



## HIT Policy Committee Privacy & Security Workgroup Final Transcript April 27, 2015

### Presentation

#### Operator

All lines are bridged.

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

Thank you. Good afternoon everyone this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Policy Committee's Privacy and Security Workgroup. This is a public call and there will be time for public comment at the end of the call.

For those of you who are following along using the on-line webinar in the past if you had left a public comment via the webinar we just made it part of the transcript but we may now with some discretion be sharing those as part of the public comment at the end of today's call so just letting everyone know that we may be sharing those comments.

For the members and those participating if you could please state your name before speaking as this meeting is being transcribed and recorded that would be appreciate. I'll now take roll. Deven McGraw?

#### Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Here.

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

Hi, Deven. Stan Crosley? Adrienne Ficchi? Bakul Patel? Cora Tung Han? David Kotz?

#### David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

Here.

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

Hi, David. David McCallie? Donna Cryer? Gayle Harrell? Gil Kuperman?

#### Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Here.

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

Hi, Gil. John Wilbanks?

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

Present.

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

Hi, John. Kitt Winter?

**Kitt Winter, MBA – Director, Health IT Program Office – Social Security Administration**

Here.

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

Hi, Kitt. Kristen Anderson?

**Kristen Anderson, JD, MPP – Staff Attorney, Division of Privacy & Identity Protection – Federal Trade Commission**

Here.

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

Hi, Kristen. Linda Kloss?

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Here.

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

Hi, Linda. Linda Sanches?

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Here.

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

Hi, Linda. Manuj Lal?

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Here.

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

Good afternoon. Micky Tripathi?

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Here.

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

Sarah Carr? Hi, Micky.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Hi.

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

Sarah Carr?

**Sarah Carr – Acting Director – Office of Clinical Research & Bioethics Policy – National Institute of Health**

Here.

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

Hi, Sarah.

**Sarah Carr – Acting Director – Office of Clinical Research & Bioethics Policy – National Institute of Health**

Hello.

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

Sephania Griffin? And Taha Kass-Hout?

**Taha A. Kass-Hout, MD, MS – Director, FDA Office of Informatics & Technology Innovation – Food & Drug Administration**

Here.

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

Hello. Anyone from ONC on the line besides Lucia Savage and Angelee Patel? Okay, I'll turn it back to you Deven.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

All right, great, thank you all very much. Let's go ahead and go to the next slide. Today we're going to spend time talking about a couple of provisions of the Meaningful Use Stage 3 Notice of Proposed Rulemaking. For those of you who were able to join our call last week we discussed a couple of provisions in the Certification Notice of Proposed Rulemaking and we have one more call this week, I think it's on Friday, to sort of wrap up the discussion both on the Certification Notice of Proposed Rulemaking, NPRM, and the Meaningful Use Notice of Proposed Rulemaking.

So, whatever we did last week we are going to capture the discussion in a set of draft recommendations that will be ready for us to look at this Friday, similarly, what we're able to accomplish in discussion today we will endeavor to try to spend our call on Friday in wrap up.

We do not usually have this many meetings in so close a succession and the reason why we're doing this is because we have just a short period in which to weigh in on both of these Notices of Proposed Rulemaking and so we needed to add one more call to our schedule in order to get that done and the only time that generally worked for folks and probably didn't work for everybody was to sort of crunch these all together in the way that we have.

You will get a bit of a break after this before we turn to our next topic which we're currently in discussion with ONC about what that will be, but I suspect we'll return to big data or we may pick something else up that's on their near-term agenda where they want us to give them some feedback.

But in the meantime we do, unfortunately have a bit of a truncated time table for these NPRMs and your patience and your diligence, and your willingness to hang with us on all of this is very much appreciated.

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

Hey, Deven, this is Lucia; I just wanted to say...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah?

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

In my official capacity say thank you to everyone because we're all working really hard to get all this done in time and we recognize how much we're asking you guys to lift and we're very grateful.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, thanks, Lucia. Well that's why we're here to try to be helpful so we'll continue to try to do that. Next slide.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Hey, Deven, it's David McCallie, I'm late to join, just wanted to let you know.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, that's all right, David, thank you, good to have you.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

I'm also here too Deven, this is Stan.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, hi, Stan, great, terrific. So, again, we're here on the 27<sup>th</sup> we have another call on the 1<sup>st</sup> to wrap up the NPRM comments that Stan and I will then present on the May 12<sup>th</sup> Policy Committee meeting. Next slide.

So, the two topics in the Meaningful Use NPRM that we've been asked to take on are reviewing proposed objective one on protecting patient health information and here are the relevant citations, pages in the Federal Register and the relevant rules section.

And then the ramifications of increased patient access to data and we were specifically asked by both the Consumer Empowerment Workgroup and Paul Tang, the Chair of the Health IT Policy Committee, to think about what the privacy and security implications are for this increased patient access to data through view, download and transmit, and also through the API proposed certification option. So, next slide, please.

So, I thought we'd tackle the first...the objective that is specifically on protecting patient health information first. Both of these topics are ones that the Tiger Team has opined on previously but this is a new Workgroup and some new folks and so it will be interesting to get feedback on whether there is more we can and should say about really both of these topics because we've opined on both of them before. So, with that I'll just go ahead and jump right into this first one.

So, the proposed objective, which is the first objective for Stage 3 of Meaningful Use is to protect electronic PHI, which stands for electronic protected health information, which is identifiable, that's created or maintained by certified EHR technology through the implementation of appropriate technical, administrative and physical safeguards.

Now this objective articulated with a focus more on the technical safeguards has really been part of Meaningful Use since its inception, it is part of Stage 1; it was part of Stage 2.

Here in Stage 3 what CMS has proposed is making it clear that the protections that are supposed to be deployed by entities participating in the Meaningful Use Program are not just the technical safeguards usually which come in the certified EHR technology but also administrative safeguards as well as physical safeguards. Next slide, please.

So, what the covered entities who are participating in the Meaningful Use Program, what they need to do is to do the risk assessment, again, it has always been the security risk assessment that's been required as part of Stages 1 and 2, but here in this proposed stage CMS is making more clear that the risk assessment should be addressing not just the technical piece but again the administrative and physical safeguards.

They need to...Meaningful Users need to assess the risks and vulnerabilities to ePHI that's created or maintained by the certified EHR technology. So, the focus is on the domain that is governed by the certified technology. It must be conducted or reviewed for each EHR reporting period, that's a full calendar year, and include any security updates and deficiencies that are identified as part of the risk management process and then implemented or corrected by the process. Now this is a set of expectations that the eligible professional or the eligible hospital then attests to as part of their Meaningful Use attestation in order to be eligible for the EHR incentive funds.

Now we've determined that this is largely consistent with what the Tiger Team had recommended when we had an opportunity to weigh in on what these rules should look like, although let me describe to you exactly how it's consistent and maybe not so consistent. Next slide, please.

We had a lot to say about this as a Tiger Team in part because we had received a presentation both from CMS as well as from The Office for Civil Rights that when each were doing audits for The Office for Civil Rights these are audits of covered entities for HIPAA compliance not for Meaningful Use compliance, but whether people were meeting their HIPAA privacy and security rule obligations and on the CMS side it was an audit of entities that had attested for Meaningful Use to find out whether in fact that they had attested truthfully to having met all of these objectives.

And in general what was reported to us at the time was that the security risk assessment was not being done as consistently and as completely as was required or expected and so we really wanted to underscore the risk assessment, we didn't want to add any additional criteria for the privacy and security category for Meaningful Use, but instead to sort of underline and make very clear that this expectation is quite serious and is connected to HIPAA Security Rule obligations, you know, not exactly the same because what's expected as part of Meaningful Use is, you know, a risk assessment related to the certified EHR technology and the expectations under the HIPAA Security Rule are far broader than just the EHR technology.

But we wanted it to be clear to entities that it was the type of comprehensive risk assessment at least of the certified EHR technology environment that otherwise would have been expected and is expected on the security rule because HIPAA applies to certified EHR technology as well.

And so we had asked...we wanted CMS to make a more clear connection between the HIPAA Security Rule and the security risk assessment that's required for Meaningful Use and in fact what we did get in the proposed rule is the addition of the terms administrative and physical safeguards for one that aligns the risk assessment for Meaningful Use a bit more clearly to the type of security risk assessment that is expected under the HIPAA Security Rule.

We also suggested that Meaningful Users be required to identify who the individuals are for conducting and documenting the risk assessment not because we were trying to point a finger at somebody but instead to underscore that this is something that someone should be assigned to be doing and should take seriously. This recommendation was not adopted in the proposed rule.

We also suggested that rather than having a single attestation as part of Meaningful Use that instead CMS break it up and have the attestation be linked to specific Meaningful Use objectives that might pose an increased security risk, this was partially in response to some commentary that we were privy to from some chief information security officers within entities that they often do not get brought in to Meaningful Use discussions and instead are just asked to bless something at the end of the day. And so we wanted people to understand that this risk assessment isn't just the sort of the check the box, end of the list sort of process, but our recommendation here was not adopted.

We wanted...we asked CMS to make it very clear that security professionals really should be fully involved assuming you're dealing with an office that has a security professional but they should be involved in discussions about Meaningful Use and here we did get a nod to this in the commentary that supports the proposed rule indicating that it may be necessary for a Meaningful Using professional or hospital to involve the security or Health IT support team, so it's not a requirement but a suggestion.

And then we urged both CMS and OCR to provide additional education to providers and there are references in the proposed rule to some very good risk analysis tools that OCR has put out there and what's terrific about this I think is not only are those sort of available on The Office for Civil Rights website but they're also...now the links to them are part of what entities will review when they start preparing to do their Meaningful Use security risk assessment.

So, we did not get everything that we asked for but we did get an endorsement of the need for more guidance and education, the need to emphasize that there should be security and IT personnel involved in this, and a more clear tie to the sort of comprehensive kind of risk assessment that the HIPAA Security Rule requires. So, not everything we asked for but I think a lot of the spirit of what we asked for. Next slide, please.

So, we just drafted, you know, a straw comment which is that, you know, we support the proposed requirements here and that by adding administrative and physical safeguards to the current requirements there is a more clear alignment with the HIPAA Security Rule, which was something that we recommended, again, not because we think one is a replacement for the other or that a risk assessment of certified EHR technology is your only security rule obligation, that would not be the case, but there certainly is some overlap and we wanted people to take the Meaningful Use risk assessment seriously. Any thoughts on this?

Do folks...and this is a straw comment for discussion. If people are disappointed that some of the stuff that we had recommended previously didn't get taken up or think that there is more to be said here now is the time to chime in.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Deven, this is Linda Kloss and I can support the straw comments and I think this will be a great step forward.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Great, thanks, Linda.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Deven, this is Micky, I agree.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay, thank you.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Hey, Deven, this is Manuj, I agree in principle, just one question.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Sure.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

For those solutions that don't necessarily maintain ePHI on their premises and it's just kind of use in the cloud or via their...actually, I take that back. If they don't have any control of the ePHI for example, will they still be subject to the more physical type of safeguards that may not apply to them?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, so are you thinking of a...now keep in mind that these are Meaningful Use requirements that apply only to eligible professionals and eligible hospitals that are participating in the Meaningful Use Program. So, not to the vendors.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Right, they're going to pass them down though, right?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, but they're the ones that have to attest that it gets done, right?

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Yeah.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

So, you know, they may ask a vendor to help them do this but that ultimately it's their responsibility for making sure that there is a risk assessment and that it addresses all three types of safeguards, and that they have addressed any deficiencies that they have identified, that's...it's their legal responsibility as a Meaningful Use attester.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

So...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

So, they can't pass the legal buck, they might pass the contractual obligation.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Right, right.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

But they can't pass the legal buck.

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

They can't pass...they can pass the process along Manuj, this is Lucia, but they're the ones who are attesting that the process was completed and that the controls are in place.

**Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise**

Yeah that's fair, okay, yeah, that makes sense, thank you.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay, sure. All right any other thoughts on this? Okay, terrific thank you all very much, we will pass this comment along as part of our report and now we'll move to the next slide.

And now we're going to move to talk about the ramifications of increasing patient access to data either through the view, download and transmit functionality or through APIs. Next slide.

So, again, we were asked by Paul Tang who is the Vice Chair of the Health IT Policy Committee to investigate the privacy and security ramifications of this. We have taken this on at least with respect to the view and download functionality very early in...I mean, I'm saying very early, it was August 2011, so the Tiger Team had been together for well more than a year by then, but this was almost, I'm counting on my fingers here, four years ago that the Working Group initially took up this issue of, you know, what happens when you're giving patients greater access to clinical data and they can download it and do what they want to with it, you know, recognizing that you've got some potential privacy and security risks for the consumer in terms of what they might subsequently do with that data and we took this on even before the proposed Stage 2 rule. So, we took it on through the lens of just view and download not even thinking necessarily about transmit.

And then, as I mentioned earlier, the Consumer Workgroup, which was a Workgroup that didn't exist when we initially took this on, is addressing these objectives in terms of the value to patients of both the objectives and the certification functionalities but it's really our task to evaluate privacy and security risks of them. So, with that let's sort of try to dive into this a little bit. Next slide.

So, objective five, patient electronic access to health information is really the objective that sort of more specifically raises the privacy and security issues and the proposed objective for Stage 3 is eligible professionals and hospitals need to use the communication functions of certified EHR technology to engage with patients or their authorized representatives about a patient's care.

And there are three measures associated with this, you have to report on all three of them and meet these specific thresholds for your choice of two out of the three in Stage 3.

Now again, it's not our job to opine on whether these numbers are the right numbers high, too low that's really the Consumer Workgroup's charge, our charge is to look at the privacy and security implications, but you can see that they are very strong incentives here not only to make access available but to get more than 25% of patients to actively use them, again, either through view, download or transmit, or through an API, you know, there are two other measures that deal with secure messaging and the incorporation of patient generated health data.

There are a few exclusions that include professionals who do not have office visits as well as professionals in hospitals in areas with insufficient broadband access those are exclusions. Next slide, please.

So, in thinking through sort of this issue of what are the ramifications from a privacy and security standpoint of increasing patient access to data either through view, download or transmit, or through APIs we sort of divided them up based on sort of who is responsible for sort managing those risks and on the provider side, you know, there might be heightened security risks from increasing numbers of APIs connecting to electronic health records. They might have some increased responsibility if they're dealing with a vendor who doesn't have a clear understanding of the implementation of privacy and security legal requirements or a vendor not necessarily following through on implementing an entities privacy and security policy.

On the patient side the patient may be using an App either for downloading or for transmitting, or through an API. They may be using an App or device that has weak security controls or they may be using a tool that either doesn't have a privacy policy at all or has a policy that's really unclear, or has a policy that shares data liberally with third-parties or allows broad uses, which for some would be a privacy risk and for others would only be a privacy risk if it was unclear that this was actually happening because in fact there may be some cases where a patient or consumer uses an App or some other third-party tool and it's totally fine with what happens to that data, but that...for some people would consider liberal use of that data by the App vendor or a third-party to be a privacy risk and hence why it's framed in that way, but fully acknowledging that it's a risk for some and maybe others might not see it as so risky.

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

Deven, this is Lucia...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Of course they would have to know that. Yes?

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

Deven, this is Lucia, I just want to ask a clarifying question. In the provider column the vendor that you're referring to is the organization who has provided the certified EHR technology?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

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

Okay.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, yeah.

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

Okay, so it's not that...it's not the vendor who has provided the technology the patient wants to send it to it is more about the technology where the data source is.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

That's exactly right and Lucia that's a really great question and I'm wondering if you intended it.

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

No I didn't...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

The certification requirements are only attached to the technology that the providers use. Patients do not have to go out and get their Apps certified.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Deven, does this set of ramifications apply to all three of the criteria or is this...I'm assuming it's overarching but if we were to break the ramifications out by type of criteria for example a patient provided patient generated data would this set of ramifications look slightly different?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

You know it might Linda and that's a good point. We really focused on the ramifications of the way that patients obtain data from providers through VDT or through the API as opposed to the inbound piece of this in part because even though there is a Meaningful Use objective that can be satisfied by the inbound of patient data unlike...providers are not required to adopt that criterion they can make some choices about whether they're going to accept data coming in from a patient whereas if you have a provider who is a Meaningful User who is utilizing either VDT or the API to send data to patients and they're using that as a mechanism for getting patients access to their data per HIPAA then as you'll see in a second they don't have...they don't really have as much of a capacity to say "no I'm not going to send you this data." I mean, they still have choices to make because Meaningful Use is not exactly...you know, isn't the same as HIPAA, but I think we thought of them differently Linda but it's a really good question.

Most of these slides that we prepared have been about the outflow, the issue of outflow of data to patients and providers and we didn't give as much thought to the inflow issues.

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

And Linda, this is Lucia, if I could just address that as well, so it kind of circles back to the first point Deven made in response to my question which was of course the patient's behavior is essentially unregulated legally. They can disclose whatever they want about themselves and they can supply data to their physicians in whatever quantity of completeness they choose to whether that's orally or through some other way. And I think measure three is about whether that inbound supply can be happening in a technical way in the space where the patient's behavior is essentially unregulated.

But I think you're raising a valid point which is where, you know, we have in other realms at ONC we're working on the issue of provenance which is partly so that physicians will be able to make appropriate judgements about inbound data from whatever source orally, family members, Fitbits, you know, FuelBands whatever, right, and that work remains a work in progress but it's not an issue we're unaware of that we don't want to...we want to make sure that physicians have the ability for inbound data that they haven't collected in a conversation with the patient to make a judgement or make an appropriate act based on the source of that data that's not reflected...we don't have a slide about that today.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

So, one thing we will do is when we get through the slides that we have prepared we'll toss back into the conversation the issue about the inbound data just to...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Thank you.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Make sure...thank you, Linda.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Okay.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Deven, this is Micky.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Hey, Micky.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Hey, one thing and I haven't looked through all the slides so maybe it's there somewhere, but one thing we might want to think about in terms of how we frame this is that...because I'm looking at the title "ramifications of increasing patient access to data..."

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Either through VDT or APIs." I mean, we're focused specifically on privacy and security ramifications, right?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Because there are other ramifications that I think aren't within the scope of what we've been asked to look at but that are nevertheless important and indeed the Policy Committee has battered around those areas of concern with respect to APIs and Apps and whether, you know, consumers and/or providers understand the uses to which these Apps maybe, you know, using data and whether that's appropriate or not, aside from the privacy and security aspects of it.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right, so we, you know, we'll make sure that if we end up keeping this slide in a subsequent presentation we will be clear that it's really privacy and security aspects, ramifications.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

Hey, Deven, it's John Wilbanks; can I make a quick point?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Sure.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

So, just to reinforce that not all the Apps are going to be clinician or physician facing a lot of them will be research Apps, this is something we've run into a lot with the first set of research kit Apps on the iPhone is the desire to pull data out of...to pull ePHI out of health records to transit into clinical studies...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

So, that's going to be one use case and one thing that we've learned there may be of note, which is that consumer developers of applications frequently don't...the technical teams don't understand any of the issues that come from the health privacy space and so some set of best practices for Apps that receive ePHI that could serve as guidance to those developers or at least as armor for battles with those developers when they say "we don't need that" would be really, really useful because it took us six months just to get vocabulary in place to talk about how important it was not to bleed data.

A lot of these things are not what people think about when they develop traditional consumer mobile applications but they are very important in dealing with PHI and that culture shock could be managed a bit if we could point at the kind of...these kind of guidelines and say, you know, we just want to follow the ONC's guidelines for building Apps that receive ePHI.

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

Hey, Deven, this is Lucia; John that is really a great comment and I can now talk freely because it's in the public realm, we're actually working on some mobile health developer best practices with Cora's team from the FTC, I don't have an ETA when it would be done, but I would invite you to include that comment in whatever you make as official because I think it's really important to capture and document as validated by our volunteer expert.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

Well that's good luck I don't usually hit that well, so thank you.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well terrific, I made note of that comment...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

We'll definitely fold that in it's a fantastic idea.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And Deven?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes, David?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

This is David; I think that, you know, to go along with that, I mean that's implications of what ONC or CMS could do in terms of creating guidance but it seems almost inevitable that in the long run some other kinds of certifying entities will emerge that can bless or validate consumer Apps given that they don't fall under HIPAA regulations and that they could easily meet FTC regulations while at the same time not meeting the standards that people expect of healthcare Apps.

So, I wouldn't be surprised to see independent entities emerge that would certify Apps as some kind of consumer trust symbol. I don't know if there is any business of us to comment on that but that seems almost inevitable.

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

David, this is Lucia, I'm going to ask you a leading question, are you implying or validating the idea that people think HIPAA applies when it doesn't?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, certainly, I mean, that's what the previous comment I think brought forth is that the developers of these Apps don't even know what HIPAA means so anybody who assumes that health data flowing over a government approved channel to an App is going to follow the rules of HIPAA is going to be sorely disappointed. So, yeah, I think that's correct they don't know what it means.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay, well, speaking of HIPAA, we actually have a few slides so that people understand the connection between the HIPAA Privacy Rule and patient access under Meaningful Use and I'm glad we have Linda Sanches from The Office for Civil Rights on the phone in case I trip this up and don't get this quite right.

Again, HIPAA's obligations are separate from Meaningful Use obligations but HIPAA does provide a baseline right for patients to be able to access their data and as you'll see in a minute the form or format that the patient gets this information in is one that the patient requests and if the provider can comply with it then, you know, they have peace and harmony and the transaction can go forward.

If the provider doesn't have the technology that the patient requests then there is a bit of a negotiation about what the patient can get, but when a provider has tools that they can provide patients with easy electronic access if that's the kind of form or format that is satisfactory to the patient then the provider can help meet their HIPAA obligations using their Meaningful Use or their certified EHR tool set in order to do that.

So, it's important I think to sort of understand where there could potentially be some overlap in the use of these tools to help at least when these tools are used to help providers meet their HIPAA access requirements. Next slide.

So, again, what was made clear in the 2013 Omnibus Rule is that when patients want an electronic copy of information that's maintained electronically they have the right to get that electronic copy, again in a form or format that the patient requests but it needs to be readily producible in that format.

They also have the ability to direct that this information be provided to a third-party rather than having the information to come to the patient first and then be sent on, the patient can say "I want you to send it to x" and as long as they've given the proper address and the provider or the health plan puts the proper address in there then that meets that obligation.

It does not require providers to make access to their administrative systems because the HIPAA right is to information that's called...that's in a designated record set, which is information that's used to make decisions about the patient just in shorthand, and it applies to information that's present at the time the request is fulfilled. So it doesn't give a right to a continuous feed or to a subsequent feed, it applies, the patient says "I want this information" in a time that they've requested it that if that information is available then the patient can get it.

Entities also have the capability to reject a patient's request to use a specific type of external portable media if they think...if the entity thinks that connecting to that media would cause an unacceptable level of risk for them from a security stand-point. Next slide.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

But its risk to the provider not to the patient.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

To the provider that's correct, thank you, David. Next slide, please.

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

And actually I think David it's...Linda can correct me, but I think it's actually risk to the provider's obligations under the security rule.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah that makes sense.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Yes.

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

It's just not any old risk to the provider or any old risk to the patients, the provider's obligation under the security rules would undermine those.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Right but it doesn't imply for example that the provider thinks that the App is a bad App.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

It provides...

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Correct, you're right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

...

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

The security issue here is with whether external media might be a risk to the covered entity's systems.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Right, right.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And that was Linda Sanches from OCR, thank you Linda.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Yes, I'm sorry, thank you, Deven.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

That's okay, terrific, all right, so next slide. Then we have two slides that talk about whether the provider can reject a patient's request for access to data and there are...let's see I think we skipped a slide, can we go back one? Okay.

So, they...a healthcare provider could reject a patient's request and that rejection would be not subject to review if what the patient is asking for is protected health information that's not covered by the right of access like psychotherapy notes for example.

If the covered entity is a correctional institution there are circumstances under which the request could be rejected.

If the PHI being requested is part of research, an ongoing research protocol, and providing that information to the patient would be detrimental to the research because it is still going on so it could be rejected for that matter.

If you have a covered entity who is also covered by the Federal Privacy Act and the information access requested is exempt from disclosure under the Privacy Act well then the entity can deny it in this circumstance as well or if the information that the patient requests had been obtained under a commitment of confidentiality and providing that access would breach that confidentiality then the request from the patient can be rejected and that's not reviewable. And here we reiterated here the issue that we just discussed. Next slide, please.

Now, providers also can reject for some other reasons but those are subject to review. If the patient is not satisfied they can ask for an objective review of the decision. So a provider can deny a patient's request if a licensed healthcare professional has determined that the access that's requested is reasonably likely to endanger the life or physical safety of the individual or another person, or the information makes reference to another person, not the provider, but another person who is not the provider and a licensed professional determines that the access is reasonably likely to cause substantial harm to that other person or you have access that's requested by a personal representative and the professional determines that the access by that personal representative is reasonably likely to cause substantial harm to the individual or another person. In all three cases the professional in making this decision has to be exercising his or her professional judgement.

And the reason why I emphasize this and it's probably pretty obvious to most of you, but just in case it is not, is again, if a provider is using the portal as a way of allowing patients to access data that they have a right to under HIPAA their ability to say "no" to that patient, absent that security risk issue that we just talked about, is very limited.

So, if what the patient is asking the provider to provide them information is, you know, to report the data to iratedoctors.com or if the patient wants to contribute to a research database, or if the patient wants to sell the data to a commercial interest, you know, none of those things fall into these deniable categories.

And again, HIPAA not precisely the same as Meaningful Use but if you're using your certified EHR technology as a mechanism for getting patients records per their HIPAA access right you have limited capacity as a healthcare provider for denying those requests.

All right, so the next few slides go into some of what the Tiger Team said previously, can I have the next slide, please, on the issue of risks that the patient takes on when they view or download their healthcare information.

And for those of you who may remember this discussion we urged best practices on the part of both vendors and healthcare providers with respect to these risks, we thought that it was not a great field for a one-size fits all certification style requirement but we thought guidance for healthcare providers and for vendors in terms of providing what are really a set of transparency tools for patients when they are viewing and about to download their record.

And we very much relied on some material that the Markle Foundation had pulled together with respect to the launch of the Blue Button functionality in terms of, again, making sure that patients got some notice about the transfer of risk when the patient takes the data and asks for it to be directly transmitted to another person or another entity, or has it downloaded or moved into a device, or a mobile App that that's a transfer of risk to the patient that the patient should know that that's what they're assuming.

And so some of the best practice suggestions that we had was that providers who are participating in the Meaningful Use Program offer their patients some clear and simple guidance with respect to view and download, and again, this is for Stage 2.

And with respect to view the guidance just should cover the potential risks of viewing the information on a public computer or viewing it on a screen that may be visible to others or failing to properly log out after viewing. Next slide, please.

And all of you received a copy of the transmittal letter for this but I'm going to assume that at least some of you probably didn't have time to read it.

With respect to download the guidance should ideally be offered at a time that the patient indicates a desire to download the information. So, ideally it would show up on the screen and not just be provided on a separate piece of paper that a patient might not have with them when they're getting ready to download at least for the first time.

But the guidance should remind patients that they're the ones who are going to be in control of the copy of information that they're downloading and it's their responsibility to take steps to protect it in the same way that they, the patient, would protect other types of sensitive information that would include a link or links to resources with more information on topics of like the download process and how they can best protect information. And before the download occurs get some independent confirmation from the patient that in fact given all of this that they want to complete the download transaction or transactions that they are about to do. Next slide.

We also recognize that if patients got this notice more than once they'd probably be irritated and so ideally this would be something, a functionality, that could be turned off if the patient didn't want to get repeat notices and providers could work with their vendors to capture this functionality in their EHR software but also in a way that doesn't keep cash copies after the session, the patient's session with the...in the portal or I don't know if the same thing would apply for using an API that's an interesting question and providers could also ask their vendors to request that there be an automatic termination in the event of a period of inactivity if the patient opens up their account and then leaves it open inadvertently. Next slide, please.

We thought that this guidance would be valuable both for providers as well as for vendors and we did point to the policy briefs that had been prepared by the Markle Foundation in advance of the Veterans Administration and CMS providing some guidance to their users with respect to Blue Button which they did incorporate some version of what we talked about before and it sounds from my description like the kind of notice that was provided was fairly heavy but it was actually very brief, you know, no more than, you know, three or four short bullet points.

So, it was a very light sort of notice focusing on, you know, your downloading this information are you sure this is what you want or you're viewing this information make sure that, you know, if you care about the sensitivity of this information that you're not doing this on a public computer in a place where people can see it. It was very...the idea was the layered notice idea was where patients get something very easy to see and then if they want with links to enable them to download to more information if they want it.

So, in no way did we, at the time that we first took this on, next slide, please, say that patients shouldn't be...not permitted to do whatever it is that they want to do with this data but some transparency around risk offered at the...just in time, right at the time when patients are about to engage in a transaction that might encourage some of that risk for them that this would be a valuable thing.

We suggested that it be done by guidance and not through the certification process, again, because we wanted providers to have an opportunity to work with vendors and determine what was the best option for them and it just didn't seem like a place where a single sort of one-size-fits all standard or a certified capability was the right way to go at least at the time.

So, I'm interested in what sort of reactions you all have. Again, we really did not have the transmit function in mind when we took this issue on because I don't think that one was added until the proposed rule and we should consider whether or not that makes a difference in terms of these recommendations.

We should also consider whether we have a different set of recommendations now that four years have passed and we're a little bit more knowledgeable about the subject matter, maybe some of us maybe and we have more people on our Working Group frankly this time around who are working directly in this space of consumer facing technologies and that was not necessarily the case when we came to these recommendations previously. So, I'm going to open this up for comment.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Deven, this is David Kotz, since I have to leave fairly soon, actually early, I will...I just thought I'd add one thing. Back when these were discussed before we probably were thinking in terms of browsers being used for the viewing of this data and increasingly I expect Apps are the mechanism of access to these portals and that may not change our recommendations but it might change the way that providers phrase their best practices.

For example, if the data is downloaded into your App the patient may be thinking of it as viewing the data but it actually is downloading a copy into the phone or tablet and then from there it could be at risk of disclosure...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

If you lose your phone, so we might want to update those best practices if they live somewhere to keep that kind of risk in mind.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Got it.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

It's a technical issue more than a policy issue I suppose.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, except it may be worth noting, and again, we did not...we called for guidance but didn't take up the task of writing it.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Yeah, right, okay.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

But we did, you know, in the transmittal letter we did note specific types of risks that we thought ought to be accommodated by the guidance...

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Yeah...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And this would absolutely fall in that category.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Yeah.

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

Hey, David, this is Lucia, I'm...with the John comment I think that's really timely and helpful and I will talk to the team and the FTC, maybe when we get farther along on what we're actually working on for that space that's basically unregulated mobile health maybe we should just have you guys check it out. I don't know, I'll talk to them and we'll keep the Chairs posted.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So, Deven, this is David, I have some, the other David, I have some comments?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Sure.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

One is with respect to the providing of notice it is probably the case that when an App authenticates itself into the portal the patient typically would have to...they would be redirected to a screen where they would essentially log into their account which is the indirect way that the App gets access to the account. It's probably the case that this screen could display the appropriate warnings to the patient that we would have put in the browser in the early recommendation.

So, I think there is a technical spot for that information, you know, we could make a similar recommendation that when the patient uses an App to authenticate into the portal account that the portal should notify the patient about the potential risks of downloading the data, so just a technical footnote there.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

More substantive I think the questions that come to my mind are do we think that the Apps should be registered or certified in some way, I know we don't necessarily have authority for that, but the question, you know, was hotly debated in the Blue Button Plus Workgroup as to whether there should be a registry of trusted Apps.

And then sort of implicit from that is should a provider have the power to refuse to connect to an App that wasn't registered or certified in some way, and again, I doubt if we have authority to make such a recommendation, but we could certainly debate whether or not that is something that ought to be sought.

So, there will be providers who basically say "I refuse to let that App connect to my system because I don't trust that it's in the best interest of my patients" admittedly not...that doesn't fall under one of those categories in the Omnibus Rule but it could be an issue that comes up in the real world.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Right and, this is Micky, just to that point, is that...to that last point that David just made, is that what the last bullet on this slide is getting at Deven?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, that's part of it, yeah, we came up with some straw questions or comments and, yeah, I mean the security, you know, where there is a security...genuine security risk that's posed, you know, the...I think, you know, certainly from a legal stand-point where HIPAA is concerned there is an ability to reject that sort of form or format way of giving a patient access, but assuming that isn't the case and it's really just that the provider thinks it's just a bad idea or feels threatened by the App in some way, even if it's not a security issue, that their ability to sort of say "no" you know it will mess up their numbers from a Meaningful Use stand-point but it's hard to see how, again, since we're talking about the Meaningful Use Program a provider gets to sort of...has some level of control over how they make their portal or API connection available for Meaningful Use, you know, if they're going to rely on it for HIPAA purposes they might have less ability to reject things that patients may want to do with it as we talked about, but if it's just about, you know, well this is Meaningful Use and this is how...this is how I'm going to run my Meaningful Use Program.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And...

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

Well, Deven, this is Lucia; I mean, the other, the sort of reverse facet of that is something we talked about two or three meetings ago when we were sort of working on the roadmap comments where there was a dialogue about, you know, we know that there are permitted disclosures under HIPAA but maybe they don't happen enough because people aren't sure what their liabilities are once they permissibly disclose.

If this is of the same nature, clearly not under the same rules, but if it's of the same nature I'm permitted to let this patient go get this data that's there, in fact I'm required to, you know, are there ways we can...that further guidance could or whatever we want to call it, further information could be elicited which would either be not only the grounds the physician has to say "no" as you've articulated in your bullet, but, you know, what is the physician's liability once the data goes out the door if any.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well that's, you know, so, you know, there is both...there is the carrot and the stick approach where, you know, the carrot, that Meaningful Use has a set of objectives that must be met in order for payment to flow through and there are some constraints on how those objectives are met, but generally the provider or hospital participating in the program they can make decisions about that, but if we make it easier for them to say "yes" to patient connections, again absent the security risk issue that we've already discussed like clarifying in the way that the Omnibus Rule does frankly that, you know, once...that where the patient transmits it to is not the healthcare provider's responsibility.

As long as they've followed the patient's instructions in terms of where it's supposed to be sent that's the end of their liability. The Omnibus Rule is really clear about that so making that same kind of clarification in this circumstance, you know, could be helpful.

I'm interested in people's views about David's idea about a registration or certification of Apps as a sort of...as a desirable end point even if we can't require it.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

I mean, this is David again in the discussion from the Blue Button pull era I don't recall the exact details, but there was a belief that you certainly could support unregistered Apps but that there also needed to be an optional registry mechanism as part of the technical standard that would enable someone to detect whether an App was in fact registered in some registry that you trusted.

So, there was debate that, you know, there probably needs to be just unfettered access as a baseline but also that the technical standard should support some way to detect whether an App was registered and that's not necessarily relevant here accept just to say the ground was covered that there is a belief that it will at some point be probably a good idea to have some way for consumers to know if this App has been vetted by professionals in some sense that it actually behaves the way it claims and that it does things that aren't going to be harmful to the patient like selling their data on the black market, selling their identity on the black market.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

This is Micky; I think that seems to make a lot of sense except it seems very premature to try to specify what that might look like. It seems like the ecosystem needs to develop and conventions around this need to develop a little bit before getting to that level of specification.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

This is Linda Kloss...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, I...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Could we at least address it from the stand-point of the desirability for the patient to have this as a voluntary mechanism or something that's not mandated but encourage the development as an industry of this kind of voluntary assessment or voluntary accreditation process?

My second question and well maybe finish out this line of discussion, but I have little different take on the comment.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Sure, I had a follow-up question for you Linda is, what would we be evaluating or what would we recommend that these Apps be evaluated for? If we were to say that there might be some value to some sort of registration...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well, the...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And/or certification process?

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

I think...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

What would be the components that would be valuable to the patients much less, you know, from the provider's stand-point?

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Well, I think that...

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

This is David, I would suggest...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Patients are being...

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Sorry.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, can I just...since I...David, I know you have a little bit of time...

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Yeah.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

But since I posed to question for Linda I want her to respond first...

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Sorry.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And then you.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

I would suggest that particularly the government principles in the area of privacy, security and the way the App is handling the accuracy of data.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And any particular principles that you're thinking of or...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Secondary use, redisclosure...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Of data and certainly some data integrity processes.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Let me let David ask...have his response because I want to push on this a little bit more. Go ahead David.

**David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College**

Yeah, I would...in addition to those I guess I would be looking for some technical assurances that the App is storing the data in a way that is not likely to leak to third-parties in particular ad providers which is a known problem in many of today's Apps. And that the data can be deleted and wiped from the App or the phone or what have you easily, it might be even automatically on a routine basis.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Deven, this is Stan and I know you want to follow-up on this, I'd like to chime in a bit as well.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, go ahead.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

I'll let you finish your follow-up.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, I was only going to say, like are we asking for the Apps, not on David's points about, David Kotz's points about leakage or the ability to control disposition of data particularly at the end of the relationship which I added David Kotz because that's what I was thinking when you made your point, but are we...in terms of the governance pieces are we asking for transparency about those aspects or are we saying they should have policies that don't sell data?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Registered.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Because admittedly I have a problem with that.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

I think...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

And this is Stan and we're thinking parallel paths here Deven, you know, I think the best we can do or at least what I would, maybe the limit of what we should do, in my opinion, is suggest, you know, appropriate diligence by the patient, give them the warning that this is no longer regulated space, but beyond that, I mean, you know, there will be some incredibly good uses from incredibly good Apps and we don't want to discourage this activity either.

And there is also simply no way...I mean, this is going into an ecosystem that includes wireless carriers and operating system providers and hardware providers, you know, and the data is simply going to be moved around and giving a direction to the App itself could also give a little bit of a misdirection to the patient potentially saying, well if the App is good then I don't have anything to worry about, you know, the bottom line is that once it leaves that ecosystem, you know, there are probably a dozen different entities that are now involved in handling and managing that data and so just to say it's an App specific inquiry is, you know, also problematic.

So, you know, I don't think there is a way you can win once you start down this path other than to say that, you know, once it's disclosed you understand that, you know, it's no longer protected by federal law and, you know, you have to be sure you're comfortable with it.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

This is David McCallie just to chime in on that, I think that, you know, the minimum would be the App and the ecosystem that provides that App to you has to have a privacy policy that describes what they do with your data. We wouldn't probably want to describe what that privacy policy should be but at least it should be clear so that something testable FTCish...if somebody wants...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Yeah, you know, that's...I actually like that suggestion that, you know, make sure the App that you download, you know, has a privacy and security statement that describes how your data will be used. I think that may be a real good way to at least approach it.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And that opens the door to FTC enforcement if there is a contractual violation right?

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

I mean, I don't think we can mandate it by the way that they have a privacy statement, I think we can just suggest it that they put that on their list and then, yes, it does in fact open...FTC can also enforce for unfairness without an affirmative statement that's just a harder prosecution.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

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

So, interestingly...this is Lucia, interesting just a data point for y'all, in early 2013 in conjunction with OCR we published two items one with a model notice of privacy practices that can be downloaded by a small physician practice that resides at OCR's website. It has had upwards of a quarter of a million hits.

We also did the exact same text but in an HTML format so developers could download it and put a notice of privacy practices in their Apps, David McCallie, probably less than 500 hits. And maybe those hits on the HTML document will go up, it's embed in Apple, Apple Healthkits, you know, sort of standards document, but, you know, we do...there is a limit on what we can do when we don't regulate.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Right.

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

And clearly some people really want to do this and some people who have no interest in it whatsoever.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

I will say that the MMA, the Mobile Marketing Association, has a standard basically safe harbor privacy statement for Apps that is utilized fairly widely.

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

Right but it's not healthcare...it's not about health data specifically, right?

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

No it's not.

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

Right.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

But it is about data, no you're correct.

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

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

But, you know, this is David, the other David, to go back to Deven's initial question or someone's question, you know, if there were to be an entity that certified Apps what would they certify against? I mean, I think we're saying that at the moment there is no government role for that so if a private entity wants to take that on one of the things they could do is to evaluate the Apps privacy policy and security policy.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

There are other things as well, but we're basically postulating the emergence of private entities that would take this work on like the MMA.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

I'm sure there are others out there...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Well, you know, this is...now you're echoing and I think this is a great idea too, you're echoing what both the FTC and the White House have done is call for self-governance and so, you know, industry self-governance around how they're going to handle data and, you know, put together a guidance that says, here's how they're going to handle it which then becomes enforceable to your point.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

But there actually...AppTek was an organization that was looking at...was evaluating App software in the health space but I think it might have been for physicians and they got bought by another digital health company at the end of 2014. So, I think its worth...I have to refresh my memory about what happened there.

I mean, we...I think it sounds like what we're coalescing around is a statement that there is value...there still is value to transparency to patients and even so far as telling them, you know, you should be looking for a privacy policy which is clear to you ideally about what happens to the data and if it's not you should consider whether that's a transaction that you want to engage in that there might be some value down the road to someone in the private sector to, you know, create some sort of a registry or certification process for these Apps that addresses the privacy and security risks that we've talked about but there is not one today.

And that absent a security risk to the provider of connecting to a particular App we don't think providers should be making judgement calls about whether what a patient wants to do with that data is appropriate or not.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

The entity that I had in the back of my mind, I couldn't remember the name, but I just looked it up; it's TRUSTe, the small letter "e."

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, yeah, they...right. Stan knows who they are.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Yeah, they actually went for profit about four years ago and spun out an entity called the privacy projects with their non-profit money that TRUSTe has survived as a for profit entity doing things.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right but that's the little certificate that you see on websites right?

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Right, exactly.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Right but they claim to have 5000 business members so whether they're the right one or not those kinds of entities will emerge in this space I think.

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

And this is...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Yes.

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

...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

This is Linda Kloss and might we embellish that recommendation that you framed Deven to also include that this is an opportunity both for Office for Civil Rights to do some additional training materials and an opportunity for providers to reinforce their training, you know, their orientation with patients.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah I think that was part of what we had said originally so it seems worth reinforcing and then John's point from very early on our call about giving guidance to the patient facing space is relevant as well it seems like. I thought I heard another voice trying to come in but it was a little garbled.

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

This is Lucia I was just saying that my understanding is TRUSTe actually had a settlement with the FTC after it spun off for something it represented it was doing that it didn't do, I could be wrong about that, but...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

No you're correct.

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

Yeah, so I'm just...you know, even that is not the be all...that alone is necessary but insufficient right? To have certification the certifier has to actually live up to what they say.

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Right.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Other thoughts on this topic? We're making great progress.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So, Deven just to be clear if such...if these entities do emerge the provider, do they have the ability to...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Do anything other than counsel the patient about it? Can they refuse? Are we asking for changes...I mean, could you broadly interpret the provider could claim if it's not a trusted App it could harm the patient and then use that clause, that reviewable clause about refusing treatment?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

No, but that's...let me just go back to that slide, that's...if we can go to slide 14 please. Harm is articulated in a very specific way here, likely to endanger the life or physical safety.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Okay so much for that idea.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, I think...so, but here's the thing, with access through view, download and transmit or the API functionality of the EHR HIPAA doesn't require that this is the mechanism through which providers make, you know, data available to patients who are trying to exercise their HIPAA rights.

So, while HIPAA has these sort of very clear rules about, you know, if the patient's exercising her right under HIPAA to get data, you know, you have limited ability to say "no" to that, you know, absent the circumstances that we talked about on this call.

But the use of the portal, when a patient is not using it to exercise her HIPAA rights, whether the provider could say "yeah, no not through my portal." I think it's a...it's a little bit of a sticky question, right? Because on the one hand if the patient says the form or format I want is through your portal, just to use the shorthand, and the provider says, well, you know, for that App that's not readily...I don't know how that dynamic would play out and it might be helpful to have some more guidance of the circumstances under which a provider can refuse if the provider is using that EHR functionality as a mechanism for honoring patient's requests for data and the patient may ask for it via that mechanism.

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

And Deven, this is Lucia, just to sort of add some thought to it, right, the way the rule works...one way the rule, the access rule might work right now is the patient might ask for their designated record set and the physician might actually print that designated record set out from their EHR or provide it on some kind of, you know, CD ROM, right, and then the patient has to do something else with it, which could actually be more insecure than supplying it to an appropriate App using API technology and so we just have to think about this is really an important policy point which is what is it we're expecting the collaboration between the physician and the patient to result in?

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Hi, this is Linda Sanches from OCR; this is a really interesting conversation. I mean, we certainly assume, assume is probably not a good word to use when talking about regulations, but, you know, the view, download, transmit capacity is likely to satisfy most of the access needs of many individuals, but you're absolutely right their access right is much larger than that it's to the entire designated record set which may or may not be available via the portal and so that would be something they would need to work out with the covered entity.

I think, it would be...I got a little confused at some point when we were discussing the provider's portal versus other APIs, it seems...are you suggesting Deven that a provider may not be able to use their own portal because of concerns with their own security or...I would assume the API concerns would be with other applications from other entities trying to get...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right, no, no...

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Not their own.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

In terms of security it is the sort of other entity, other vendor connecting in.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Right.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

The vendor of the patient's tool. I'm just thinking of the circumstance where, okay the provider is a Meaningful User, they have either view, download or transmit and the API infrastructure to offer to patients. The patient comes and says "I want to make my App that says...that's called weratedoctors.com; I want it to connect into my EHR and get my discharge summary from the last time that I was there and that's the form or format that I want."

And the doctor doesn't really like that or the hospital doesn't really like that connection, or the doctor doesn't like that connection but let's assume there is no security risk that can be used as an excuse and the patient has requested the form or format for that data that the provider has but doesn't like. Like can they reject in that circumstance if in fact that's going to be the exercise of the HIPAA right. There is I think HIPAA is implicated.

Then you could come up with a sort of a less connected to HIPAA circumstance where, you know, the patient wants to make the connection but hasn't necessarily...isn't asking for it with respect to the exercise of the HIPAA right necessarily.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Yeah these are...I think it's helpful to get specific use cases for us to consider.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

That's useful.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

But if we did those it sounds like there is an appetite for doing some guidance on those specific use cases.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Maybe, you run that through, I'm sorry, I didn't mean to try to pin you down necessarily.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights**

Thank you, Deven.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

I think we could say...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Deven?

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

From a recommendation stand-point that coming up with some use cases like that and requesting some guidance on that would be a valuable exercise for us to do.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

Deven this is Linda and before we run out of time there is one other area that I'd like you to at least think about and that is, is there any guidance available that we could put forward on situations where perhaps a provider is concerned that the request is not really coming from the patient, because, you know, identity theft is becoming such a major issue and this could conceivably be a route for getting protected health information that is going to be used for identity theft and it seems like we at least should acknowledge the need for caution in that regard.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, that's a very good point Linda. I had not...and that is...that's sort of a similar scenario to the one Linda Sanches just raised about, you know, whose security risk are we worried about here.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

It is.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

It may not be a security risk to the provider system and yet it's arguably a security risk for the patient.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And...

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

And our taking the issue of putting in administrative steps and other processes to guard against identity theft through their master person index processes and other things and it seems like this is an area that could become a vulnerable point.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

But, this is David, it's no different than the download capabilities or the transmit capabilities. The APIs would be exposing the same data...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

In a way that's more friendly for programmers but it's the same data that the patient would have exposed by downloading and not taking good care of their C-CDA or whatever else they choose to download or by transmitting to some third-party.

So, it's a risk threshold because we think Apps will be more easy...will be more prevalent, easy and convenient and therefore will get a lot more use than download or transmit did, but nonetheless it's the same technical issue.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

It's the same data, yeah.

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

And Deven, and David, and Linda, this is Lucia, if you go back to the Tiger Team recommendation of requiring or recommending independent confirmation from the patient if that or something was built in, and I'm not saying it will be I'm just connecting the dialogue, that would then satisfy the API causing fraud just like fraudulent person's seeking portal access.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, unless they've programmed the fraudulent API to answer that question in the affirmative by default.

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

Well, you've got...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well the way...

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

To have something in there that shows there is human intervention.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right, right with like a capture or something.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

The way that OAuth works is the portal provides the conversation to capture the authentication from the patient not the App.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So the portal maintains control of that if it's properly implemented.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Is that...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And not the whole...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Part of what's required?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

No that is certainly what the Argonauts are working on and everybody else, that's what Blue Button Plus used, OAuth 2...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

That's just the...that's the way the Internet works, that's the way Facebook works, Twitter, Google Apps it's, you know...you could certainly do it in other ways but one of benefits of the OAuth model is that it maintains control over the actual capture of the authorization in the native App, the portal itself. So, the portal can display whatever confirmatory captures it needs, it feels necessary before returning control to the App with the appropriate secret token that enables the App to actually get the data.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So, that's, you know, by design that way.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, David, that's very helpful. I'm going to...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Maybe we could even recommend that as part of the guidance is that, you know, the authorization...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, let me pause...I want to go right back to the point, but we have to open up the lines.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Oh, yeah.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

So, that we can cue some people up in case there is public comment, so let's do that and then we'll come back to this. So, Michelle or Altarum?

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

Caitlin can you please open the lines? I'll wait for Caitlin.

**Public Comment**

**Caitlin Chastain – Junior Project Manager – Altarum Institute**

Sure, 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 phone and would like to make a public comment, please press \*1 at this time.

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

Deven we do have a comment that was submitted through the comment field so if you want to wrap up then I can share that comment with you all.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay, great and we'll see if anybody else cue's up. So, a few more moments on that OAuth point but we can also pick it back up on our call on Friday.

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

So, Deven, this is Lucia, just extending an offer, we've had a lot of different members of different Workgroups, people have such different skill sets and expertise, we'd be happy to set up informal off line time with some of the technical people in OCP or otherwise to sort of answer questions about things like how does OAuth work and how do APIs work. Trust me I felt stupid and asked stupid questions too, so there is no question that deserves...all questions deserve to be answered of people who are giving us this advice who need some more technical background.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay. I just don't know how much we want to dive into this since we usually take this on as a policy matter, but it feels like something that we might want to tee up for some more policy discussion on our next call. Does that make sense David?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, what...I mean, I'm happy to do a brief summary of the technical things but I agree that that's...the only point is it does raise the question that we could suggest guidance that behavior is for authorization protocols that ensure that the authorizing source actually be directly exposed to the patient and not go through some kind of a hidden App controlled sequence.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

And this is Micky, when we say, request guidance we're just talking about guidance, right?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Right.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

That's all we have.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, I mean, unless we were to recommend some sort of certification aspect to this.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Right or a regulatory if you include another policy lever, which I'm not recommending, I'm concerned about even asking for guidance starts to get us down a slippery slope that we may not want to be jumping onto.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Well, you know, keeping in mind that if a...on the provider end they do have to do a security risk assessment on this aspect of their technology not only for...

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Right...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Meaningful Use...

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Yeah, yeah so I...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

It's also in the security rule.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Right so I wasn't speaking to the security aspect it was related to the comment I made at the very beginning that if we're focused just on privacy and security that's one thing but we've strayed over into a whole bunch of other things that are not about privacy and security.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Like what I thought we've been pretty privacy and security focused?

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Well, yeah, okay, I mean, I guess...well I guess, I mean, the things about what would be constituted as appropriate use so the physician or the provider who is concerned about the patient's use of data for an App that they may or may not, you know, like or find valid.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right, it...

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

That's not...privacy and security issue.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Has implications for the patient access rights which are under HIPAA, which is privacy and security that's why I thought it was still germane.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

Okay. Because we haven't discussed it but you get into issues of licensing intellectual property all the other stuff that...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, yeah, yeah, yeah.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

If you go and look at the Uber API there's 10 million other things in there that aren't...

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Right.

**Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative**

That they're going to come into play here as well.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Yeah, no...well said Micky we don't want to touch any of that. So, okay, recognizing the time we should go to the comments and return to wrap up both of these discussions from last week and this week on Friday.

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

Okay, Deven, so from Mark Underwood from Krypton Brothers he left a fairly long comment so I'm going to read it to the best of my ability. A security consideration, direct EHR to PHR is frequently provided to patients, instead providers are directing patients to print or download PDFs which makes it difficult to transfer data free to a PHR.

Given weak citizen engagement with best security practices and rapid data proliferation during periods of high velocity treatment not having certification at least to an intermediate electronic format for PHR export can be seen as a weaker security/privacy.

For example, not requiring export to HealthVault to name one or an open standard means that movement towards PHR is not only inhibited but there is a de facto encouragement of lower security and even worse lower assurance of data quality.

Information transfer practices, the conversation around API certification does not address this directly since that is developer to developer, App to App, certification could help this but not as PHR management products are not called out.

So, and I will also share this via e-mail with the Chairs so that you can see it.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Oh, that would be great.

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

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Do you want us to react to that or would you rather not?

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

No, it's just public comment so you're not expected to react to it.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Okay.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

We should...can we share it with the rest of the group?

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

Yes.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

And then we can pick up any lingering aspects of that that people want to focus on in the next call. Where there any others?

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

No that's it.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay.

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

And there is no one on the phone either.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Okay, all right well that...if we wanted any evidence about whether the type and functionality for comments was appealing to people we got some because we had a comment that way that was interesting. Okay, we'll get that circulated and we'll have some draft recommendations from the certification NPRM as well as the discussion that we just had and we'll do clean up on all of this on our call on Friday. Thank you all very much.

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

Thanks, Deven.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Look forward to...

**Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP**

Thanks a lot Deven good job.

**Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP**

Talking to you at the end of the week.

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

Thanks, Deven.

**Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.**

All right, thanks.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

Thanks.

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

Talk to you all again on Friday, bye.

**John Wilbanks – Chief Commons Officer – Sage Bionetworks**

Bye.

## **W**

Thank you.

### **Public Comment Received During the Meeting**

1. May wish to site the NIST Special Publication: Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Figure 2 describes a Risk Management Framework which may be helpful to align expectations in regard to mitigating Privacy and Security Risks. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>. Thank you for this opportunity to submit a comment. The above document may be considered as guidance.
2. A security consideration. Direct EHR to PHR is infrequently provided to patients. Instead providers are directing patients to "print" or "download" PDFs, which makes it difficult to transfer data error free to a PHR. Given weak citizen engagement with best security practices, and rapid data proliferation during periods of high velocity treatment, not having certification at least to an intermediate e-format for PHR "export" can be seen as a weaker security / privacy. E.g., not requiring export to Healthvault (to name one) or an open standard means that movement toward PHR is not only inhibited, but there is a de facto encouragement of lower-security, and even worse, lower-assurance (data quality) information transfer practices. The conversation around API cert does not address this directly, since that is developer-developer. App-app certification could help this, but not if PHR-managed products are not called out.