

Health IT Joint Committee Collaboration

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



Health IT Joint Committee Collaboration Application Program Interface Task Force Final Transcript March 28, 2016

Presentation

Operator

All lines are now bridged.

Michelle Consolazio, MPA – Federal Advisory Committee Lead – 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 meeting of the Health IT Policy and Standards Committee's Joint 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 the roll. Josh Mandel?

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

Hi, Michelle.

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

Hey, Josh. Meg unfortunately isn't able to join us. Aaron Miri?

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

Good morning, Michelle.

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, Information Systems – Surescripts

David's here.

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

Hi, David. Drew Shiller?

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Good morning; here.

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

Hi, Drew. 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

Hey, Leslie. Linda Sanches? Rajiv Kumar? Richard Loomis? And we have Robert Jarrin back, right?

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

I am here, Michelle after a very long absence. Thank you very much for understanding.

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

Thank you for coming back. And from ONC do we have Rose-Marie and Lucia?

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

Lucia's here.

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

Hey, Lucia. And I believe Rose-Marie is on as well. So with that, I'm going to turn it over to you Josh.

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

All right, thanks Michelle. And thanks for those who are here, I know that this was one of the meetings that got added to our schedule relatively late, so I understand that not everybody was able to free up the time. But we've got a bunch of important issues to go through on today's call and a little bit of planning in terms of next steps.

So first of all, let me just see if I can get the screen share working on my side. I'm going to go share my screen and hopefully folks can see where I've got my browser opened to our shared document. Can someone confirm that's visible?

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

You're up and running.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It is.

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

Perfect. Thank you. So big picture, what we're hoping to do over the course of the next week is to freeze this document to the point where we're not going to be adding any more sections to it; we think we've got our content basically laid out. Of course there will be a few areas where we're going to continue making changes and tweaks, but what we would like to do is freeze it and say, the basic structure is in place, and that way people can really focus on any last comments or suggestions rather than sort of wholesale new additions.

So what I think that we'll do is Meg and I will confer offline and we'll get any sort of final tweaks in place and aim to freeze the document in the middle of the week, so by the end of the day on Wednesday and share out, again, just a link to the same document asking folks to take a look and review what's there and identify whether there's any sort of important high-level changes that need to happen. So that's our basic plan is we'll have it frozen by the end of this week and then have a week for review before our next call.

On this call I wanted to go through a few of the issues that were more around the technical and API and registration side. And then on the next call when we'll have Meg back, to focus on HIPAA and some of the regulatory issues, but that there's a couple I think that we'll touch on even today, and especially since we've got Leslie on the call, this would be a good opportunity to go through, I think, a couple of the outstanding issues where we need some clarity before we can really flesh out our recommendations.

So, what I'll propose to do is to take us through I think four areas, four topics in the document and just review what's there and get feedback from all of you. Before I do that, are there specific topics that folks on the line want to make sure that we can discuss on today's call? It's a small enough group that we should probably be able to zoom into particular areas of interest.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Hey Josh, this is David Yak.

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

Hi, David.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Hi; and, you know we may have covered this or it's in the document, you tell me but one category that seems to have popped up in my mind recently has been this concept of whether any sort of guidance or requirements that we may head towards can be superseded by commercial agreements or by license agreements.

Because there was a comment I think from the public period at the very end of the last call that alluded to the fact that these blacklisting I guess preventing someone from blacklisting may be in violation, or maybe I have it wrong, it's the other way around that blacklisting someone may be in violation of a commercial agreement. So, do we feel that we need to explore that area a little bit more to know whether we've got a concern about problems with jurisdiction and what's the controlling agreement on a particular item?

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

So I think it's a good question and we've got some folks who can help us with the legal review, in terms of support on the ONC side. So it's an area where as we're starting to formulate...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

If you have a legal use thing, I just wonder if we have to be aware of that and ensure that we're not, you know saying something that we can't say; you know what I mean?

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

Sure. So I think as we have our recommendations better in shape, it'll be easier for us to get that kind of review and anything that we're stating as a recommendation saying, here's how we think the world works or should work, will be a much clearer target for that kind of analysis. So I think we're getting to the point where we can ask those questions.

You know when it comes specifically to this issue of blacklisting I think, you know, one thing that I think we might do is try to avoid the term blacklisting; and I don't know that the term itself is very helpful. We can try to flesh out this idea of exactly what the responsibilities and the rights of a healthcare provider organization are when it comes to letting these Apps communicate, you know. Frankly...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yeah.

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

...I think we'll be elucidating a lot of what it means for the patients to have certain rights under HIPAA. Of course HIPAA's not the only regulation in effect and sometimes that there are various competing motivations that are at play here. So I think that you're right, it's something where we can do a better job of describing where there may be competing concerns.

And there was one call; I guess it was the public comment at the end of our last call which brought up another related point which I think we can get to when we go back over that sort of blacklisting section. So let me add that to our queue as well. Are there other iss...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Okay, thanks.

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

...sure thing, thanks David. Are there other issues that people want to make sure we can bring up on today's call? Well, I'm sure things will come up as we go and so don't hesitate to shout out as they do and I'll also pause at other points and see what else is on folks plates?

So what I would like to do then is to start with what's on the screen right now, which is a short section where we took some of the work that had been put together around different types of applications, so this was originally Leslie and Aaron M. who had worked on a list of types of applications. And so we took a set of different types of applications and incorporated them back into our sort of variations on the App scenario, so, you know, we had a list of various kinds of organizations who could be writing these Apps and purposes for which the Apps could be written.

But we wanted to focus here in this section about...on the topic, particularly on the recommendation that at the end of the day, we think that ONC and CMS should make it explicit. I think they do a

reasonable job here, but it's not totally explicit that the type of App and the kind of organization who developed it are not considerations when it comes to patient access and that the relevant things are just technical compatibility, making sure that the App is in compliance with the way the API works on a technical level and patient choice, so giving patients and consumers the ability to pick the things they want.

We recognize that there are lots of different kinds of Apps that are written by lots of different people for lots of different reasons and it's important and useful to think about them. But at the end of the day, when it comes to recommendations on that front, this seems to me like the main and perhaps the only thing that we wanted to say about different types of applications. So let me see, am I missing something? Are there other kinds of recommendations that we feel like we should be making when it comes to the variety of different sorts of Apps that could be written for this ecosystem? Fair enough...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Josh, this is Leslie; I just think right now we're thinking of the relationships between a patient and a provider; I think the Apps will evolve to be the patients and multiple providers. I don't know if we need to explicitly state that, but it does add a little bit of complexity where the relationship might be primary with one provider, but secondary and tertiary with many other providers, if that's...I don't think it changes this supposition; it just makes for a more complex environment to be considered.

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

Yeah, I agree with you and, you know, I think ultimately what we're doing is we're providing a building block where you can connect, you know, one patient App to one provider. But of course if you have that building block then an App can start to bridge across systems and build new interesting things. Yeah, at the end of the day it's not clear to me that we need to call that out, but if there is specific language that you think would be...that would be useful there, umm you know I certainly wouldn't object to including it.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Uh this is Drew Schiller; I just want to make sure that we're not limiting the scope by calling this out. I don't think we are but, I mean one of the beauties of...beautiful things about technology and APIs is that we probably can't imagine some of the things that will be built on top of...technology.

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

Yes, I agree with that point and I'm over and over again impressed by the new and interesting ways that people find to combine some existing capabilities along with some new technology. So I think this is okay; if folks come up with other additions to this section, you know by all means feel free to share. I just wanted to make sure that we had reviewed this as a group together and that folks had at least seen what's there right now, and of course we can always come back to it.

A couple of meatier topics that I wanted to dig into; one is the topic of dynamic registration. And I know it's hard to do with a small group, but I thought we could at least review what's there today, so that folks are oriented to it. And what I've done with this section, which is...the topic is, registration process including dynamic registration and self-service registration, is first trying to define a couple of terms. You know, what do we mean by registration in the first place and try to understand what ONC has said about the registration process in the existing regulations.

So, I'm going to go through this in a little bit of detail, just because I don't know a better way to summarize some of this. You know, the bottom line is that registration is a term that has to do with introducing an App to an API provider and allowing the API provider to record some details about that App; so things like what is the App called? What website does it live at? Who was the name of the contact person, you know, responsible for this deployment of the App? And, you know maybe a list of other folks who are responsible for helping to host this application.

So registration is all about introducing the API provider to those details, and in some protocols like OAuth 2.0 as a prime example, registration is this technical requirement. The App needs to have been registered before it can ask for permission to access data; that's just...that's how the technical protocols work and there's no good or widespread way around that.

And so when registration is a technical requirement, you know just because it needs to happen doesn't mean that it's a policy barrier. It doesn't mean that it's a place where an API provider should come in and start to impose lots of requirements, but there has to be a process for it to work, because the App needs this registration process in order to proceed with even asking for access. So the bottom line here is, the key point that I thought was relevant was this notion of a fast and easy and frictionless registration process.

And I think that there's two ways this happens in the consumer App world today. One, which is pretty common, is a self-service registration portal. So this is like when Google hosts a developer website where developers can log in and create a new App. Typically the registration process itself is automatic in the sense that there's no delay. There's not like a person sitting down and reviewing it and checking up on lots of details. The developer fills out a form. They might actually offer some proof, like they might prove to Google, for example, that they own a specific domain by hosting a file of that domain or by setting up a DNS record or receipting an e-mail to an administrator; something that proves ownership. But there's not typically a manual review process in these consumer web deployments.

And it's important to say that just because you've registered an App, just because you've completed that registration process doesn't mean you have access to any user data at this point; all you can do is ask the user for access. So the App approval, you know really is still contingent on that patient approving anything before data flows. So, no matter how you do it, registration itself is sort of a low risk activity in a sense that you're not immediately allowing data to flow, just because that occurs. So that's sort of the self-service portal way that developers can sign into a site and fill out a form and create an application.

And the other pattern that we see is called dynamic registration, and that's an API. The API provider hosts this registration end point and an App can, in a fully automated way, send a message to that end point saying, please create a new client for me. And so for example the OAuth dynamic client registration protocol is an example that does this kind of thing. And the whole thing can be automated end-to-end and developers don't have to sign into a website and fill in any forms manually. And again, there's no waiting period. And again it has this property of a low risk activity because the mere act of registering an App doesn't actually cause data to flow.

So, it's certainly possible for an API provider to do one or both of these things together. You can have a self-serve registration portal and a dynamic registration end point, and that can be pretty convenient because, you know some developers have a workflow that works better with one of those scenarios than the other. This is all just sort of background, trying to define terms and describe what we've seen out in the world.

And then the last piece of background is me bringing together a couple of statements that ONC has made in the 2015 EHR Certification. I guess the most important one is they said, our intention is to encourage dynamic registration and I guess we strongly believe that registration shouldn't be used as means to block information sharing by APIs.

So they wrote that, but then at the end of the day, they didn't actually require dynamic registration. Instead they said, "From the comments received it was clear that our intention was not understood and furthermore, open source standards for dynamic registration are still under active development and there's no consensus-based standard that we could apply." So that's sort of what went into the process.

And then later on, still in the same certification criteria ONC said the following. They said, a health IT...when they were sort of justifying why there was no dynamic registration protocol in place, they said, "A health IT module that's certified to our criteria needs to be able to ensure that user credentials are valid and that the provider can authorize the user and application connects through a trusted connection, and these certification requirements together should be sufficient to allow access without requiring further application and preregistration."

So I sort of added the emphasis to the end of this sentence here because I couldn't understand what ONC was driving at with this particular claim. It seems like they're writing that, umm, if an API provider does all the things they ask that registration shouldn't even be necessary, that you should be able to run Apps against a system without registering them at all, and that seems...to me that doesn't seem quite true. You know, depending on what authorization protocol you use, sometimes registration is just a technical requirement and you can't get around it, at least I don't see how you could. So I wanted to highlight that under finding, as something that we've seen that we don't necessarily know how to make sense of yet. So before I move on...

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Josh?

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

Yeah, please go ahead.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Yeah, this is Drew Schiller. I totally agree with you there, I think that from a technology perspective it does not make a lot of sense. I think that a simple registration would benefit all parties and it would not be cumbersome and it's...plus it's pretty much what you would expect in an OAuth type of a situation. So, I'm in agreement with you that that's a good call out.

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

Yeah, and at the end of the day, you know I don't think that it's our job necessarily to sort of recommend that everybody in the world uses OAuth, but I think we can point to it as one best practice that the industry has converged on and certainly the regulatory thinking should allow for that. And I'm not...it's not clear to me that, you know, this highlighted portion on the screen here actually does allow for it, so I wanted to call it out.

Before I get on to sort of what I want to recommend, you know what I think that we as a group have been discussing here as recommendations, let me just pause and see if the background that I just

provided is clear enough or if I've said things that are confusing or controversial because background should not be confusing or controversial.

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

Yeah, so Josh this is Aaron Miri; I agree with you. I think also, this goes back to why I'm big on definition. It may be worth asking ONC to define registration for us, what do they term registration to mean? Because I agree, technically you can't do this without technically registering something so that the data bit knows where to traverse to. But I think, I wonder if they're trying to come at it from continue to promote a free market and their concern that this may limit innovation in some way; but we may be speaking apples and oranges.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And this is Leslie, I agree with that. I also think that it's worth noting that if we're bringing in patients for the first time in this new ecosystem, recommendations should be consistent with the consumer App world and not restricting it through an artificial imposition against something like OAuth 2.0, which is prevalent in the industry.

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

Yeah, and for what it's worth, I don't think the ONC is saying anything that would prohibit something like OAuth from being used, it's just they seem to be saying that they don't think it's necessary and that you should be able to get by without registration and that's the part that I find confusing.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Hi, this is David Yak. There's something else that came up near the end of the last session that I think...and I don't know if it's...I don't know directly related to this, but let me just raise it because it...I think it's something we have to consider, which is this question of whether users are individually registering for access or whether it's the application that's registering.

And the reason it came up was that some of the permissions or access control or "blacklisting" is sort of determined by the application level, not on a user by user basis. So I think yes, defining registration would be really valuable because I think we're maybe getting words mixed up here about an application registering, and does that only need to happen once and then there's a user registration or handshake that needs to occur? Or are we talking just about user by user and every time there has to be an application "registration" that's happening for each and every user or how's that...what's that hierarchy of relationship between applications and users, as far as registration goes?

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

Yeah, so, and let me just say sort of from my perspective on this one, um, there's a lot of technology and some of it's moving pretty quickly. So three years ago the answer was more or less, you know you register the App once and all the users just use it. And today there are more middle ground solutions that feel sort of like, well, you register the App a little bit just once but then each user registers their own copy of it a little bit, and dynamic registration APIs can allow you to actually, you know subdivide the registration process like that. And you get some interesting security properties and guarantees that way, you know, but ultimately this is getting pretty detailed and perhaps too detailed for our purview.

One thing I think we could say is, at the end of the day it's a user making a decision about what Apps they want to use and so what that means is, at the end of the day the users need to have the ability to say like, yes I want this App or no I don't; and just because a different user says no, I should still be able

to say yes. And if we have this kind of ecosystem where Apps can dynamically register or can register in a very low friction process, then at least as a last resort an individual user can register a copy of the App themselves. I don't think we need to say that's how it should work or that's how it does work, but at the end of the day, that's always possible. And so if we want to think about it from sort of a systems design perspective, we know that a user sort of can have that level of control if they need to.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

And I guess ultimately that's what we want to ensure so we should probably keep that fairly general, which is to say the user has the ability to determine which applications they want to consider for registration with the data source and then how that...I think we should stay away from how that's happening behind the scenes. Leave it at the user level and if that means an App-to-App registration or qualification that needs to occur, because there may need to be some testing or some, even light certification by the data source of the Application.

I think at some point you can't just assume that this stuff all plugs and plays and that somebody's going to want to qualify the App that yeah, it works and it generally, you know delivers the data that it's intended to deliver. But then the user has control over whether they have access or not.

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

Yeah, I think I would say it a little bit differently. I mean, I think it's the users decision about whether they want to use an App or not, and if registration is a prerequisite for that, umm, then either the App has to be registered ahead of time or the user has to be able to register it themselves. In the real world, most users are not going to sit there and register Apps, it'll be a pretty poor user experience; it's more, I think it's more of a safety valve.

So I think we have to say the App can register in a low friction process and most of the time it's probably the App developer who takes care of that for you. But in the worst case, it's something the user could do themselves. But in terms of what's really the important characteristic is that users can say, yes, I approve this App, and...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yeah, I agree with that. I agree with that.

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

...if they have to register it to get to that point, well so be it, but most of the time they, you know that should be taken care of for them.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Well, and it's kind of like this question again of, what's registration, right? If this is just a user through their consent process saying, I want data from this App, and they check some kind of box or they say yes, is that a registration or is that just a, give me my data step and registration already had occurred. I think to a user that's not a distinction with value.

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

I agree with that; to a user the distinction with value thing, like yes I approve this thing and registration is really about setting up this thing so that the API provider actually knows how to ask the user whether they want to approve it. In other words, before I can say yes I approve this thing, you know, my doctor's office has to know enough about this thing to be able to show me the screen for approval.

And that's...so I'm trying to use these words in a way that lines up as well as possible with the security standards, so that's why I'm making this distinction between the authorization process and the registration process because for folks who are thinking about it from the technology perspective, that's a distinction that's there. It's possible that that's not serving us well here, I, you know I'd certainly appreciate feedback if folks think that that is...if this is getting in our way.

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

I...this is Aaron Miri; I think it's appropriate use of the word. I think we just need to define it and I think that will put a lot of worries to ease because I think, I truly think we're talking about the same thing; I think folks are just misinterpreting it.

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

And so I've attempted to write, well maybe definition is too strong, but tell me why you think, you know this first paragraph here where I talk about registration, is this getting at a definition in a way that's helpful to you or do you think we need to make this more rigorous and do you have ideas about how we could make it more rigorous?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I think it's indicating that this is a technical...we're using the term registration aligned with security and privacy framework and this is a technical registration process term versus just, cuz I think if you read the first paragraph that's written, you don't know that it's just simply a technical registry...registration that's happening.

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

Hey Josh, this is Lucia. I, you know I try to be really quiet but I think Leslie's on to something. I think the key thing is both of it's this and not that; so not only is it two systems technically recognizing each other, but it's not intended to be about business choices and policies or whatever the right language is, right? It's this but it's not that sometimes helps people really wrap their heads around a definition.

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

So thank you, Leslie and Lucia. I've just tacked on a little bit to the end here to say we're using the term registration in a technical sense and it's not intended to represent business choices and policies, at least, you know as a place holder. Is that sort of triangulating the position well enough, in terms of what we are and are not describing?

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

I think it's headed in the right direction.

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

Okay.

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

It'll probably get some tweaking over time...this is Lucia; that's sort of you guys will ruminate on it and come up with something better, I'm sure.

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

Yeah, fair enough and so I'll just sort of highlight this and say, can we clarify this further? At least that'll remind us to take another look at that; so, fair enough.

But let me briefly then outline sort of the recommendations in this section, at least as I saw them, which were relatively straightforward; at least I hope so. The first thing I said is ONC should clarify that, you know, the App registration itself is not...is, you know must not impose an unreasonable barrier to patient choice. And so in scenarios where client registration is a technical requirement, it should be frictionless and it should not impose any delays and it's not intended to be a point where Apps undergo rigorous testing or clearinghouse approvals or on-site inspection or other kinds of high bars of control.

And instead ONC should say that self-service registration portals and dynamic registration protocols are two complimentary ways that Apps can have a frictionless registration process. And that in future rulemaking ONC should require both of these, since they can address different developer needs and if you already have a dynamic registration protocol, it's very easy to build a portal, a registration portal on top of that protocol. So that was sort of block one of recommendations about where to go.

Two was, I thought it would make sense for ONC to sort of retract this claim that the existing certification criteria are sufficient to allow access without further preregistration, because I don't...I think it's out of line with real world authorization protocols that we know about. Or if it is inline, it requires more justification, and I don't know what that would be.

And then finally I think ONC should develop guidelines describing when and how API providers can charge for registration of patient-facing Apps. And, you know at a minimum, maybe API providers need to say, publically disclose any registration or pricing information. And I guess I should add on to this the fact that it's a patient doing the registration themselves, there can't be a charge; and maybe that...maybe that's an important point to note. So let me just pause and see if these recommendations make sense and if we're missing something that we should have captured here.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So I'm confused a little bit Josh because you're saying if the patient is registering an App themselves there's no fee. We're assuming that the patient is the one controlling any App that's attached to it. So, and again we're saying that the registry is a technical provision and not a policy and a business term; are we getting now into policy and business terms? And it's really not the registration's function that we're saying there shouldn't be fees for, or is it? Umm, I'm con...I'm a little bit confused by this.

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

Yeah, so I think that's fair and I think it's a thorny issue and I don't know that I have the answer here. So here's the basic question, you know if I'm a healthcare provider organization or maybe even EHR vendor and, you know a patient wants to write their own App that's going to run, you know, like there's just going to be one or two or three copies of this App in the whole world and it's going to help the patient, you know track their lab results over time, it seems clear to me that that's like patient access and that I can't charge them for it, umm, but...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay, I see, so maybe clarifying that to just, and if a patient is an App developer, self-App developer and registering its App directly, there cannot be a fee.

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

Yeah, but there's, I mean, there's just this incredible gray area here, right? I mean, so what happens when the patient writes the App for themselves and then, you know, they share a copy with somebody else. You know, if they share it in a way that says, well I'll host this for you and then a million people can use my hosted copy, is that different than saying, well I'll just distribute this and let a million people install their own copies and each of the million people can register it themselves? It becomes very gray very quickly.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It does.

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

So I'm trying to figure out like, are there some principles here that we could at least highlight, even amid all the gray?

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

So Josh are we inheriting some concepts about not being allowed to charge for information that maybe we should just avoid because if it's covered somewhere else, because we are infringing, again this is that point about commercial agreements and if a provider has this super-duper amazing data analytics that they did and they want to charge fifty-cents or a dollar for someone to access as a value-added service, is that something that we at this point want to prevent or, like are we getting out of bounds by getting into the commercial side of things here?

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

Oh so certainly, you know, I want to make sure I understood the example you just gave. But if an App you know, builds some analysis that has value and they want to charge patients for it, that seems entirely fine, I don't think anybody is objecting to that concept.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Oh no, no, this is on the other side, this is on the data provision side. So if somebody wants to do a super-duper data integration from 12 different providers and then be the channel to provide that integrated information to an App and they want to charge the user extra for that particular feature, is that already outlawed through other regulations that someone cannot charge for the patients access to data?

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

No, I mean if that somebody, for example, in what you just described it doesn't sound like that would even be a HIPAA covered entity necessarily. It sounds okay...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Potentially that's right, it could be an integrator, so what are we saying then about not being permitted to charge or not...

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

So the principle that I was trying to get at here is, if I'm a patient and I write my own App, I should be able to connect it to the system without having to pay; that's sort of one piece at least. And then what I was trying to figure out is whether and how that generalizes.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Oooh, I think this is a super slippery slope and I'm not sure why we would make the comment about a fee not being permissible in any case, never mind if the patient is the one who "writes the App."

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

Well, so we said that a patient can only be ch...so first of all, we're talking about like in the realm of HIPAA here.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Mm-hmm.

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

The fees that a patient could be charged to access their data can only be sort of the reasonable fees that cover the actual cost to the provider of sharing it that way.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Right, photocopying and things like that and...

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

Those kinds of things, the incremental costs; so that's sort of the realm that we're working in here and so the principle here that I was trying to get at is, if I build an App for myself and the provider says, well before you can use your App in our system you have to go through this registration process, you know, the registration process shouldn't be contributing to that cost. I mean if there's an incremental cost to accessing my data, that's fine, you know, charge me the 0.0003 cents that it costs when I want to issue an API call, if you really want to, but just to get to the stage where I can actually click the button to request my data, I shouldn't have to pay, or at least I shouldn't have to pay any more than the actual incremental cost.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Well maybe...there should not be a fee or cannot be a fee for the registration process itself.

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

Say that again?

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Maybe we should say that there either cannot or should not be a fee for the registration process itself.

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

Because the flip side is that we have seen...this is Aaron Miri. The flip side is that we have seen in the marketplace, especially as a provider CIO, where certain vendors out there will charge exorbitant fees for connection fees and it prohibits the little guy from being able to do anything.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Right.

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

And so I could see that same philosophy playing out, especially with some of the bigger players saying, I'm going to squeeze the little guy out because I'm only going to cater to the big players and it's going to

cost you, I'm making this up, \$10.00 a transaction, no matter what you do. And that would totally preclude any small person from being able to leverage that appropriately and thus, is a form of information blocking, which is very prevalent in the HIT community.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

(Indiscernible)

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

So I can totally appreciate where Josh is coming from.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

But Aaron, does the HIPAA Rule already take care of this, which is to ensure that there cannot be charges for access to information, whether it's paper, electronic or now API, over and above what are considered to be acceptable costs?

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

Umm, I think we ought to defer to the experts on the phone for that, but, I do know that what I see often, and this is in real world is that it's a business fee, not necessarily a fee to collect patient data. And so folks will coin it different terminology to get around the law or the rule as written by saying this is a form of business and therefore you can't govern how I do my business, therefore it costs you, again I'm making this up, \$10.00 a transaction or whatever it be. Just to give you an example, just to transmit claims to a payer costs me dollars.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yup.

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

I mean, I'm actually spending money to electronically transmit a claim to payers so I can get reimbursed for procedures and this is to eliminate error and issuance when we were doing paper...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yes.

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

...many years ago. So everything is charged now a days.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yup, no I'm with you. I just want to know whether we're overstepping our bounds and whether this is already covered under other rules. I agree there should be no incremental costs associated with this, but I don't know if we necessarily need to...how far do we have to go into...are there things that we are not already covered for in terms of this issue of no charge?

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

Yeah, so David, I think this is what I heard you say, see if I've...this right, but ONC should clarify the API providers must not charge a fee for the App registration process itself, but as always under HIPAA, reasonable charges may be applied for access to the data.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Yes.

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

But that this shouldn't be applied to the registration process before they start...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

I agree with that as long as reasonable charges are both defined somewhere and covers APIs, I'm perfect with that.

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

Yup.

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

So...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

You know I...this is Les, and I struggle with this because of the...it is the patients data. I agree with the registration function that there shouldn't...it shouldn't apply that it could become a form of blocking for the little guy, as Aaron pointed out. And perhaps the HIPAA reasonable charges are where this lands, but it is difficult to articulate to a patient why they should pay for their own data.

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

I...this is Aaron, I completely agree. The patient should have absolute access to everything they want to know about their own data themselves. Unfortunately we all live in the HIT landscape that we do and all these other market forces are at play and everybody's commoditizing and monetizing everything and it's a sad, sad situation. I totally agree with you, Leslie.

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

Yeah, I mean...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So perhaps it's the fee...the UR, we'll really assume there's some sort of commercial relationship between the patient and the App provider, whether that's a free relationship or whether it's a pay for services relationship. And so the payment of...to the App developer is a...is within the patient's control to say yes or no, and I will pay for that App. And then say, no, we can't charge for registration, which is agreed upon, I wonder why there needs to be any sort of fee for data access, because...

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

So to be clear, we're not saying that there needs to be a fee...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Right.

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

We're just...I'm sorry, go ahead.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I just think that the relationship that the patient has the ability to say no to is the one for the commercial relationship with the App provider and then when going to the provider itself with the App connected to the API, it...do we want to say that reasonable charges are, in fact, appropriate? That charges at all are appropriate? Is that within our purview?

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

Well I...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Because if our purview says that registration should not include charges, but the other...maybe you're right that they could apply reasonable charges, but I don't think a provider should charge a patient for access to their own data.

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

But...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And today, for view, download and transmit they don't have that ability.

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

Oh don't they? That's an interesting point. I wonder, if a provider wanted to say, to click the download button you need to pay us 0.000003 cents, because that's our incremental cost; I mean I suppose they could.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But for instance the cost face-to-face to bring it down, Wisconsin Health Information Network did a study and said that it cost five dollars per page to do...to go to the medical records department and get that record; it's much cheaper online to provide those services. So, I don't know whether we should be silent in this or ask for clarification, but it seems to me that if we're not charging on VDT, we shouldn't be able to recommend charges on an API App relationship.

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

Yeah, so I mean one thing that we could say is that we could recommend that ONC clarify that reasonable charges in this context are exceptionally...are vanishingly low, you know, even to the point where it wouldn't...where the...where levying the fee might cost more than you would actually collect.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Bingo, yup.

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

But...

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

There you go, I like that. I like that.

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

If only I could spell the word levying, that would be a real coup. But at the end of the day, you know, this is just something that HIPAA allows and we can't change it, you know all we can do is point out the practical consequences in the electronic world.

And, you know, if you look up what various API and hosting infrastructure services charge for this kind of thing, it's pennies per gigabyte and health data are, you know on the order of megabytes, so we're talking about on the order of a very small fraction of a penny; that would be sort of the reasonable charge. And yeah, try actually doing that, try making somebody sign up with their credit card to do that, I think people will start to look at that as information blocking if I have to sign up with my credit card to pay the penny to access my data; it's an interesting world.

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

Unfortunately I can see it definitely happening, it's sad.

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

So, are we reasonably happy with where this landed then, which is to say, you know registration shouldn't have a fee; of course access to data could have a fee, but it would be a very, very, very tiny fee.

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

So Josh, this is Lucia. The only thing I would say about that, and I've sort of been holding my tongue, is we can actually go back and look at your draft, and I know Linda Sanches isn't on today, but she can validate for us whether things you have put down in your draft are consistent or slightly off of people's existing authorities and where the rules are. So for example this is one of those areas where OCR has been very clear that fees are for the actual process of photocopying and the medium of the copy process, not for search and retrieval. So we would have to make sure that this, at the end of the day, whatever happens with this paragraph reconciles with guidance OCR has already published.

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

Sure, I think we would very much benefit from that kind of analysis and at the end of the day, if there are areas that you already know, Lucia, are standing out as potentially in conflict, you know, by all means let us know what they are.

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

I haven't yet, but I'm mostly letting you guys talk and get where you need to go and then we'll sort of give you any input we need to, but I think you guys are doing a great job.

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

Cool. All right, fair enough.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

This is Drew Schiller. I've been sort of holding my tongue as well; a very fascinating discussion to hear the different sides. From a, just to...and I know Josh, I think that this is where you were coming from originally, from a technology perspective, this should be something that is set up once and then able to, through the technology, deliver the service over and over and over again with no human intervention;

so the incremental cost should be nil. There should be no incremental cost for delivering an API outside of maybe supporting a server.

So, I think that that should be something that is considered by all parties when the fees are considered is, what are we actually doing for the fees, because it's not like when a request comes in, someone manually approves it and then the API data goes out. It's much more likely that the request comes in, the data goes out, a human never actually even sees it.

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

So I totally agree with your description of the incremental cost; I don't think they're quite zero though, I mean, like let's say I have a server that's doing all this stuff automatically, but I'm still paying my, you know let's say it's running on AWS. I'm still paying AWS some fraction of a penny per gigabyte of data that I transmit, so there is an incremental cost, it's just incredibly low.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

That's, yes, fair, and...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And much less than the manual alternative.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Yes.

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

And I think in practical terms it's so low that it wouldn't make sense to try to recoup it.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Yes, exactly.

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

All right, are there other comments on this topic before we move on to talk about limitations on sharing? All right, let me switch over to the limitations and safeguards. This is one where we spent a bunch of time last week, but there's one area which I think we didn't talk about and for some reason, my link is broken. Let me just fast forward to this point in the document, okay.

So the first thing that I wanted to talk about on limitations, which we didn't talk about last week is this question of when a patient is approving an App, do they have the ability to say something more fine grained than, share all of my data? And, you know, one thing that we've certainly seen is that while you could come up with lots of use cases for fine grained access, and there's lots of places where they would be sort of nice to have, it's also a huge challenge to implement that consistently and correctly in the real world. And, you know, depending on what your EHR system looks like and how you store your data and whether and how deeply you've annotated those data and how much metadata you have, it could be very difficult to be able to support that.

And so the question is, is there some sort of reasonable middle ground where we can allow some degree of fine grained sharing without going crazy, without going overboard? And so the place that we had come to in previous discussion, which I've just tried to write up a little bit more formally here umm is that, I think yes; patient's should have the right to say something a little bit more fine grained and in

particular what they should be able to do is share at the level of data categories, because the certification criteria today already have this notion of APIs at the data category level.

So an App has the ability to say, get me the patient's meds or get me the patient's allergies or get me the patient's immunizations. The data are already divided up by those categories, so I thought it would make sense to allow the patient to approve access at those categories as well, since we know that every certified system is already capable of dividing the data along those lines, so we wouldn't be asking them to go and implement some fine grained leveled access that they might or might not be able to cover, they would have to be able to cover it because they already know how to respond to an API call for just allergies or just immunizations.

So I tried to write that up here, and I'm going to...I got a few comments on this which indicated that perhaps I haven't written it up clearly enough. So I'm just going to read this paragraph and hopefully figure out number one, whether these ideas make sense and if they do, whether we can adjust the wording to make them clearer.

So what I've said here is ONC should update the EHR certification criter...requirements to ensure that API providers enable patients to share data with certain coarse grained, for now, limits rather than all or nothing. Under the updated program, or under the updated requirements let me say, patients should be able to list which Apps currently have access to their records, revoke access at any time and make sharing decisions that restrict the scope of access. While we believe in the value of fine grained permissions, we also recognize that implementing many narrowly scoped access control policies would require costly and difficult redesign of existing systems.

Therefore, in the near term we propose a pragmatic approach that ties back to the capabilities described in the 2015 EHR certification criteria. Since EHRs must already enable access through separate API calls at the data category level, for example medications, vital signs or lab results, ONC should ensure that patients can approve access at this same level. In other words, the pragmatic approach is for ONC to require that certified EHRs enable patients to share data with Apps at the category level.

So let me pause and see if that made any sense and if there's areas where it could be clearer. It's a small enough group that I can pick on people by name.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So Josh, it's Les; a patient should be able to list which Apps currently have access; list generated by whom and to whom?

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

Ahh, so this would be generated by the portal, by the EHR provider.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay.

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

And for the patient to see, so like...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay.

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

...online in the portal where they would approve an App, they can also get a list of outstanding Apps that they have approved.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay, so maybe we should just clarify that, it looks like they're writing down a list somewhere which Apps they currently have access to versus...

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

Uh huh, yeah, of course, of course, of course...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, right.

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

...should be able to view a provider-generated list of Apps that currently have access to their records.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Hey Josh, this is Drew; I have a question that may be a total red herring, I don't know. I have a question that this paragraph really made me think of more than the others. Is it our intent to explicitly say that EHRs are the sole provider of these APIs? Is it possible that a third-party service could come in and provide API access for a provider that is not an EHR?

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

Yeah, so it's not our intent to use the word EHRs, it's really the...what's the right name for the certification criteria? It's the certified electronic health record technology, right, that's the term.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Okay.

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

And in general, the certification program is modular, so you can have a vendor that basically just does a patient portal and API access and they can get certified for these criteria independent of, you know the big transactional EHR system. They would need to be able to work with those big transactional EHR systems in a real world deployment, but at the end of the day we're talking about whatever product it is that provides the API.

Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Gotcha. Okay.

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

And we'll update these acronyms to match the appropriate language, whatever it is. I think CEHRT, is that current? I don't know, we'll get it right.

Robert Jarrin, JD – Senior Director, Government Affairs Qualcomm Incorporated

Yes, that is current.

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

Okay. Other comments about this general notion that it makes sense to allow patients to approve access at the category level, given that Apps already are able to make requests at the category level?

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

This is Aaron Miri, I think it's a phenomenal point, Josh, I totally agree with it and, you know, as evidenced by the fact that you're now seeing information from genetic testing now being used to deny people life insurance, and that wasn't the intent of the patient as they were looking for a predisposition to cancer or some sort of thing. I think it's important because there's going to be some information we want health IT information to flow, but if you know that insurance companies or whatever else is going to take this data and run with it, you're going to want that fine grain of access as a consumer. So, I think it's important that we note this.

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

Okay and I...we don't have Aaron Seib on the phone, so I'll try to check with him separately, but he was concerned that this is a slippery slope down to extremely fine grained access, and my goal was to be really explicit and say, we're not going to have a slippery slope, we're going to just align the sharing decisions with the requirements that already exist today for category level access. But I want to make sure that he's satisfied that we won't slip down this slope; I hope that what's here will be convincing, but I'll make sure to check with him on this.

Umm, this was also the section that we talked about last week when we had our blacklisting discussion, in fact, just in this previous paragraph here. And there was one point that I thought we should come back to and that David Yak raised earlier here which is, this question about, you know, what happens if there's other commercial agreements or license agreements in place that sort of have an impact on this blacklisting decision. And there was a comment that was made through the public comment process last week pointing out that we had language in here about terms of service and violation of the provider's terms of service might be a reason to blacklist or suspend the App.

And as we had described it last week, we said patients should be able to override that, and someone pointed out it doesn't make sense to allow patients to override a violation of the terms of service of the provider, which does seem true. So I've updated it to say, a patient should be able to override a suspension in the case where it's really just the provider trying to protect the patient. But if it's...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

(Indiscernible)

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

...the provider trying to protect their own system or if the App had violated a terms of service, it's not up to the patient to be able to make that call.

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

So Josh, this is David Yak again. So this implies that there is some sort of a contractual relationship between the provider and the application provider, because then there would be terms of service that could or could not be violated or come into play. But aren't we talking about a lot of use cases here where there is no commercial or business relationship or contractual relationship between the provider and the App provider such that a patient can request access and then a provider has no over...no...there is no overriding agreement that could come into play.

So shouldn't we, I mean first of all, is that going to be the case? I believe so; let's confirm that. But then are we really only talking about a minority of situations where there is a relationship between the provider and the App provider that has terms of service that...I think this is a difficult question as to whether a consum...a patient can override a business relationship that exists between a provider and an application provider. So first of all, are we talking about that being the minority of cases? In most cases is there going to be a business relationship between the provider and the application service provider?

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

So, that's a good question and one way I can frame it is to say, during that registration step, is the App developer or is the App provider somehow agreeing to a set of terms of service? And if so, you know, could those terms of service be literally anything or could it only...

David Yakimischak, MBA – Senior Vice President, Information Systems – Surescripts

Right.

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

...make certain kinds of restrictions? So, for example, it seems totally reasonable for a provider to request that an App only issue data requests at a certain rate, right? You know, please don't issue 1000 calls per second, because that will overload our server and, you know, if you want to register your App with my system, you have to agree to those terms. That kind of thing seems totally reasonable. And then, of course, you could ask for other things that would be quite unreasonable.

And so there's a question in my mind of, you know, how do we construe these terms of service? If they do apply, how do we ensure that they are limited to the sort of reasonable things they might expect an App to do without imposing, you know, further limitations on how the App could work.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

Josh, this is Ivor; this is just really minor and not related to sort of the bigger discussion, but the term blacklist, you might want to reconsider that...

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

Yeah.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

...maybe we say block or something like that.

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

Yeah, I'm just going to do this, and thank you for reminding me, I've been meaning to remove that word because it's...I think it's controversial and unhelpful. We've already used this term suspend API access and I think that conveys everything that we actually mean. Is that...

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

All right.

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

...does that work for you? Umm, so that's fair. There's still this issue of the terms of service and, you know, when can there be terms of service and what can they say? And frankly, I don't know how to resolve this.

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

Josh, this is Lucia; it is okay for you guys to pose questions that need resolution like what...where do terms of service between the App and the provider end and HIPAA begins might be a question you want clarification on, and that is perfectly okay to say, we identified something that might be a barrier and we need more information about how it works.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

This is Ivor; can I...I missed, I apologize that I missed the conversation last time with relationship to this. Are we talking about things with malicious intent or things that perhaps have been breached and then need to be blocked? Up higher in that paragraph, blacklisted is up there for suspicious acts...

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

Yes, thank you.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

...as well...so, are we talking about it in terms of something that's malicious or are we talking about something that, umm, perhaps had been breached in some way or are we talking about both?

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

So, what we're talking about is both Apps that might have been written with malicious intent or Apps that perhaps were previously good and now have been hacked. And the basic question is, you know to what extent are providers obligated to pay attention to this stuff to protect the patient? You know, if a patient has said, share my data with this App, and then the App gets hacked.

The folks in this task force seemed pretty...everybody felt like providers need to have some protection in that scenario, it can't be their fault if the patient-designated App then gets hacked. If we tell providers that they're supposed to be on the lookout for this stuff, they'll be very hesitant to ever allow access to anything. So it seemed clear that providers can't be obligated to do that.

And then the question became, well what if a provider wants to do some of that anyway, you know, what if they want to protect the patient and they protect the patient too aggressively and they suspend all the Apps all the time because they, you know are worried that there could be a 0.03% risk that the App has been hacked and that goes over their threshold of 0.02%, you know and the patients get annoyed because there Apps are being turned off all the time. You know, how do we sort of strike that balance?

That was basically the discussion that we had last week and where we landed was, if the...so first of all, the providers not obligated to protect the patient, but if they want to protect the patient by suspending Apps, they need to do it in a way where the patient can say, you know, thanks anyway but just from now on, leave my access enabled. I don't want this help from you anymore.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

Got it. Thank you.

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

Hey Josh, this is Aaron; I have a quick question, and this just came to mind. Do we need to also go into detail about this specific section, where we say suspension or blacklisting, can we also somehow work in the concept of throttling? In talking to some folks recently I've been hearing about various vendors throttling data flow to other vendors and slowing that down, therefore it's not as adopted mechanism and that's a way of...it's a new way of information blocking that's starting to occur now in the marketplace. So I don't know if we want to even mention that, but data throttling seems to be a new thing that's come up recently.

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

Yeah, and it's interesting; the term data throttling feels to me like it has a bit of a value judgment built in; it's a bad thing, it's blocking. The term rate limiting, on the other hand...

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

There you go, yeah that. Yeah.

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

...it means the same thing and it feels like it has less of a negative valence. And I think this highlights the fact that there is a legitimate issue here and there's a real gray area. Every real API provider in the world implements rate limiting, and it's just a question of what limits do you impose? If you impose a very low limit and say, oh, as soon as you go over one request per week, you're violating my limit; okay, well that's a bad thing.

On the other hand, if you say, as soon as you go over 1000 requests per minute you're violating my limit, well maybe that's okay. And so there's this interesting threshold that happens where the general concept of imposing these limits is fine, but the actual details are where this sort of distinction between reasonable limitations and unreasonable limitations will have to play out. And so yeah, I think it is an issue that deserves to be addressed, and maybe that falls...

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

So who would...I guess I have question, who would be imposing the rate limit?

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

So, well let's just take a consumer API example, right. If I register an App to talk to services that Amazon provides, for example, or Google...

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Right, correct, correct.

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

...you know if I could.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Right, but I mean in a healthcare environment, who would be instituting the rate limit?

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

So practically it's whoever is administering the servers that are hosting the API. But I think I'll take your point which is, if it's Boston Children's Hospital contracting with Cerner to host the API, you know, it

really shouldn't be Boston Children's Hospital saying that 10 requests a week sounds like too much; it should be engineers at Cerner saying, our servers can't handle a load above "X".

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Right, right, and then trickle that down into, you know potentially affecting the operators and then we start getting into things like net neutrality, etcetera and that's where I'd like to stay away from.

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

Agree, I just know of very specific examples recently where very prominent vendors are starting to play these tricks with each other to squeeze the hospitals out in saying, oh, we can only connect at this certain rate and only this certain amount of traffic can go over it at any time or otherwise we'll shut down the pipe.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

That's terrible...

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

And it's just...it's maddening because there's nothing out there that provisions you can't do this unless you have a contract that states that.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Yeah no, agreed.

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

Yeah, so I've just sort of highlighted this in the footnote here about clarification, and maybe terms of service really is where this applies. Could you have a limit like no more than "X" requests per minute? You know, does it depend on "X" and what about specifically no more than one request per week, you know, this seems obviously unreasonable.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And perhaps a note that says, where do complaints of this kind go?

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

Mm-hmm.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Because this will be quite varied and as the technology improves, sort of the have and have nots of those gaps might widen, where there is some sort of rate limitation that has malintent versus the great technology that's making it quick and available. Where do those kinds of complaints...

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

Yeah, for both consumers and for providers, right?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

(Indiscernible).

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

Or for anybody really...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, right.

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

...could mean...that's a very good point, Leslie. I mean again, as a hospital CIO, I mean I wanted to pull my hair out sometimes with some of the games that are played, so, agreed.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Right.

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

Good, so I at least captured those questions, including the one about where complaints should go, attached as issue here. It makes me feel better to at least know that we're raising them, even if we don't have answers. Umm, okay, if we have, I guess we've got 12 minutes or so; so one topic that I would like to go into is, back to our question about where BAAs are allowed and required.

I know that we shouldn't try to resolve this issue right now, but I want to make sure that we've highlighted any open questions. So that's what I'll do in the absence of other suggestions, but let me open it up for the folks on the phone; are there topics that you want to make sure we get to before that, because we do have a little bit of time to jump here or there?

M

I think it's just keep on, keep on.

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

Okay, so I'm going to go back to this earlier topic of when does an App developer need a business associate agreement? And this is an area where Leslie had been, you know, deeply involved and listed a bunch of scenarios and here's where we are right now.

One thing that we've found is that the Office for Civil Rights has produced some specific guidance, including a set of scenarios about when health Apps need a BAA. And you know, based on that guidance we can recognize some scenarios where no BAA is required, but of course relationships between healthcare organizations and health IT developers can be complex and it can be difficult to map real-life circumstances into OCRs prescribed scenarios.

And maybe there's gray areas where App developers offer some services to a covered entity but the App, you know, cannot access data except when a patient explicitly approves it. You know, there are scenarios where we think we don't know the answer and it's hard to map to what's been listed. But what I wanted to do is to get to the point of real precision, to be specific enough to say, here's a scenario where we don't think the guidance is clear; it seems to be different from the scenarios where we do have guidance. And so I had asked, you know, for folks to list scenarios in cases where we thought there were some outstanding issues.

And Leslie responded with a comment that I'll just pull up in a separate window so we ca...so it's big enough that we can read it here. This is just Leslie's comment who said, you know I question this one big time. And then Leslie had quoted some of the scenarios from the OCR guidance, and so there was one scenario about the health App that is recommended for a patient and the patient uses it, where in the scenario OCR said, well the developer's a business associate of the provider because it's creating and

maintaining the information on behalf of the covered entity. And Leslie says, I question the yes on this scenario.

So there are two kinds of issues here; one is, if we think that OCR has it wrong and two is if we think there are scenarios where OCR just hasn't weighed in. And, you know from my perspective, I don't know. I thought the guidance was pretty clear and reasonable, but I think it's clear at least that Leslie has issues here. So let me just see if Leslie can weigh in on both of those; number one if they're getting it wrong and number two, are there specific scenarios where they just haven't made a recommendation, but we need them to.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Right, and maybe it's the latter makes the prior seem that it's wrong. But it...here's my concern is that the...is the relationship between the App and the API ba...the developer of the App and the developer of the API, is that, or excuse me, let me start over. My concern is that a covered entity has a relationship with Cerner, that example. Cerner comes up with an App for the patient to use. The only way the patient can connect to the API with that Cerner App is if they take explicit action.

So there is no benefit to umm, there's no explicit relationship between that App developer, even though they're Cerner and the data that exists in the EHR; it's not a prepopulated App, there's nothing that the relationship between the BAA, Cerner and the covered entity. There's nothing about that relationship that's different when the patient is controlling the movement of the data. And so if the scenario state that because the...Cerner in this case, has a BAA in scenario number one, they always have a BAA in scenario number two.

The concern is that the prevalent initial App rollouts for the patients will come from certified HIT providers, and we want to make sure that there's a high degree of adoption. But if, let's say Cerner develops or purchases a consumer-based App that they use and that can be connected to the APIs with the patient's direct action, that App should be free of the constraints of HIPAA. My concern is that all of a sudden now, that App, all the data held if it has to be under the auspices of HIPAA, it has to be in a secure environment, it has to get encryption at rest, all of those things that are constrained now have to apply to that App of the patient's choice. And so that's my concern.

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

Okay. So let me sort of play this back and forth game. I've got the scenarios now open from the OCR guidance and on the second page they have a scenario that to me looked a lot like the one that you just described. It's the last scenario they list and it says, a consumer downloads an App to her Smartphone, in this case it's offered by her health plan and she gets it and to store her healthcare records and check the status of claims decision. And the App...the same App is available to the plan's wellness...sorry, the same App also contains the plan's wellness tools for members so they can track their progress. Health plan analyzes health information and data about App usage and the App developer also offers a separate direct consumer version of the App that consumers can use to store, and manage and organize their health records.

So there's the same company offering the same App in two different contexts, one is on behalf of a provider and one is direct to consumer. And the guidance says, you know in terms of whether a BAA is required, the answer is "yes" with respect to the one that they're offering on behalf of the covered entity and "no" with respect to the direct to consumer version of that same App, which I thought that that's sort of the answer that you're looking for, but maybe not.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

But what is it about that that creates in the first scenario that's a yes, that if that it is. If the patient is totally responsible for the data movement from the API to the App, what is it that makes it now being a covered entity, because there is no data movement without the patient's permission and consent? Why? Now if you take that initial one and it says the Smartphone download the App provided by the health plan and it's now under BAA, then how do you manage that App with a HIPAA security framework on a...that's downloaded to a phone? Do we actually help in adoption?

So I'd really like guidance about what makes the relationship between any covered entity and a BAA. What makes it...what makes that a relationship versus from taking that forward and saying that relationship exists, therefore now with any sort of endorsement coming from that provider would imply that that App is now covered under HIPAA. And so that's my concern is that...

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

Okay, so...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

...there...it's not clear and I don't want to have a marketplace where the provider is constrained because they want to choose an App from Cerner, but now they have to go through all of the same mechanisms, all of the same issues to protect the patient and data because it's deemed a covered relationship versus just an App connected to the API.

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

So, okay. When I read this scenario, and maybe I'm reading too much into it, I see what looks like some justification here that you know maybe it could be more explicit. Let me see if you agree with sort of the way I read into this. So in this scenario it says, the health plan is going to analyze the data that the App collects to understand its usage and that the health plan offering users this App.

So when I sort of put those pieces together, what I hear is, the health plan tells me, here's an App you can use then if you use it, the health plan will just see everything you do and they'll have access to that information. And so that's why in this scenario the App is being offered, you know, basically on behalf of the health plan and my information is being shared back with them automatically; that's sort of how I'm reading it. And because of those things, the App is acting like a business associate in that scenario. I think your real question might be, well could we tweak it so that more or less everybody got the same experience but with a few more explicit permission steps in the process and cause it not to be a scena...a covered entity anymore, not to be a business associate, rather?

So, you know so for example, could we take this scenario and tweak it step by step and say, if you make the following three changes, umm, it wouldn't be a business associate. And those changes would be like, you know change number one, umm the only way information flows is after a patient explicitly signs up; that's the only way information flows into the App. Change number two, umm, nothing a patient does in the App is shared back with the provider, unless the patient consents to that. Umm, you know, maybe that's it; so, are those the kinds of changes that you have in mind and if we made those two then it shouldn't be a business associate anymore?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, I think that fits that. And then if we go back to the other one, which was really just it looked to me more like a commercial relationship between certified HIT and the provider, I...maybe it's just can we get an idea when a certified HIT provider with one relationship with a...certified App provider with one relationship with a provider does not necessarily mean that all relationships continue to be under that BAA.

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

So for me, and I expect that for OCR as well, it would be really helpful to have specific scenarios and to have them related to each other, you know, if we have scenario 1A and B and C and we say, well here are the tweaks that are applied, and we think because of these tweaks we've moved from the realm of a business associate to no longer a business associate. Leslie, if you could write out, you know, a set of these and say here's how we think the analysis works, I think that would get us to the point of specificity where we need to be. If we ask just for sort of guidance about things like "X," I think the risk is that we'll get back something that doesn't actually address the specifics that you're worried about.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay, I'll attempt to do a table that kind of gets to those outlines. And then there was one other area that, what about the App within an App so you have an Intel inside equivalent, you have an App that is not addressing the...like a plug-in that's not addressing anything related to what's HIPAA covered; how does that work? How does that downstream trickle effect work? And so I'll include that as well.

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

Okay, and I think that, you know, the best thing would be is if you write up, almost in the same format as this PDF, write up a scenario and write up what you think the interpretation should be and that way if there's...I think that'll help us to identify gaps, or it'll help OCR to look at your analysis and say, "Oh, yes we agree, this is very clear or no, this is where Leslie went wrong, you know, through the following assumptions."

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay.

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

But the more you can spell out the reasoning, the easier it will be to identify where those gaps are.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay, fair enough.

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

Good. Okay, umm, and then in terms of that table, if you want to insert it in the document before Wednesday, that's great. And so you could just go to the document and type in it, rather than writing a comment; you can just come in here and I'll add a table actually, here and you can just fill this table in. And, umm, okay.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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

Sure. So we've got a couple of minutes left if we want to dig into another topic or at least to raise something briefly. Let me just pause and see if anybody's got something they want to bring up in the last few minutes.

All right, well we can finish up a couple minutes early and move on to public comment at this point, since no one else has issues they want to raise. Let me just remind folks that we'll lock the document Wednesday night; that means you won't be able to edit it directly anymore, but then please do come and review the document and share feedback. With that, let me turn back over to Michelle. You know, thanks all for joining and for the discussion today; I appreciate it and I think we're actually making it through to the point where we've got some recommendations that are going to be quite helpful.

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

Thank you, Josh. Lonnie, can you please open the lines?

Public Comment

Lonnie Moore – Virtual Meetings Specialist – 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

We do have a public comment from Adrian Gropper. As a reminder, public comment is limited to three minutes; please go ahead, Adrian.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Hi, I have a small point, or concern around the terms of use. We need to consider rate limiting, if that's what we're looking at, should not limit the ability to get clinical decision support Apps working at the point of care. So in...if, we'd like, for instance, for an App to be able to look up a drug price in GoodRx as soon as that prescription is entered, and so the definition of terms of service and rate limiting needs to consider that kind of capability. Thank you.

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

Thank you, Adrian. And we have no further comment at this time. So thank you, everyone and as a reminder, our next meeting is Tuesday, April 12.

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

Great, thanks all.

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

Thanks, have a great day.