it applies in some of these potential scenarios. Okay, so I will turn it over to Marissa.

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Great, hi, everyone. So, if you'll look at the slide that is...there we go the components. So, the components of the recent guidance that we put out were a fact sheet that was pretty extensive talking about different aspects of the individual right to access their own health information and then along with that we had several sets of FAQs on the issues that are highlighted here, scope of the right to access, form and format, and manner of access, and timeliness requirements, as well as a couple of additional FAQs that didn't fit into some of the big categories. And we have additional FAQs that are in development, there will be a lot more about permissible and not permissible fees for individuals and about directing access to third-parties. So, next slide, please.

So, a general statement of the right is that an individual or their personal representative on the individual's behalf has a right to access and/or receive a copy of their information upon request of the information in a designated record set. And a designated record set is a group of records maintained by or for a covered entity.

And if you look at the next slide I have put a number of examples of what is included, information that is subject to the right to access. So, you'll see that it goes quite a bit beyond the traditional medical record or an EHR, any other medical billing, payment type records, clinical laboratory test reports, all of these other things including old and archived PHI and designated record sets held by Business Associates are subject to access and this includes both information maintained in paper as well as electronic form that fits the definition.

On the next slide you can see examples that we provided in the guidance of information that's not included in that designated record set. So, these are the entities QI, QA records, patient safety activity records, business records and these are because they're not considered to be used to make decisions about individuals, that's sort of the underpinning of examples or the underpinning of what's in a designated record set that it's used to make decisions about individuals, whether it's the individual themselves that's the subject of the information that's making the request or other individuals.

So, then I have this very important "but" at the end of the slide, any underlying protected health information that's relied on in developing these business type records is subject to the right to access. So, the next slide.

So, in making requests a covered entity is permitted to require that requests be made in writing and on the covered entity's form as long as the individual is informed of this, and may offer the option of making an electronic request but cannot create a barrier to or unreasonably delay access and I'll talk a bit more about what we mean by unreasonable barriers.

But first I wanted to talk about verification because I understand that these issues come up in this area. And so we require a covered entity to take reasonable steps to verify the identity of an individual who is making a request for access.

We don't mandate in the rule a particular form of verification like obtaining a copy of a driver's license but we generally leave the type and the manner of verification to discretion and professional judgement of the entity with a very important caveat that the processes and measures of verification cannot create barriers to or unreasonably delay the individual from obtaining access to PHI and I'll talk more about that again in a moment.

But, verification can be done orally or in writing and in many cases it's going to depend on the way in which the individual requests or is going to receive the access itself whether that's going to be in person or by phone, if permitted by the covered entity in that way, or by faxing or e-mailing the request, or a secure web portal or by whatever other means are used.

So, if a covered entity requires that an access request be made on its own form the form could ask for some basic information about the individual that would enable the covered entity to verify that the person making the request is the subject of the information or is that individual's personal representative and Nick will talk after Linda about authentication requirements associated with the Security Rule.

So, if you look on the next slide here we are, what I've been promising, examples of what are unreasonable measures. So, we allow, as I said, an entity to require a request be made in writing and we say that there has to be a verification of the identity but there cannot be unreasonable barriers.

So, examples are an individual who wants a copy of her medical record mailed to her at her home address should not be required to physically come to the doctor's office to request access and provide proof of their identity in person to can't be required to use a web portal for requesting access because even in this day and age of course not all individuals have ready access to a portal.

Can't be required to mail an access request. This would...is considered to unreasonably delay a covered entity's receipt of the request and thus the individual's access.

So, a covered entity, as I said, may not require individuals to request access in these ways, but individuals can, you know, be permitted to do so and we encourage covered entities to offer multiple options to individuals for requesting access. So, the next slide, please.

In providing access we have timeliness requirements, it must be provided no later than within 30 days from when the request is received either by the covered entity or by its Business Associate if that is the entity that is receiving requests. For example, if the covered entity designates...informs individuals ahead of time that if they want to make requests they need to send it to a, you know, release of information vendor or something like that as long as doing so doesn't create a barrier.

So, regardless of which entity receives it 30 days is the limit, however, it may be extended to 30 days if the covered entity isn't able to meet the 30 days, but the individual has to be notified of this within the initial 30 days along with the reason for the delay and there can only be one extension per request made. Next slide, please.

So, form and format and manner of access. The requirement in the rule is to provide access in the form and format, and manner requested if it's readily producible in that way. So, if the request is made for paper copies the covered entity is required to provide a paper copy that is considered to be readily producible by all entities.

Then if requests are made for electronic copies, if PHI is maintained only on paper then we have, you know, if an electronic copy is readily producible it should be produced in electronic form and I'll move passed that one because we're talking really about APIs and electronic information here.

So, the important piece for this is the next bullet point, so if there is request for PHI that is maintained electronically the entity must provide access in the electronic form and format requested if readily producible and this includes unencrypted e-mail if it's requested by the individual.

We state clearly in the guidance that we consider unencrypted e-mail if requested by the individual to be readily producible by any entity and they, however, need to alert the individual of the risk of unauthorized access during transmission, but then go ahead and need to fulfill the request as made.

If it's not readily producible in the electronic form and format requested then in another agreed upon alternative electronic format so there is some, you know, room for back and forth with the individual and it's only if the individual refuses every offer to electronic format can an entity provide access on paper, provide a copy on paper.

So, we have a statement here on the next slide and in the guidance about the intersection here between the access right and certified EHR technology where we say that if a covered entity uses certified EHR technology the electronic PHI is readily producible as a general matter.

Covered entities can use their VDT mechanisms to fulfill access requests but only if the individual requests or accepts it in this way. As I said earlier, the entity can't require that the individual accept their information in this form, format and manner.

And I noted at the beginning that this right extends far beyond what's in, you know, certified electronic health information or certified EHR technology so that the individual always has a right to access other electronic PHI and other PHI in general in a designated record set that's not available through certified EHR technology.

So, if we look at the next slide we have a couple of additional elements I mentioned that we will have much more information coming out about fees in the next set of FAQs but we do talk about the basics of fees in the fact sheet that we released and so I'll go over it a little bit here.

The fees that are permitted are very limited. So, they can be...they have to be reasonable and cost-based and limited to the following items, labor for copying the information, supplies for creating a copy, postage if it's going to be mailed and preparation of an explanation or summary if the individual agrees. I haven't talked about that last piece so I'll just say briefly that we...a covered entity can produce an explanation along with the PHI to the individual if it would like to put the information in context or explain aspects of it as long as they ask the individual ahead of time and the individual agrees to receive that explanation.

Similarly, a summary can be produced by the entity in lieu of providing access to PHI, requested actual pieces of the record for example, only if the individual agrees. So, if the covered entity receives a request and determines that, you know, based on the nature of the request it seems that the individual is asking for, you know, a lot of information that might not make any sense to them. This could be a situation in which they say, you know, either we'd like to provide an explanation to you or they can say "we don't think this will be meaningful to you, can we provide you with a summary instead?"

In both cases the individual would need to agree and including agree to any fees that might be associated with developing those documents.

And then we explicitly say that fees that are reasonable and cost-based do not include any cost associated with verifying the individual's identity, with documentation, with search and retrieval for the information including if getting the PHI involves going to an offsite location where information is stored, costs of maintaining systems, and recouping capital along with other costs that we haven't expressly said are permitted.

And the very important star, point down here is that, you know, we're very aware that states have fee schedules in many cases about what types of fees can be charged to individuals to obtain their records and if those fees include for elements that are not permitted by the HIPAA Privacy Rule the Privacy Rule pre-empts, so those fees authorized by state law would not be permissible if they are...if they go beyond what the HIPAA Privacy Rule permits. And I think that's the last slide.

Let's see, and so I have questions here but I believe we want to get through all three of us and then do questions on the whole at the end. So, I will pass this onto Linda.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Thank you, Marissa. I'm going to talk just a bit about the guidance that we posted on our portal some weeks ago and you should have received already. Thank you for putting it to the next slide.

The two main, well let me back up, the guidance was designed to assist health IT developers who are not familiar with the requirements of the HIPAA Rule especially those related to Business Associates and in the guidance we provide information in sort of three different ways. We make some general statements about the requirements, we present a series of six scenarios and then we provide some key questions for entities to consider. So, all of the information on these slides is actually drawn from that guidance. Next slide, please.

So, the two main questions we address in the guidance are ones we have seen in many questions posed to us. The first is what protections, if any, from the HIPAA Rule might to information in health Apps used by individuals and when is that App developer covered by the HIPAA Rule. Next slide, please.

We also want to remind covered entities that in all cases it must use reasonable safeguards to protect health information and comply with all the other relevant rule requirements. Next slide, please.

So, when might an App developer be acting as a Business Associate to a covered entity? Well, the quick answer to that is when it's offering the App on behalf a covered entity and it involves health information.

So, a Business Associate is a person who creates, receives, maintains or transmits protected health information on behalf of a covered entity. You will see this language often because this is drawn from our Reg text and we want to help App developers consider these definitional terms.

So, again, it's create, receive, maintain or transmit protected health information on behalf of a covered entity or another Business Associate of a covered entity. So, next slide, please.

So, most vendors or contractors, including subcontractors that perform services or functions for covered entities that involve protected health information are Business Associates. And a company that has

access to PHI through a covered entity to provide and manage a personal health record or a portal offered by the covered entity to its patients or its health plan enrollees is a Business Associate.

So, as I mentioned, there are six scenarios but I've included only three of them here and I want to sort of walk through how we organized them. This is the first and it's the most simple, in this scenario a consumer downloads a health App to her smartphone and she puts her own information on it. There is no indication that there is any involvement with her provider are all.

So, based just on those facts we would not consider the App developer a HIPAA Business Associate because it's not creating, receiving, maintaining or transmitting PHI on behalf of a covered entity. Here it is clearly providing a service directly to the consumer to help her manage and organize her information.

So, the second scenario, next slide, please, what's new in this scenario is that she is drawing data from her doctor's EHR and using it in her App for her own purposes. So, she has a chronic condition, she downloads data from her doctor through a patient portal and then she uses it herself.

So, this also does not lead to the App developer being considered a Business Associate because while the App developer is helping the individual to draw information from the provider it's not doing it on behalf of the provider, it is really still hoping the consumer obtain information for her own purposes and there is no indication here, from the facts presented, that the provider or Business Associate of the provider hired the App developer to provide or to facilitate this service. Next slide, please, scenario three.

So here we've mixed it up a little bit more. So, here a patient goes to her doctor's office, the doctor request that she download a health App to her smartphone, the provider actually has a contract with this App developer and it is using the App developer to assist it with patient management services, remote patient health counseling, monitoring of patient exercise, providing messaging, and some, you know, application interfaces and some integration, and information the patient inputs is automatically incorporated into the provider EHR.

So, in this case we would definitely consider the App developer a Business Associate because it is in fact creating, receiving, maintaining and transmitting protected health information on behalf of the covered entity. The provider has contracted with the developer for these key services, these two key treatments and operational services and the App is a means for providing those services.

So, we've provided these scenarios to help App developers, you know, think through whether this is consistent with their own potential business plans and then we provide some key questions. Next slide. Next slide, thank you.

So, here we want entities to be thinking about what they're doing and the first question is, you know, does the App actually do anything with identifiable information? If in fact it doesn't then they don't need to be worried about this at all.

The next question is, who are your clients, how are you funded? These are various ways to think about whether you're doing work on behalf of or as a service to a covered entity or a Business Associate of a covered entity. So thinking about who are their clients, how are you paid, who is the final recipient of your services if you're a subcontractor? So, these are just various questions to help people think this through.

So, I'm going to stop there and turn it over to my colleague, Nick Heesters, who is going to talk about the Security Rule and how it might apply here.

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Thank you, Linda, hello, everyone, so my name is Nick Heesters and I'm going to talk a little bit about the application of the Security Rule for Apps and APIs.

So, one thing, just to be a little bit holistic, there are some general overarching considerations for Security Rule compliance and we've...I think both Marissa and Linda spoke to those, but just to echo those again, some of those general requirements include that the covered entity or Business Associate needs to ensure the confidentiality, integrity and availability of all of ePHI that's created, received, maintained or transmitted that they need to protect against reasonably anticipated threats or hazards to secure the integrity of ePHI and also protect against reasonably anticipated user disclosures of ePHI not permitted or required under the Privacy Rule and to ensure workforce compliance with the Security Rule.

There is also a maintenance component to this which I didn't include in the slide but it's just worth mentioning that is also an overarching requirement that for whatever security measures are implemented that those measures are, you know, reviewed and modified in response to new situations to enable the protection of the security of ePHI that's protected. Next slide.

So, from the prior workgroup meeting there were some API certification criteria so I thought it would be good to look at maybe how some of that certification criteria would map into some of the Security Rules technical safeguards. So, one of those areas we had in the API certification criteria included the authentication access control and authorization, and that maps into technical safeguards in the Security Rule for access controls and person or entity authentication. API certification criteria for trusted connections would fall into the Security Rule's integrity and encryption standard and specifications. And the auditing actions or auditable events of certified API would fall into the Security Rule's audit control standard. Next slide, please.

So, in the Security Rule access controls is there for a requirement to implement technical controls to only allow access to ePHI to those persons or programs that have been granted those access rights. Now the Security Rule was designed to be flexible, scalable and technology neutral so that as new technologies were implemented, new threats were discovered that the Security Rule could be flexible and scalable to be able to meet those new requirements.

So, one of these was envisioned in the area of access control. The Security Rule, as it was, originally envisioned did propose a few specific access control types context-based access, role-based access, user-based access, you know, what have you. In the final implementation of the rule those were all deleted to provide the flexibility of the rule and of the covered entities and Business Associates to be able to implement whatever type of access control would best be able to be used to ensure that the access to ePHI is limited to only those individuals or programs that are supposed to have that particular access.

A little typo in my slide, I list some implementation specifications regarding the access controls those are not all addressable the first two are required and the automatic logoff and encryption/decryption are actually addressable specifications.

So, just to go over those, unique user IDs need to have some mechanism of uniqueness into who was accessing or what is accessing ePHI to be able to identify and track that usage, emergency access depending on what type of App is being used, you know, would go to how any type of emergency would be foreseen or implemented, automatic logoff. In an API scenario this may be related to maybe some token parameters either token revocation or expiration it could potentially be addressed that way.

Encryption and decryption in an access control perspective is looking at the encryption of stored data. So, if there is an App that is going to store data then it is going to need to consider how they're going to meet the specification for encryption of the data that is stored. There is a separate standard and specification for PHI that is going to be electronically transmitted and to ensure that this is secured and we'll get to that in a little bit. Next slide, please.

So, person or entity authentication, so this is fairly straightforward and what the rule requires, it requires that there be technical procedures that are put in place that is going to verify that the person or an entity that is going to seek access to the ePHI is the person or entity that is claimed to be seeking that access.

And again, you know, similar to access controls the Security Rule originally had some very specific ideas as to how authentication would take place. There was a requirement to include one of either a biometric, a password, a PIN or a telephone call back as a solution or the use of a physical token to facilitate that authentication.

And again, in the spirit of being flexible, scalable and technology neutral in the final rule these were all deleted to make this be more open for entities to be able to choose what authentication mechanism is going to be most appropriate to their use so long as it meets the requirement to verify that person or identity that is seeking that access to ePHI that they are in fact the one claimed. Next slide, please.

Integrity, there is an integrity requirement that we talked about in the context of the API certification criteria. There is a...and this is just to ensure that ePHI is protected from improper alteration or destruction. There is an addressable specification to authenticate ePHI. These could be accomplished by, you know, many different mechanisms some of which an API or App may build into itself or which may leverage the capabilities of a particular network layer, HMAC or some type of hashing mechanism could help in ensuring the integrity of the ePHI data in this respect. Next slide, please.

Encryption, this is encryption with respect to protecting the electronic transmissions of ePHI and that, you know, within the specification of the rule that this is addressable to implement a mechanism that is going to encrypt that ePHI whenever it's going to be an appropriate mechanism for ensuring the protection of that data as it is electronically transmitted.

There is some guidance as part of the breach notification rule for what it means to secure PHI and part of that guidance talks about what it means to secure electronic transmissions of PHI so that it can be made unusable, unreadable or indecipherable by use of encryption and that guidance includes the potential use of encryption at the TLS and SSL layer, such usage should comply with the NIST special publication guidance on TLS and SSL or a transmission encryption solution which uses FIPS 140-2

encryption solution and I believe that this guidance for encrypting electronic transmissions mirrors some of the encryption certification criteria that's out there for the API certification. Next slide, please. Next slide, please.

And audit controls, another one that is...maps to one of the API certification criteria and this is the mechanism by which that activity...that there are some kind of controls or mechanisms that are in place that are going to be able to record and permit the examination of activity in information systems that are going to contain or use that ePHI. Next slide, please. Okay, so I think that was all.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Okay...

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Okay, great, fantastic, this is Meg, so are we...are you able to open up for questions now?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Yes.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Okay. Leslie, was that you? I think I talked over you.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Yes, that's fine.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yes, this is Leslie, I have a question. So, I'd like to go back to slide 22 as a reference point that talks about scenario three and this is a scenario...and I want to understand the trigger points of when a relationship switches from a consumer relationship to a relationship that is covered by the BAA.

So, for example, I think there will be very likely that providers will have their own App Store and these Apps might simply be ones that the provider says "I endorse" or "trust." They may have a Business Associate relationship, they may not but let's take the example of one where, for instance, let's say somebody is an Allscripts user and they want to incorporate the population health product from that vendor, that population health product might simply need to use an open API and establish a relationship with that patient apart from the BAA relationship from the provider, it's simply an endorsed product versus one that is directed by the provider.

The dataset moved might be both the minimum dataset or the common dataset we talked about or the definition we used up above with the access rights data, but let's say in that initial phase it is just what we have on the open API.

I think there will be many cases where there will be provider endorsed, but not directed, and data provided to the patient through the API with the assumption that the BAA relationship does not exist but this is a new established relationship with the consumer to use the product, it might include something like a notice of privacy practice or a warning label.

So, I'd like to understand what are the trigger events that move an existing BAA vendor of a provider who has products that will use the open API and not have a relationship with the provider other than this endorsement. Where do they fall in all of this? Because this seems a very likely scenario.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Yes, you know, I'm now kicking myself that I didn't present all the scenarios because we have two scenarios that gets to that although I have to say we didn't address the API component of that in the scenarios.

We...I don't want to speak exactly to what you just said because I'm sure I will miss something, but two thoughts, we definitely anticipate that there are entities out there who have many different products and one of their products may be with...providing the service to a covered entity like Allscripts, they may in fact be the vendor for a particular provider and obviously are a Business Associate there, but may in fact have other offerings for which they are not going to the healthcare provider, which they might be offering directly to an individual and the individual is making the choice to use that particular piece of, you know, software and in that case...you know if that is the case and the protected health information of the provider is not being managed in some way by the App developer then, yes, they would have to wear two hats. They would be a Business Associate to the extent that they are offering a product or providing services to the covered entity and then their other product, which is directly to the consumer, would not be a BAA relationship.

So, the information that is part of the relationship with the covered entity would be covered by the HIPAA Rule but the information that is circulated in a variety of ways through the other consumer-directed App would not be subject to the HIPAA Rule protection.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay, so that's confusing. Let me just follow-on, because if the data originating under the EMR or the HIT that's provided under the BAA relationship...if I move that to the API model and that API is connected to an App that the consumer directs regardless of what the relationship is that the data should still be at the consumer's control and is not covered under HIPAA, correct?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Ah...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Because it still was at one time PHI, it's not when they now connect it to the new App, so that's questions one. And then follow-up to that is...and that should be independent of whether the App creator was a BAA or not.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Now if the App creator then also by virtue of being a BAA provides data to the API that's beyond the clinical dataset we...the dataset we originally think of in this open API does that make them fall again now into a BAA or are they still, based upon that API connection at the patient's will, still considered a consumer App and therefore not falling into it? Because this is...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

An...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Area of gray is going to be I think the highest initial use.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Sure and I'd love to talk with you later to see if there are ways we can clarify and add to the guidance we have out there. But generally the way to focus is on what is the relationship of the developer to the consumer and the source of the data? Are they doing work on behalf of a provider? Is the provider paying them to be doing whatever it is they're doing with the protected health information or sorry the health information, we don't know yet if it's protected?

If they're working on behalf of the provider, they're getting paid by the provider then it's quite likely that they are a Business Associate and subject to that work, to those requirements.

But if they're really only doing what they're doing at the direction of the consumer then they're not a Business Associate for that particular function because, you know, as you pointed out there are lots of organization out there that have a variety of product lines and some based on their relationship with the covered entity will in fact be Business Associates and some will not.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So...right, but I think it's highly likely, let's say provider number one is a Business Associate with Allscripts and they say, look we want you to provide a population health App and that needs to be direct to consumer relationship because that consumer might have 14 different providers with which we don't have a BAA agreement. So, the patient comes in, goes to the website, downloads the App that connects to the API.

The licensing arrangement for the use of that App is from covered entity number one but the actual control and attachment of the App is from the patient and the patient will then use that App to connect to many, many other providers on the open API.

What we want to make sure is that whether the initial relationship that had the licensing agreement is not hampered by the...or becomes ineffective because of that relationship when they move to a much more open and much more community level product use.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, I can't speak to the licensing agreement.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Because that's not really within...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I'm sorry I thought that's what you meant by business agreement and paid for. If you pay a software vendor for something...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Right, well, I'm...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It's a license generally.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Talking there about the Business Associate Agreement which is something required in the privacy and the security rules that basically there are certain provisions in it in which the Business Associate swears basically or agrees in the contract to ensure that certain protections are in there, that the protected health information will be safeguarded, that they will not do anything with the information that wouldn't be permitted under the Privacy Rule or the Security Rule, that the safeguards are appropriate. So, there's a variety of provisions in the Business Associate Agreement that apply. So, that's what I was talking about there.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

And this is Aaron Miri I'm a CIO for a hospital and I really appreciate the explanation but I want to tag on and just add a little bit more color as a provider to what Leslie is speaking towards in that a lot of the development work that the provider community is working on, and there are some phenomenal organizations right now doing excellent pioneering in this, you know, custom developing Apps and whatnot, but the fear factor that's there because of those triggers not being so readily defined is holding

back the community and/or creating an ecosystem of likeminded individuals only. So, we're all sharing the same EMR platform and we're only going to share among that one EMR platform or whatnot.

And so inadvertently, in the quest to do the right thing, which I think every provider is in agreement with the OCR that we must protect patient's rights, we must protect their protected health information that's a given, we must do that, the unknown factor of how do you open up your EMR data without exposing yourself as an organization inadvertently is leading to a culture of "I want to but I'm going to standstill and let somebody else go first."

And so I have to echo what Leslie is saying there in that even I as a hospital CIO I'm very clear when it's my EMR vendor, okay, they're going to do some work for me, I must have that BAA, it must be clear, but if it's somebody else out there that wants to simply access their EMR data with a personal App now how does work, because, you know, there are, to your point there, some scenarios, some limits there, some triggers but at what point is it that I must have a BAA with them or should I just default and always have a BAA with anybody accessing it?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

You only need to have a BAA if they're actually working for you. If you call them up and hired them and you're paying them to do something that's the easiest way to think about it. Are they doing it for you? Or did you just say to your patient "this is a really nifty App you might want to download it and use it and when you use it you can get some of your records out of my EMR." Okay?

The Business Associate relationship is when you're using that App developer for yourself. And if you go back to scenario one and two.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Actually go back to scenario two. You know in this case, you know, she has downloaded a health App, she uses it to get information, the provider I'm assuming knows about this, is aware of the App that she might be using and is providing the information but there is no need for a Business Associate Agreement in this case because the relationship of the App developer is with the consumer.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right and I completely understand it. I guess where I'm falling upon and it could just be maybe paranoia on my part again trying to do the right thing is you're basically staying towards net benefit, so you're saying there's a...if there's any sort of net benefit towards the organization have a BAA even if the work is for free if I'm going to get something out of it maybe even it's, hey a better diagnostic interpretation because the data is aggregated in some form or fashion that BAA should exist. But if you do something with the data and I have no net benefit as an organization, hey, it's "I don't care about it." Is that what I'm understanding?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Why don't we go down a few slides to the key questions? One further up. No, there you go. I mean, yeah, net benefit is a good concept and it sounds like some of these Apps might be working for you for free, but what's really...it's even a step back further than that or forward than that, you know, did you hire them? You know are they really working for you?

If they're just an organization that's come to you saying "hey, I think this is a really cool thing, would you, you know, make this available to people" and they're not working for you, they're not...and you're not giving them protected health information so that they can do something on your behalf with it then they're not a Business Associate.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So, this is Leslie again and I have big concerns about this because it's a form of data blocking in some way because the...what we're saying is that if it benefits an entity there's a BAA agreement, if not and it solely benefits the patient to know and understand there isn't, that further increases the divide of information because really the provider entity can't exist without a patient relationship. And when they do something to benefit that patient like access to the information they want to benefit the whole of that patient in their future care or in that care today.

And so we want to make sure that we're not penalizing the providers who have good will and want to say "hey, this is a really great App and we know it because it is...we know it we're a Cerner shop and this is provided by Cerner and, you know, we pay for a big relationship with Cerner, they're doing this free, but, hey if you connect to the Cerner API through your open App you've got all that information and you can choose to do stuff with us back to our provider or not, it's all your choice, you can use it any way as you want."

But if we somehow tell the main EMR vendor that their relationship can solely be one as a BAA then we will actually disintermediate the patient from the richest information that's going to come beyond the current constraints we've defined in the API.

So, I think there is an unintended consequence of this kind of interpretation that I'm concerned about.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

But I...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

The ideal situation would be that any patient's App whether it is funded by or endorsed by a provider, or on a list of the Good Housekeeping Seal of HIMSS that says these APIs would work or these Apps would work, the patient should benefit from that information and benefit from that access and if it's constrained in a way that means one vendor has higher consumer goodness than another we actually stifle the creativity that might come out of the largest funded organizations right now which are the EMR vendors who are trying to move to a more population health holistic way so they'll say "hey, we've got this App, it's great for population health, we want the patient to own and control any use of it but

because we've used the open API as well as some of our proprietary information we now can contribute in a way to help manage that patient across providers who use or don't use our EMR." So, I...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

And that's completely permitted by what I was just saying.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

As a BAA but not as a...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

I think...I think I must have misstated something and I apologize completely. When an entity has a Business Associate relationship that doesn't mean that they can't provide information to a consumer at all. It only means that they must work with the covered entity to assure that appropriate protections are in place.

But in addition, the kinds of things you just talked about are permitted. If you have a large vendor who wants to offer separate products to the consumer they are absolutely able to do so and they do not need a Business Associate arrangement to do so if they're not using protected health information provided by a covered entity on behalf of the covered entity.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But the nature of the...is that they will always be using PHI that was originated in the covered entity if their consumer App connects to the API. It is generated as PHI.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

So, they would...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

They would be doing it...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

They...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

They would be doing it on behalf of the patients...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Right and that's permitted.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Who have now signed up.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

And there is no Business Associate arrangement required. Under this, if you go back to the scenarios, two or, you know, scenario two. The individual here is getting access to provider information, right? She is using the App to get information from her doctor but there is no Business Associate arrangement required here because the developer is doing this on behalf of the individual. So, she is gaining access to her doctor's information or information about her, PHI, held by her doctor. She is gaining access through this App and using it for her own purposes and there is no Business Associate arrangement required because the developer is working for the consumer and not for the covered entity.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right and...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But they might...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

This is Aaron Miri again just...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But they might be doing both.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

So...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Go ahead, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Let me ask this and I'm going to try to add this from a consumer perspective because I love stories and scenarios sort of help me understand in my non-clinical mind. So, me as Aaron, if I were to download my data from my EMR and I suddenly see, oh, you know, what my weight is trending up, my blood pressure is trending up, I've got to lose some weight so my blood pressure comes down and I go exercise, okay, that construct, the way I downloaded that software that gave me the net benefit as the patient, hey, guess what there's no BAA needed.

But, if I were to take that data and suddenly go back to the hospital and go, hey, what do you make of this, what should I do? You know there's some better interpretation of this data. Does that mean now a BAA is needed?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

No.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Because the hospital got re-involved again?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

No. No, because the doctor is not involved in the creation...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Right.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Or storage of that information. There is no relationship here between the doctor and the vendor. The relationship is always through the individual and there is no BAA required there.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yeah.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Well, I think this...this is Leslie again, I think we really need clarity on what is a relationship...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

I agree.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Between a BAA...as a BAA and when does that relationship allow it to be a consumer App, because this area I think that we're seeing huge innovations from the EMR vendors who are going to come forward with Apps that connect but they may have, by virtue of their licensing arrangement with their covered entity, the ability to offer free services to their client. They shouldn't be then...a BAA in that new relationship with the patient.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So it's just...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

She hit the nail on the head and guys, I'm happy to...this is Aaron again, I'm happy to talk more off line on some real world scenarios. This is what has killed...this lack of understanding and clarity...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yeah.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Is what killed HIEs, is what's killed the ability for hospitals to want to share with each other, has killed a lot of the innovation, again, inadvertently and I think we could really kill a lot of birds with one stone by simply clarifying this for everybody.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Sure.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

I'm happy to talk off line more about it.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

We developed this...the guidance that was shared last week with all...the six scenarios. I believe you received it last week. We developed it actually for that purpose. So, I would be...it would be really wonderful if you all could take a look at all six scenarios and if you feel like there is more that needs to be...if you have some other specific questions I would love to hear them and I'd be happy to try to address them.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

So...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Wonderful, thank you.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

This is Aaron...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

That would be great, thank you.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

This is Aaron, I just want to confirm I have read all of those and I want to make sure that I understand, you know, from a different perspective how or when a BAA would be required. And I think about it more from the perspective of who is making disclosure decisions, right?

So, if my provider has an EMR that offers a consumer-facing application and that makes it easy for me to...for my application to have access to PHI stored in the EMR but it also allows me to have access to bring in data from other sources or to annotate the information from the EMR that's used by my provider, but as long as the provider doesn't have the authority to access the consumer controlled data no BAA is required.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, it's not...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

What understand the BAA is not required but the consumer can push back or release or authorize to disclose back to his provider or any of his providers the information in that without requirements for a BAA.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, in the case you just mentioned no BAA is required but it doesn't matter whether the provider has access to it or not, it's whether...it's whether work is being done on behalf of the provider.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Okay.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

In the case you just mentioned this is all consumer generated, consumer centered...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yes.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

And there is no requirement for a BAA in such a circumstance.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

But...

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yeah, this is Aaron Miri again; I guess it goes back to the net benefit of the organization. And just for clarification, there are two Aaron's on this call, but I think it goes back to net benefit, who benefits from this, from the data.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, I mean...

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

So, this is...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

I think in all cases the consumer should benefit. The provider might benefit as well because they may be receiving information. In one of the scenarios we have, you know, reports going from the individual to the provider and so the provider is gaining information necessary to improve providing care but since it's all done at the direction of the consumer there is no Business Associate arrangement required.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Yeah, this is Josh; I just want to clarify...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But I don't...I think the benefit is not just the consumer but the providers. I mean, we want providers to be...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

At risk, yeah.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Informed.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yeah.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

We want providers to feel that their patients are engaged and contributing to their own health and they're co-producers of health.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Yeah, so this is...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And so...so it's just a concern that this idea of net benefit, it should, as you said earlier, it should be the patient that benefits and if we believe that there's a holistic patient relationship with providers they do. And I just want to make sure that a provider who is trying to be thoughtful and promote something with an organization they currently have a BAA with to use a consumer-facing App that both the provider and patient benefit from they are not in any way hamstrung by having to have a BAA agreement for a consumer who...the consumer is the only one who can take that App and attach it to the API. They have an action to take and that relationship should be the action that determines whether there's a BAA or not. Not whether there was a licensing fee or an existing business relationship or...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Whether the provider has some gain it's too hard to interpret. The only thing we have is to have...the only action we know that's deliberate and contained within the consumer's authority is to attach their App of their choice to the API regardless of whether it comes from the main EMR vendor or an existing BAA relationship. And that's the kind of clarity we need...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

As we go down a path to say who benefits we will have the same confusion we have now that Aaron brought up HIEs, you know, trying to figure out how to get things done, EMR vendors cautious about participating and stopping innovation when we really do have a huge opportunity as a result of this API connection...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Where the consumer is directing it. Let's give them everything they can and not prohibit them because innovation is perceived to benefit a provider and I'll get off my soapbox.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Okay, so this is Josh...

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

This is...

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

I just want to say I think we're being sidetracked by this concept of benefit. I thought the guidance from OCR was quite clear and it never invokes or mentions the concept of benefit and I don't think it's a helpful concept for our discussion. Lots of people should benefit from lots of things but it's not the crux on which these issues hinge, at least as far as I can tell.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Correct.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

I just want to also note, because I want to be sure there isn't a misunderstanding here, that if there is a situation where there is a Business Associate relationship that relationship does not stop the entity from having another relationship with the individual, with providing the services to the individual. The only reason that wouldn't happen is if the provider said they could not and I don't think that's what we're talking about here.

I think in these...you know if a third-party creates an App and it is taken up by the individual and used by the individual then there is no Business Associate relationship created.

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

And this is Marissa in OCR, I also want to...I want to highlight what Josh said a minute ago I think that this hopefully is helpful in improving the understanding that, you know, the benefit is not a helpful concept in understanding here. The important aspect is, you know, whether the provider itself engaged the services of a vendor; in that case the actions taken with the vendor using protected health information make them...put them into a Business Associate relationship with the provider.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

And this is Josh, I want to see if I can follow-up right on this point because I...so I think the notion of whether the covered entity engaged the services is somewhat clear but it's not obvious to me that this is the essential thing.

So, I could imagine, for example, a scenario where a hospital decides to make an investment in an App development company that they think could, you know, provide some useful features today and they think, you know what next year if they offered these new features it would be even better. So, they hire the company to build some new features into their platform and they make it available to their patients but it's still only available to the patients as a patient decision. In other words the covered entity is not

sending any data to this App except in cases where the patient authorizes it and agrees. In a situation like that would they really need a BAA just because they had hired the App developer?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

No and...

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Well, the question then would be whether the App developer has access to information as it does its work. So, it wouldn't be about whether information is going through the App in that case. If you're, you know, you're talking about modifying technology as the service that they're providing to the provider then the question is whether in doing that they have access to protected health information.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Yeah, so...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So, what you're...

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

And it seems to me...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Can I...this is Linda; I just want to add on to that. If it's all consumer directed, if it's always the consumer saying, give me access to this information or provide this information to my provider, if it's always consumer directed then it is highly unlikely there's a Business Associate arrangement.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Yeah, so I think that's very clear...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But...

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

And it's slightly different than what the...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yes.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Guidance says today. The guidance is really focused on this notion of hiring, which is a shortcut and a useful shortcut, but it seems like the real crux of it is does the data flow without the patient's permission or is the only way for data to flow because the patient authorized it?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And so that could be...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

So...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

In two forms, right, Josh, I could have a BAA relationship. I've developed an App that uses PHI not through the open API but it requires patient consent to use that App that's one function and the other function then says, if the patient takes an active step in connecting the data...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Right.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

To an App that the only source of that data comes through that action then that's clearly not under a BAA even if that App was provided by Cerner who was the EHR...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Agree.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Under a BAA. Correct? Is that right?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, I think I lost part of you in the middle, but yes, the fact that it's offered by Cerner is not relevant. It doesn't matter if Cerner has a relationship with the provider to provide all kinds of things.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Right.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

They can have a...offer a separate product that is not based on their relationship with the covered entity. They can offer it directly to the consumer. The consumer can take it up and use it to exercise her access right to the information in the provider's certified EHR and there is no Business Associate

relationship that's involved with that. She has downloaded it, she's using it, she's using it to access her information. It doesn't matter if it's Cerner or anyone else.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

So, this is Meg, here's my question and I just want to make sure that we're not un-intending, you know, that the consequences aren't putting up these artificial barriers just to get to that BAA because some providers are going to be more comfortable there.

So, in your scenario where Cerner or Allscripts, or whomever, what can we do to make sure that what you just stated does not lead toward Allscripts or Cerner creating an App for every one of their providers and therefore because they're engaging with that provider it requires the BAA.

And I think that what we want to get to...we don't want to have further segmentation like the issues that we're seeing with portals, right, and I think Aaron and Leslie talked really well around the, you know, the value of having the ability for these Apps to do data aggregation.

So, I just want to make sure that, you know, the rules that we're hearing aren't setting up these artificial barriers where the consequences will be because the providers do want that, that BAA because they will feel more protected that they won't engage with a Cerner or engage with an Allscripts specifically to create an App just to get that BAA.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, I'm not sure...

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Another way...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Go ahead.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

I want to try this, this is Aaron Seib, I'm a hospital administrator, I'm running a hospital, I'm at risk and my EMR vendor provides also a PHR product that I want to sponsor and make available to my consumers. As long as it takes an action of the consumer to use it there is no BAA required?

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

This is Marissa, you can't make that type of categorical statement.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yeah, too much?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, it's because there's...if you have hired them it's hard to know what else you have hired them to do and whether...and to what extent they are managing protected health information for you. So, that's why if you look at our scenarios we're saying based on the facts presented.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Yeah.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

So, if you're hiring them to run the PHR then likely they are your Business Associate because you've hired them to design a way for information to flow to your patients.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Right. So, for that particular service where its consumer controlled data it still requires a BAA between the covered entity and the product vendor?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

If the covered entity is hired...has decided to offer that product as a way of communicating with its...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So, that's where it gets critical because...so there is one example, in the normal tethered PHR that seems to be reasonable because a tethered PHR is using PHI as part of their operation.

Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)

Right.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But now I have a new product offering that's not tethered and that the only way that product offering can have access to data is through the API that the consumer controls the attachment of. And in that case, what you just described, it would not be covered...it would not be a BAA regardless of whether that second offering was done by Cerner or done by Joe's Barber Shop.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

It is correct that a separate product line that is offered to an individual who then uses it to gain access to their information...you're right it doesn't matter if it's made by a local college student or Cerner because it's a separate product line and you can actually...I think that's actually our scenario number six in the handout...I'm not sure.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Josh, I think we got the six scenarios.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

So, maybe...this is Meg, maybe one of the things that would be helpful is for us to create and maybe document and perhaps even diagram some of these additional use cases and get your feedback from, you know, just to make sure that we're all on the same page with our understanding of where the BAA would be necessary or where it would be helpful and where we could expect it. Does that sound like something that we could maybe do and come back to you with?

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

That would be wonderful.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

I would be glad to look at it.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

And this is Aaron Miri, that would be super helpful as a hospital CIO too because then I have further questions how the FTC and other organizations play into this especially as related to protected health information. There are just a lot of variables particularly as a hospital we're dealing with manufacturers, App developers, EMR, I mean, all sorts of players that want to use the data appropriately and responsibly. So, thank you for all the clarification, we really appreciate it.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

You're welcome and I'm happy to take a look, you know, I have to caution, I don't know if I can answer all questions because I haven't seen them yet, but to the extent that we are able to provide guidance to you we'll certainly try.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Yeah, I mean, I think, you can tell based on our passion of our comments that we were desperately seeking clarity on a lot of this stuff because it is right now a culture, real culture in the community of fear which is causing us to stand still and folks perceiving that the rules of the road are not clearly identified so nobody wants to drive on them per se and then when you have other external agencies like the FTC and others weighing in all on HIPAA items it becomes a scary proposition when we're just not understanding and it could be cleared up with some very clear communication. So, thank you, again.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

You're welcome.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Hi, can I take this in a slightly different direction?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Sure.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Yeah, hi, this is David Yakimischak, and thank you so much, I mean, this is so helpful, but I want to understand if you could just direct me or the group to areas around things like surveillance and enforcement and could you just point out under what authority this is acting in terms of, again, surveillance and enforcement.

So, under the HIPAA Rule what is the...what is the mechanism and the penalty for a provider who either fails to or cannot meet the requirements for disclosure and what about more like the specific details so they're not disagreeing or they're not trying to block access but they're just not meeting some of the criteria or conditions of the recommendation.

So, could you just speak to a moment around that whole area of surveillance and enforcement?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Well, we have wide ranging ability to enforce the HIPAA Rule we respond to complaints, we receive breach notifications and follow up on those, we open up compliance reviews so...and in those we try...when we conduct those investigations to resolve them through technical assistance and working with entities to come up with corrective action plans since the goal of course is always to improve the protection of the information.

We do also have the ability to assess civil money penalties depending on the type of violation and whether it was a simple oversight versus willful neglect and so there are a variety of tools available to us to deal with non-compliance that we find.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

And is all of that contained within the HIPAA Rule or are there other regulations that we should be aware of regarding that?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

That's within the HIPAA Rule. There are other regulatory schemes that apply. The FTC also regulates but not exactly the same way. They receive breach notifications of breaches that would not be breaches under our rule, so for...basically for non...not for covered entities who have to report for...and Business Associates.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

And by the way this is not so much about breach but more about non-compliance with the regulations...

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

Right.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

That I'm looking at...that I'm thinking of.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

So, in terms of providing someone's access rights all those sorts of tools I mentioned would apply. So, you know, we could certainly investigate to make sure that someone's access was actually applied. We can see whether this is a problem with one particular person or whether it's a systemic problem with the entity and we, you know, use various tools to go with that.

We actually do have several pages on our website that talk about our enforcement authority and I'm happy to send you some links to that.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Well, maybe that would be helpful. So, we can say that access to data by a patient to their own data is a civil right that's protected under federal law and governed within the HIPAA Rule and potentially other regulations such that there are...there's enforcement capability and penalties due to any provider who may not comply with these regulations.

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services

That's absolutely right. Marissa did you want to add anything?

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

No, I think that's well said.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Okay, and are there state regulations that either can supersede or vice versa be superseded by federal regulation in this particular area?

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Sure, so the example that I provided had to do with fees, so if a state law provides authorization for businesses to charge fees for records to provide them to individuals that are, you know, more than what the HIPAA Privacy Rule would permit then HIPAA would pre-empt that.

Our general pre-emption rule is that if a state law for example provides easier access to information or provides improved privacy or security protections for information than those are not pre-empted. HIPAA is the baseline.

But if there is something in state law that's more permissive with respect to uses in disclosures that could be made of individual's information or that provides easier access to individuals those would not be pre-empted.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Okay.

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Did I just say the same thing twice?

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

Thank you, no it's fine, I get the gist of it and that's the intent...

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Okay.

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

I was looking for. Thank you very much.

Marissa Gordon-Nguyen, MPH, JD – Senior Health Information Privacy Specialist – Office for Civil Rights

Sure.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

So, I think we might have time for one more question. We're actually...we're out of time I think...we're not going to be able to get to the rest of our topics but this has been a great discussion and I don't necessarily want to cut it off but I think before Michelle makes us go to public we might have time for one more.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

I have one more if it's okay? This is Aaron Miri and this is a little bit more technical so maybe for Nicholas Heesters if he is still on the call?

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Yes.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

And I appreciate, again as a hospital provider, the concept of making sure that technology is open and fair and sort of general, we can drive things forward, but is there any consideration for starting to raise the minimum standard of what's required?

I understand and I heard from you...say earlier that there were some more technical granular controls built in and those were removed in the final rule.

Are there any consideration points given how technology is advancing to raise that minimum standard and start saying things like you've got to have a minimum 128 bit encryption and those sorts of things? Are those concepts coming to play or are we still basically keeping the playing field very open?

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Well, in a general sense the idea is to have the requirements of the rules remain flexible, scalable technology neutral. As far as some of that more granularity regarding certainly encryption standards in order to enter safe harbor and consider your PHI secured so that you wouldn't have to go through a recertification process for encryption there is guidance in there that is accepted for what constitutes secure PHI from an encryption stand-point and that does reference some of the NIST special publications and there...for data at REST the guidance does specifically reference to use AES whenever that would be practicable and also some of the other documents that were referenced in the encryption for securing electronic transmissions of PHI regarding the use of TLS and SSL with respect to NIST guidance as well as other encryption algorithms that are a part of the federal information processing standard 140-2.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right and I can appreciate that, but I just want to interject a real world scenario here where is that I'm aware of scenarios playing out in the provider marketplace in the real world where a very detailed risk assessment, the risk is accepted, other mitigating controls are in place which circumvent the need to encrypt because you've done everything else and you as an organization discussed, documented and did not encrypt...let's assume it's a special modality of some sort that cannot be encrypted for latency purposes and thus you have manufacturers as well as providers circumventing the rule because of other controls in place.

My question was more or less eliminating some of those loopholes and forcing the marketplace to evolve to a higher standard of operating, even though that's a little bit more granular controlled, in that open model we just talked about. I'm asking is there any consideration for those sorts of things?

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Well, there's not a movement for a new rulemaking, but, you know, we do look at those items on a case by case basis from an enforcement stand-point. There have been, you know, published resolution agreements where for instance stolen laptops have had security mechanisms in place regarding software or firmware enabled LoJack systems which was used to securely wipe the laptop and some authentication on password controls for the laptop, but where the laptop was not encrypted, and as part of our enforcement activities it was determined that due to the high risk of having that PHI unencrypted on a mobile device that those mitigating controls were not sufficient.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Right and I can appreciate that. I guess, as a hospital it leaves you kind of in a precarious state of do you suddenly eliminate the entire maybe vendor or subset of vendors that are not offering encrypted devices because they feel that these other mitigating controls are there but the interpretation is that, well that's not good enough.

So, I guess that was my point was, you know, I think that there's maybe some potential for opportunity to clarify that even if you do all of the other mitigating factors that doesn't absolve you of the responsibility to encrypt or not encrypt.

And I think there's some opportunity there to clarify that to the marketplace because there are vendors, manufacturers and providers that are looking at that going "oh, I did a good enough risk assessment as part of my risk management plan and I have all these other things, I've chained it to a desk, I have a camera on it, behind badge access doors" and that's good enough, but it's actually not good enough. So, I'm just throwing it on the table as opportunity.

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Okay and just...

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

And this is Meg...

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

A final comment, we look at those case by case for enforcement, but, you know, we are...look for opportunities for some additional guidance in certain areas and we recognize that encryption in particular is an area which maybe, you know, ripe for some additional guidance and that is something that we have begun to review and, you know, maybe able to look at that a little more closely.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Thank you.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Michelle, this is Meg...

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

This is Michelle...

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

I know we're at time...yes, go ahead.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Sorry, yeah, I was just going to say that we need to go to public comment. So, operator can you please open the lines?

Public Comment

Lonnie Moore – Meetings Coordinator – Altarum Institute

If you are listening via your computer speakers you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. If you are on the telephone and would like to make a public comment, please press *1 at this time. Thank you.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

While we wait for folks to call in we do have a public comment from David Tao that was left in the chat and we'll send it via e-mail, but David Tao says, it is good to not have barriers to access, however, because the requirements for authentication, verification are open ended I hope the guidance clearly state the consequences if a CE has weak verification and releases information to the wrong person who might use it improperly and in harmful ways.

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

This is Nick and I'll just comment on that, I mean...

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

So, Nick, I'm sorry, we don't have time for comment.

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Oh, no comments, okay, all right.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

But you can certainly share that with the group after the fact. And it looks like we don't have any other

public comment, but we'll send out David Tao's comment and perhaps Nick you could share a response if you don't mind.

Nicholas Heesters, JD, CIPP – Health Information Privacy & Security Specialist – Office for Civil Rights, Health & Human Services

Okay, sure.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

All right. Thank you all, we appreciate your time. We especially appreciate OCR taking the time to speak with us today. And the next meeting is March 8th. So, thank you all and have a good day.

Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Thank you.

Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Thank you.

Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation

Thanks, everyone.

Public Comment Received During the Meeting

1. David Tao (ICSA Labs): It is good to not have barriers to access. However, because the requirements for authentication/verification are open ended, I hope the guidance will clearly state the consequences if a CE has weak verification and releases information to the wrong person, who might use it in improper and harmful ways.