

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
May 8, 2013**

Presentation

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thank you. Good afternoon everybody. This is MacKenzie Robertson in the Office of the National Coordinator for Health IT. This is a meeting of the HIT Policy Committee's Privacy & Security Tiger Team. This is a public call and there is time for public comment built into the end of the agenda. The call is also being recorded, so please make sure you identify yourself when speaking. I'll now go through the roll call. Deven McGraw?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director
Here.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Deven. Paul Egberman?

Paul Egberman – Businessman/Software Entrepreneur
Here.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Paul. Dixie Baker?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I'm here.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Dixie. Judy Faulkner?

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer
Here.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Judy. Leslie Francis?

Leslie Francis, JD, PhD – University of Utah College of Law
Here.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Leslie. Gayle Harrell? John Houston? David McCallie?

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

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Great. Thanks David. Wes Rishel? Micky Tripathi? And Kitt Winter? And any ONC staff members who are on the line, if you could please identify yourself.

Kathryn Marchesini, JD – Office of the National Coordinator

Kathryn Marchesini, ONC.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

Thanks Kathryn.

Joy Pritts, JD – Office of the National Coordinator

Joy Pritts.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

Thanks Joy.

David Holtzman, JD, CIPP/G – Office for Civil Rights

And David Holtzman from OCR.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

Great. Thanks David. And I'll just remind everybody, if you're listening through your computer speakers, if you can just make sure you mute your line so we don't get any echo from the computer on the phone. And with that, I will turn it over to you Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, great. Thank you MacKenzie. Thanks to everyone for joining us on our call, we feel like we just had a call, which we did, just last week. And we are just on – we just had a Policy Committee meeting yesterday, so, we're in a little bit of a compressed time frame here, but I'm glad that you all were able to make it. I welcome the members of the public who are joining us as well. I want to start off by doing a little agenda shifting here. We prepared these materials for you for the call today in anticipation that our recommendations presented to the Policy Committee yesterday, on the last question related to non-targeted queries, and whether we would place any additional limits on them, I think we sort of expected that that would be a relatively quick presentation, and we would be done and we could check the box off on query and move on to something else.

And the Policy Committee would like us to do some more work on the non-targeted query scenario. They were not quite comfortable with coming to a conclusion that no additional policy parameters were needed in a non-targeted query circumstance. They wanted to understand a bit more about how some of these non-targeted query models are working. What particular policies are built into those models? What's the scope of those models? Who's covered by them? What kinds of choices are people provided, is it – are people given an all or nothing choice about whether to be listed in say an aggregator type service, where their records can be found or do they have some more granular choices such as to say, well, yes, this certain – you can list that my records are located with certain providers, but not necessarily with all of them. And so, given the number of questions that arose, we thought it best to wrap up the query discussion for scenarios 1 and 2, as we had for in the previous Policy Committee meeting, and go ahead and complete the letter that goes on the web with those recommendations in it, but to explore the non-targeted query scenario in a bit more detail and come back to the Policy Committee with a report of what we've found and any recommendations that we have based on that more comprehensive look at these models. I know we have others on the phone who were there for the discussion and so certainly, I hope you think I'm characterizing it properly.

We're not going to try to dive into that today, mostly because we had prepared to take something else on already, and we need some time to do some information gathering and reach out to folks in order to prepare ourselves to do a more complete discussion of non-targeted query models, which we would hope to begin really at our next Tiger Team call, which I believe is May 20. One of the suggestions that was made was that we not just do background digging and have staff help us with that, and then present the results, but that we actually invite some people to speak to us about query models that they may have put into place and what they're doing, at our May 20th meeting. It wouldn't be a hearing, it would be more a specific invitation sent to some query models, state HIEs, for example, some vendor query models and then that would enable us to have a discussion with folks, in addition to sort of hearing directly from them some specifics about what they're doing. The other option, of course, is to do what we customarily do when we need to sort of dig in to an issue that we're not going to have a full hearing on, which is to have staff prepare materials for us to review and then we can talk from there.

So I want to get some feedback from you all about how to proceed on th – how you'd like to proceed on this, and then of course also invite others who were present for the discussion who might want to add their 2 cents on what the concerns were that were raised.

Leslie Francis, JD, PhD – University of Utah College of Law

Deven, this is Leslie Francis. I think it would be excellent to hear from additional sources.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah. Thank you Leslie. Yeah, that's my thinking as well, it was – that was actually a specific recommendation that came from Gayle, who's – Gayle Harrell, who's a member of our Tiger Team not on the call today, but nevertheless, I think it was a good idea. And hopefully we'll be able to get a good cross-section of folks lined up to talk to us on our meeting on May 20. So we would essentially devote that meeting to sort of information gathering and questioning and discussing with some of the – with some query model stakeholders and then we'd sort of begin the discussion in earnest on what we learned and what additional policy recommendations we might have, if any, at the meeting that follows that. That would be –

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

This is Dixie, Deven. It would be useful to me, and I know that most people on this call were at the meeting, to better understand what the issue – the core issues they were bringing up. It may be at the beginning of that meeting, you could go into a little bit more – or even maybe we could get the notes from MacKenzie or something.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, we can go back through the transcript. I mean I think I basically summarized it, but at a very high level, admittedly. There were a lot of questions about, well how do these queries actually work. And if you give – if patients are given meaningful choice, what kind of choice does that look like? And what kind of information is del – does someone who sends a query of asking for a locations of a patient's record to an aggregator service, what do they get in return for that? There were just a lot of sort of questions about what – the nuts and bolts of how this stuff works, and the – you juxtapose that against the idea that people have potentially few limits on these queries beyond giving patients choice and people were not quite comfortable with that.

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

Deven –

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

So they really don't – you know, not a lot of non-targeted query is done right now.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Well, and that was the other issue is, we could say nothing as a Policy Committee and the result would be that these things would just grow and be implemented in whatever way that the implementers thought to implement them, consistent with whatever law might apply, and that didn't make people comfortable either. They wanted to understand more about what was going on and it could be that after this deeper dive they say, well, we don't – there isn't anything specific that we see. And we'll be taking the first stab at that, right, after we sort of take a deeper dive into what's out there, we may ultimately say, well, our conclusion is the same as the one we drew before, but maybe we have a better rationale for it this time, based on what we've seen and heard. Or it could be the fact that we see some consistency in approaches that are being taken by other models that we think represent best practices or policies or we see gaps that we want to fill. I think we'll know a bit more after we do a little deeper dive into the environment.

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

Deven, this is David.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Hi David.

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

I think that sounds like a good plan, I just would maybe reiterate that a lot of this is in flux and it's fairly rapidly evolving over the landscape, so you'll need to be prepared to ask for planned and design systems that may not yet be deployed.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

I fully agree. Yeah. What are people thinking in addition to what is working, because I think most of these are evolving.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yup.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

This is Judy and right after the meeting yesterday Deven, someone came up to me and kind of yelling at us – yelling at me for going nationwide and basically doing what they thought was a fishing expedition, which –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Oh, oh my.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

– which was where he was quite uncomfortable. Yeah, I was – I tried to persuade him, and fortunately had a person who worked on this with us there, so she was able to back me up, that in fact we did not do that, it was targeted. But, I think that's the worry that at least this person expressed, which was, it feels like a fishing expedition if you could put in a name and look all over the country.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

And then the other thing, going with what are people doing, targeted, but targeted to a small geographic area, because often the patient doesn't know exactly the name of the clinic, which might have a different name on its door than the organization to which it belongs.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

So, a narrow geographic area around where the person's saying they are.

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

Although, as we've discussed before, there's often urgent need for knowledge when you're not constrained to that geographic area, so –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Well and that's –

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

– that seems like –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

– I mean these are all things we'll have to discuss. But, David, I think your point about asking people to talk about their plans and reaching out to entities that might be still in the planning phases versus just limiting it to existing models, is a good idea.

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

Happy to help.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, great. That's good to know. All right, so what we are going to do today is to try to get through the issue – try to get through our comments on the Request for Comment, which inevitably is preparing us to do recommendations for what we would like to see in Stage 3 of Meaningful Use, and in particular today we're going to drill down on the question of what would we like – what, if anything, do we want people to have to attest to in the area of privacy and security for Meaningful Use Stage 3.

We really got through all of the other comments that had been submitted as part of the Stage 3 RFC, some of them in response to questions that we posed as a Tiger Team, many of them in response to questions that were not posed by us but by other working groups or by ONC. And the wordsmithed answers to those are in your backup slides. As is our custom, we're not going to take time on the call to go through those, but they remain available for you all to provide feedback on. We're not going to present these before June, but I still – if you're going to give me comments on them, I'd like to sort of put that language to rest and ideally, if you could get any wordsmithing comments to me by the end of this week, that would be great. If you need a little more time, just let me know.

But what we decided that we wanted to talk some more about is this quest – is sort of attestation. We know that in Stage 1, eligible professionals and eligible hospitals are required to attest to doing a risk assessment and what's been finalized for Stage 2 is attesting to doing the security risk assessment and to addressing encryption of data at rest and attesting to both of these in the second stage. And we shined the spotlight on those two areas in order to really sort of highlight them, they are existing HIPAA Security Rule obligations but we're using meaningful use not to add to those obligations, but to shine a spotlight on them. And so really the relevant question here is whether we add to that list for Stage 3 or make a shift and emphasize something else and eliminate the first two or whether there would be something in addition.

So, what we did, in order to prepare for this was ask our liaison from the Office for Civil Rights, to pull together a presentation for us on – both on the training requirements in the current HIPAA regulations, both the Privacy Rule and the Security Rule, as well as a summary of what they've been finding in the audits that they've been doing, which can – I think will really help inform our discussion about what we might want to shine a spotlight on for Stage 3. So before I let David take this over and go through his slides, does anybody have any questions about what we're doing? All right, terrific. David, I don't know if they gave you the right to advance your own slides, if they didn't you just shout out and they'll take care of it for you.

David Holtzman, JD, CIPP/G – Office for Civil Rights

I appreciate that and they actually I will, that's something that I could just give the cue to move to the next slide.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

David Holtzman, JD, CIPP/G – Office for Civil Rights

And so, with that –

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

David –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, hold on, somebody – I heard someone in the background

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

Yeah, it's MacKenzie Deven. I just want – we're getting some banging noises that keep coming through the line, so if everyone except David for now could just mute your lines so we can hear him clearly, I would appreciate it. Thanks. Sorry David.

David Holtzman, JD, CIPP/G – Office for Civil Rights

That's all right. Thank you. So right now, we should be on slide 2, and the discussion today is to give you a very high level and heavily abridged overview of what the requirements for the Privacy and Security Rule are for training, on the requirements of the Rules, as well as to give you a very limited abridged version of – an overview of the HITECT Privacy and Security Audit Program. I welcome you to have an opportunity to see the full presentation on the Audit Program, which I believe will be on Tuesday, May 21, in conjunction with our NIST/OCR HIPPA Security Rule Conference, and we're also doing other outreach events. So, I'd like to offer the Tiger Team members an opportunity to hear the full presentation by those who are actually working on it. So, without further ado. So the Privacy, Security and Breach Notification Rules each have a requirement that the covered entity establish policies and procedures that within their organization, would comply with the requirements of the rules and implement them and then train their employees on the policies and procedures they've actually implemented.

So I guess the first take-away is, is that while we think it's important for folks in the healthcare industry, who are affiliated with covered entities in some way, who are workforce members and that's defined in the Administrative Simplification Rule and that workforce member is a very broad definition to include anybody that is given access to protected health information or electronic protected health information, who is not a business associate or contractor. They have to be trained by the organization to – in compliance with the rules. And then the second take-away is that we don't want so much to have that training be focused on the letter of the Rule, it's not so much important what HHS wrote, what's more important is how each and every organization has implemented the rules within their own four walls, and how they want their workforce to conform their behavior and their activities and their administrative processes to comply with the Privacy, Security and Breach Notification Rules that have been adopted by that organization. So broadly the Privacy Rule and Security Rule take different approaches to this goal.

So, under the Privacy Rule, and you'll recall Privacy Rule was developed first and was developed exclusively by a team over at HHS, policy folks. It kind of sets out any administrative safeguard – of the Privacy Rule that covered entities have to train their employees on the policy and procedures that are implemented to comply with the Rule. So, the idea is that the training take place, and it's sort of a first step in the orientation process of the employees. And of course we all remember 10 years ago when we were implementing the Privacy Rule in our various organizations, how we got that first introduction to the requirements of the Privacy Rule. And we allowed and encouraged covered entities to tailor that training to the scope and the actual requirements of the workforce. Some members of the workforce had a greater access to and greater responsibility to protecting the privacy of the health information. So, for example, the administrative – the individual working in administrative office who had limited access to health information would not receive the same scope and depth of training that a physician or a nurse might, who has access to all of the health information. So the level and depth of training was commensurate with the access role or the actual activity that they were engaged in.

The covered entities had to document that they had provided training to their workforce. They didn't have to have certificates or anything like that, but they did have to have some record to show that in fact, training was provided on such and such a day, and this individual was in attendance. And the Privacy Rule doesn't have a specific requirement for retraining that is time – that is relative to time. The requirement for retraining is related to when the organization has in the ruling called “material changes” to their policies and procedures. So if a covered entity, for example, created new divisions or new responsibilities, which required significant change in their policies and procedures, the workforce would be required to be trained on those changes. An example of an expectation of when training should be updated and provided again will be when healthcare providers are updating their policies and procedures for the new Omnibus Rule, which will bring about a number of significant changes to many covered entities as they comply with the new provisions of the rule.

So let's move to slide 3 please. So the Security Rule takes a slightly different approach. First of all, they call it securit – in the Security Rule, it's referred to Security Awareness and Training. It's a standard that's incorporated into the larger Administrative Safeguards area and within that, the Security Management Process area, the same set of standards that discuss as a risk analysis, risk mitigation, access logging, security incident processes and contingency planning. So within this kind of foundation of basic information security practice is the Security Awareness and Training Standard which requires covered entities and now business associates, to train each individual workforce member who is going to have access to EPHI on the organization's policies and procedures, it has implemented to comply with the Security Rule. And the goal is to reduce the risk of improper access, uses and disclosures. Now the approach that the Security Rule takes is two-fold. First of all, as we know, the Security Rule takes an approach, which calls on covered entities and now business associates, to focus its response or to tailor the scope and breadth of its training to the size of complexity of the organization in the information systems that it has.

So, the scope and depth training for a two-or three-physician small practice would probably be – could be considered to be reasonable and appropriate if it were somewhat less sophisticated or less extensive than the training provided to an academic – in an academic medical center setting. By the same token, individuals whose role is somewhat limited in the keeping the confidentiality integrity and availability of the electronic protected health information, their training would be somewhat different than the training that would be provided to, for example, an administrator – a system administrator, someone with the greatest amount of privilege to the information and whose essential role in the organization is to maintain the confidentiality, integrity and availability of the electronic protected health information. Physicians and healthcare providers fall somewhere within that paradigm. We – it's very difficult or, I shouldn't say difficult, we've not taken the position that we are setting specific goals or requirements or benchmarks for what training is provided at what level or at any specific – along the access roles or responsibilities within an organization. It's sort of like a pendulum, you get to – there's one end and there's the other and then of course we have that beautiful middle.

Within the standard for Security Awareness and Training, we have addressable implementation specifications, which as we know are benchmarks that each organization, regardless of their size and complexity, must take steps to implement and to take some approach to satisfy the requirement. But the – their approach is reasonable and appropriate on the size and scope of the organization and they can choose an alternative, as long as it's effective – as effective as the specification that is in the actual Security Rule. So and those addressable implementation specifications real quickly are the 4 that you see laid out here, that there – that is – the goal is to have not so much a one-size fits all training at one point in the process, but to have an initial training when an individual is provided access to electronic protected health information and thereafter to have little bites or updates or reminders. That's why often times you'll see in cafeterias napkin holders with these – little messages about not sharing passwords or don't download apps that you don't know where they came from.

Well, those are actually spelled – those are the actual implementation specifications in the Security Rule. There has to – there should be periodic updates and security reminders. One of the things that should be in those reminders is training people how to guard against malicious software, as well as preventing and monitoring login attempts and having some procedure to report anomaly, and also to train your folks on creating, changing and safeguarding passwords. So I'll stop here and does anybody have any questions about the training standards and requirements?

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

David, these addressable details on this current slide, are they required to be documented and proven to anyone or is this just a duty that you have to do without any reporting?

David Holtzman, JD, CIPP/G – Office for Civil Rights

Sure. As with all activities under the Security Rule, later on in the rule I believe it's 164.316, there is a documentation requirement. So any action that you would take to comply with the rule, you would document. So for example, you would document that you had engaged in this security reminder awareness program and you would keep a copy of the actual activity. It doesn't have to – you don't have to keep an actual copy of the – material, but you should keep some type of documentation of what it was and when you did it.

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

Okay. But it's not required to be displayed to anyone externally, OCR doesn't come and say, show us your documentation for this. It might I guess if it were an audit –

W

Yes.

David Holtzman, JD, CIPP/G – Office for Civil Rights

We have and we do.

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

Okay.

David Holtzman, JD, CIPP/G – Office for Civil Rights

Not so much on audits as we'll discuss in a few minutes, audit is really a special animal. But in compliance reviews and complaint investigations, we generally will ask for documentation of training.

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

Okay. Thank you.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Very helpful David.

David Holtzman, JD, CIPP/G – Office for Civil Rights

All right. So I also want to mention that in Breach Notification Rule there is also a training requirement, but it's not as detailed or extensive as what we have in the Privacy and Security Rules. Simply a mention that an organization must train their employees on Breach Notification requirement, that they've implemented in their organization. Let's move on to the audit. Again, we give a caveat, this is really just a very 10,000-foot view.

So the HITECH Audit Program was implemented, because we were told to by Congress. And, it was an audit program that was – that we worked with a contractor, Booz Allen, who helped us scope out what is it that we want to do and who do we want to audit. So we – so Booz Allen determined that we had approximately 3 million covered entities and we had to figure out some way to group them, so that we could develop an audit plan in which we could categorize it by type of covered entity and then do a review of a representative sample of types of covered entities. And we chose to classify covered entities by size. And one way we measured the size was by how large the organization was and what their revenues were.

And so, as you'll see on slide 4, with the colored boxes, we generally broke out providers in 4 levels. So, if you consider the Level 1 healthcare provider or health plan to be the largest, most complex provider or payer, and the Level 4 would be your smallest healthcare provider and not a payer. So generally your smallest – your small physician practices, your pharmacies and community healthcare providers, who generally have little use or experience with health IT. Probably the folks that we are looking at more often as we are looking at folks who use EHRs are those folks who were Level 4 entities and are now graduating into Level 3. So, moving on to slide 5. We implemented this Audit Program, as you may have heard, I'm sure you heard, we contracted with KPMG to actually go out and work with us, develop an Audit Protocol, Audit Protocol, by the way, is available on OCR's website, and we developed a plan by which to audit a sample group of covered entities, and only covered entities. And we wanted to break down the scope of the 3 main covered entities, we ended up selecting a group of approximately 150.

Now of those, we actually performed audits at 115 locations. Now the sample is a little bit over-weighted to healthcare providers and also over-weighted to level 4 healthcare providers. That was somewhat by accident, and it was also somewhat purposeful. We recognized that the smaller healthcare providers were over-represented or over-weighted in the actual presence in the real world, so we had always intended to have over-representation of smaller healthcare providers. But also, as we went into the audit itself, we found that our identification process had some defects to it and so we ended up contacting organizations that were either not healthcare – that were not covered entities or they were – or we had classified them too high. So we ended up actually doing reviews at more of the smaller providers than had actually been intended.

But – so the audits took place primarily throughout the beginning and the end of 2011 and then throughout the first half of 2012. And we don't have a complete drill down on all of the findings from our audit, but we do have, we believe, some valid takeaways at this point. So our first take-away was that most healthcare providers and plans had some findings. In other words, when we went to measure their compliance with the Privacy and Security Rules, using the protocols, we found that most covered entities, and particularly healthcare providers, at some level had some area of non-compliance. But what we really surprised about that was that of the findings we had, 60 percent were Security Rule findings. Although the Security Rule – the protocol – the Security Rule was only represented as 28 percent of all of the questions.

So we also had some surprising results in that the healthcare providers of all sizes and types were over-weighted in the number of findings that we had. In other words, we found that generally, health plans and healthcare clearinghouses are more likely to demonstrate compliance with the Privacy and Security Rules than healthcare providers. And it was by a significant amount. So 65 percent of the observations were with healthcare providers, even though they represented only about 50 or 60 percent of the total presented – I'm sorry, it's right here in the slide, 53 percent of the actual facilities or organizations that were reviewed. And we found that the smallest healthcare providers, the Level 4 providers are having challenges in Privacy, Security and the Breach Notification – so if you move to slide 7, you'll see a chart of the Privacy Rule Audit findings.

Again, it's a very high-level view here. As you can see, the greatest area in which there were findings were uses and disclosures of PHI. Frankly it's not surprising when you look at the type of complaints that we received at OCR, the majority of complaints we received from consumers are that there's been an unauthorized use and disclosure of protected health information. However, I call your attention to the administrative standards in which the training is found and that was 18 percent of all the findings, and if you flip to the next slide, slide 8, you'll see a pie chart of that 18 percent of findings for administrative safeguards under the Privacy Rule, 26 percent of those findings were for deficient or a failure to train or document the training. It's very difficult, this is really a generalization, we don't have it drilled down at this point of what exactly the training deficiency was and frankly I think the sample is so small, we're not – I don't think that we're going to find much value in trying to identify with any specific measure, what the training deficiency was. So, but general, and then about half of the deficiencies were in not having appropriate or documented policies and procedures.

So let's move to slide 9 and talk about what we found in the measures of the Security Rule. Fifty-eight of 59 providers had a finding under the Security Rule. That was very surprising for us. We did not expect to see that almost 100 percent of healthcare providers would have some non-compliant activity under the Security Rule. And two-thirds of the findings were that there was not an accurate or complete risk analysis. This is something that we had been hearing anecdotally, but this is really surprising as to the depth of non-compliance. And it's really caused us to sit up and take notice and working with our friends at ONC and also soon with our friends at CMS, we're certainly going to be attempting to address and raise awareness on the risk analysis. And also the addressable implementation specifications, there seems to be a lack of both awareness in the smaller providers as well as appropriate action on the larger providers in addressing the addressable implementation specifications.

So moving into the last slide, slide number 10, it's another bar chart, which represents the breadth of the findings under the Security Rule. As you can see, they're pretty evenly spaced out, however, we need to recognize that the protocol did not focus on technical safeguards. It was really difficult and time consuming for our contract auditor to engage in measurement and evaluation of technical safeguards. So what you are seeing here is really an assessment of a protocol that measures primarily the administrative safeguards and some of the physical safeguards, the movement and destruction of media. So, we don't have a specific measure on Security Awareness and Training in the Security Rule protocol. In fact, the protocol itself did not specifically ask or measure Security Awareness and Training; it evaluated the training overall as a part of the Privacy Rule protocol, and unfortunately our protocol was not sophisticated enough to pull out the Security Rule Training.

But it is primarily found in the Security Management Part, which is the risk analysis and the Security Incident Procedures, are the two areas where we would find the Training and Security Awareness and as you can see, it's pretty much, as we had found, that it's – that generally the covered entities are having difficulty complying with the Security Rule or not taking appropriate measures to comply with the Security Rule and training is one of those issues that is in the milieu of areas that requires further attention by covered entities. And we think that without – unless we begin highlighting this as a part of our overall approach and outreach to our new family of business associates who will be complying with the Security Rule, we think it will be a lost opportunity to not highlight the importance of Security Awareness and Training. So with that, I'll answer any questions about –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Thank you so much David. Questions for him.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

David, this is Wes Rishel. On your slide 9, which is 13 in the composite deck that we got, you've got these three panels and I'm having difficulty parsing the sentence in the right hand panel, "Almost every entity without a finding or observation met by fully implementing the addressable specification." Does that mean that the material that you reviewed did not have the necessary finding to show that they implemented the addressable specification – I just don't understand what it says.

David Holtzman, JD, CIPP/G – Office for Civil Rights

You know, now that I read it, I'm not sure I understand it either.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Well, I'm not alone.

David Holtzman, JD, CIPP/G – Office for Civil Rights

So I think the word without should be with, "almost every entity with a finding or observation –"

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Then "met not fully implementing the addressable specification."

David Holtzman, JD, CIPP/G – Office for Civil Rights

Yes. I apologize. I'm going to be completely transparent here, I lifted these slides from someone else's presentation.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Yeah, and that was – that's the larger presentation that you mentioned at the start of your talk?

David Holtzman, JD, CIPP/G – Office for Civil Rights

Yes. Linda Sanches and Verne Rinker, who are the leaders of our Audit Team, are generally those folks who present on the Audit Program, and we ha – so most recently, we had these presentations at IAPP and at HCCA and we're going to be doing a presentation on Tuesday, May 21.

Paul Egerman – Businessman/Software Entrepreneur

And this is Paul. I just wanted to say that we did ask David to present on very short notice, and he said he would just have to use somebody else's slides, so, just want to make sure people know that.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Oh, that's no problem, I'm just wondering if the deck is now publically accessible somewhere?

David Holtzman, JD, CIPP/G – Office for Civil Rights

We haven't posted the deck, but it is – we've used this deck a number of times and I have no hesitation in sending you the deck, but I think – I do encourage you, if you have the opportunity, to listen to Linda or Verne as they make the presentation. They certainly have a familiarity with both the conduct of the program and the res – let me say that the results portion of this is a work in progress. We have data, what we are doing now is we have hired a contractor to help us evaluate the validity of the data, both in the effectiveness and value of the protocol and the effectiveness and value of the audit reports and observations. And we hope that by the end of the calendar year, we will have been able to develop a complete report that will give us valid data and also give us some direction on what flaws are in the protocol that we could fix for any future Audit Programs that we – that OCR chooses to implement.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

So I'm sure that we'd all like to see the final deck, I know I would. I mean the current, most complete deck.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yeah.

David Holtzman, JD, CIPP/G – Office for Civil Rights

I will send that to MacKenzie and she can distribute it to you.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Thank you.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Thanks.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

This is Dixie David. Thank you very much for this, I think it's really enlightening to say the very least. What really, really bothers me tremendously is the risk – is that people aren't doing risk analysis. I know that the HIMSS survey has found this for years, but it would look like the meaningful use addition or attestation would have increased the number of risk assessments being done. But what bothers me most is that risk assessment is at the heart of the Security Rule and what makes the Security Rule really current as technology changes. So it really bothers me that they're not doing that. And on the other hand, I do recall that several years ago we did a – the Security and Privacy Workgroup did a hearing where testifier after testifier kept saying, tell us what to do and we'll do it. I mean, I think that they are calling out for being prescriptive and yet at the same time they seem to push back against when regulations become overly prescriptive. But when they don't do risk assessment, do you know how they explain – are they doing it because they don't know what it is? Do they not understand how to do it? Do they not understand the importance of it in security in an organization? What, I would love to get to the bottom of that.

David Holtzman, JD, CIPP/G – Office for Civil Rights

Well. First of all I cannot support or oppose the first part of the statement, but I'm glad you said it. The second, as to the drill down, I don't think we captured the anecdotal reasons for the non-compliance. I think that would be found in the individual reports, and please excuse me if I tell you that purposely OCR put up a wall between the folks who were working on the Audit Program and the folks who work on Enforcement, because we had said all along, that we are not using the Audit Program as a lever or a club to – Enforcement. And so, I honestly have not seen those reports, but I will pass along the suggestion that it might be helpful to develop some type of analysis of that feedback that we got from the covered entities.

I can tell you in my experience in doing the Enforcement work, the smaller covered entities truly have a gap of – I don't want to say awareness, but a gap of what is expected of them. And it's a challenge both in implementation, but also in policy, and I want to thank Joy and her team for partnering with us in exploring ways to develop tools that will hopefully bridge that gap.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Can I – may I follow up on one thing David that Dixie asked, that I think is more of a timing question. And that is, when did these audits take place versus when did some of the Stage 2 attestation timing – the time for attestation. I mean, because I don't know that we can conclude that that attestation requirement hasn't had any impact without sort of understanding when these audits were done.

Paul Egerman – Businessman/Software Entrepreneur

And this is Paul can you hear me?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Not very well Paul.

Paul Egerman – Businessman/Software Entrepreneur

It's just that most of the Level 4 providers do not have EHR systems in this survey, it's important to know, so it's surveying people without EHRs for Level 4 providers.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Deven I think you meant to ask about Stage 1 certification.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, so I'm sorry, I did admit to ask about the timing in Stage 1 when we talked about attestation requirements around the Security Risk Assessment. I'm sort of testing the notion that we can conclude that that didn't work based on this audit data, from a timing perspective. Paul Egerman is asking about whether Level 4 entities that are small are even using EHRs, I presume some – they're not subject to the Security Rule unless they have electronic PHI.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yeah. And they have – problem here.

David Holtzman, JD, CIPP/G – Office for Civil Rights

Sure. So, let me approach this in a couple of ways. First of all, all of the Security Rule – the Security Rule Protocol would only have been applied if the covered entity was or had electronic information systems that handled the PHI. However, the information systems could or could not be EHRs, they could be desktop computers that had Word programs with billing and patient records –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yup.

David Holtzman, JD, CIPP/G – Office for Civil Rights

– or they were EHRs, we didn't measure for that. And secondly, we did not – purposely we did not align this with any type of participation in the meaningful use program. It was almost – it was akin to don't ask and don't tell, and so we didn't measure that. My suggestion is that you talk to my colleague, Elizabeth Holland at CMS, who can share with you their findings of their recent I guess preliminary or pilot audit of attestation for meaningful use. And I think she can appropriately and more clearly share with you findings that would address your question.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

But what was the – can you just answer me what the timing was for when you audited these organizations?

David Holtzman, JD, CIPP/G – Office for Civil Rights

Oh sure. I'm so sorry Deven.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

David Holtzman, JD, CIPP/G – Office for Civil Rights

The audit took place primarily – the substantial part of the audit took place during the first, I'm sorry, I said first, during the March to December timeframe of 2012.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

David Holtzman, JD, CIPP/G – Office for Civil Rights

So the bulk of the audits were done in the summer and the fall of 2012, so these observations are less than a year old and after the time that the Meaningful – Stage 1 of Meaningful Use was in effect. However, I want to emphasize again, we did not measure, nor did we ask, about meaningful use intent of Program participation.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. Yeah, I didn't expect that you did, I was just trying to link up the timeframes. But the suggestion to talk to Elizabeth is a good idea. Thank you.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yeah, thank you.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Any other questions for David before we launch into some discussion? Okay, so we didn't tee up any straw language here. We had initially proposed that we would, in fact, do – aim for a third attestation measure that would focus on training. We did not, at that point, sort of differentiate between Privacy – the type of training that's required under the Privacy Rule versus the training requirements under the Security Rule and we wanted to sort of see, with a little bit more detail, what some of the top level results were on the Audit, before having that discussion. So now I think we have a lot more information to play with.

I'm as – I don't know if awestruck is even the right word. The results that are on the screen now where you know, Security Rule deficiencies seem to still be a major issue, and not just with respect to risk assessment, but other areas, too, seems to suggest that it's yet another area where we might want to shine a spotlight, and there is the awareness in training requirement in the Security Rule that might be a candidate. But I want to hear what folks think. We did not straw person on this one.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Well, this is Dixie again. I'd like us to think about making the risk assessment measurable, such as, percentage of the risks identified that were addressed or something, just to make it more – other than – something more than just, yes, I did it.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

But wouldn't that percentage of risk, wouldn't that require – the percentage they identified versus the ones they actually have?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

No, how many they closed – and I was just using that as an example, but I think it would be worthwhile to explore the idea of coming up with a way to measure that they did the risk assessment and addressed the risks identified. And so I said, for example, it would be the number of risks closed or addressed over the number of risks identified, which would make it measurable.

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

This is David. I have a question down a different angle of thinking. And I'm wondering, and David Holtzman, these are sort of process measures of quality, are you doing the things that are supposed to be helpful in getting the desired outcome. I'm wondering if you have done, if OCR or anyone, has done any actual outcome assessments to try to identify which processes and policies had the most useful impact on preventing inappropriate disclosures or breach or whatever your outcome measure points are? It would obviously help us to target that.

David Holtzman, JD, CIPP/G – Office for Civil Rights

That's a great question and I think – I don't think we approached it with that level of sophistication. I think the best that we are able to do is, we are preparing a small set of best practices. And those best practices, frankly I think were about clarity as opposed to – clarity and thoroughness as opposed to outcomes, because we've not aligned the experience of an entity with their success or lack of success in the Audit Program. In other words, we've not taken the results of the audit and measured it up versus, for example, the – report or how many complaints they've received and I think your suggestion is an excellent one, but I think it will be a little bit far down the road before we develop that sophistication.

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

Thanks.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

This is Judy and I too am surprised by how much people aren't really following what they need to do and I think right away as I look at it, a lot of these organizations have good people in them, is there something that they would say if we were talking with them about where they think the assessment – the risk assessment that they're being evaluated on maybe isn't the right one, or maybe they do it differently or maybe they say that there's never any danger that it's not as real as we may think it is or – in other words, what's the root cause of this?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yeah.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Judy, I think – this is Wes. I think that's an excellent question, although I think a lot of them would say the root cause is a lack of attention from teak alley.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

And it may be, it's just, is that it or do we have to go down another level to ask them are we looking at the right things?

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Judy, this is Joy Pritts and my staff works really closely with the RECs, so they've been able to get at least a little bit of insight on this issue, from the small provider perspective –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

Um hmm.

Joy Pritts, JD – Office of the National Coordinator

– and what they hear kind of repeatedly is that they're just so overwhelmed by the process that they don't know where to start.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

Okay. So, it's not that they're really disagreeing with it or feel that they have other ways, it's truly they're over their heads.

Joy Pritts, JD – Office of the National Coordinator

Yeah. Well, that's what we're hearing from the RECs and some of the – we've also had some discussions with some of the people who we call movers, the people who are in the vanguard of meaningful use and what they – these are small providers themselves, not the RECs and what they've encountered with some of the people that they are working with. But part of what it is is that they're looking for a checklist, and you know, doing a security analysis is not a checklist. And so it's just even hard to get them to understand that that you need to look at your own situation and assess it. And a list isn't – it can help, but it's not really what they need to be doing.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

You now, that's a really interesting thing. You've probably Atul Gawande's books, or heard him talk and –

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Yes.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

– his checklist manifesto and really complex things they reduce to checklists. That's the reason air travel is safe, of course. And we have, at EPIC, done a number of things now with checklists. Originally we thought we couldn't and then we did and I wonder whether we should give more thought to even though it seems to be a very difficult task, have a checklist where maybe some of the checklist, the way they do it could vary, but it still is on the checklist.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

I –

David Holtzman, JD, CIPP/G – Office for Civil Rights

So, this is David. I'd like to – because this is OCRs bailiwick. We caution that the Security Rule as it has been designed and it has been implemented both in policy and in practicality, has been done so in a way to make the approach almost individualized and that was frankly at the request of the healthcare industry. They did not want a one-size fits all Security Rule or security requirements and the challenge is that when you develop a checklist or take an approach of a checklist, generally a checklist is engineered to be a one-size fits all approach. And so, there is some danger in that the checklist will not be strict enough or not apply a rigorous enough standard or the checklist will require a standard that's too rigorous for some covered entities as opposed to others.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

Could you give an example or two?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I want to actually take us out of this deep dive into the checklist issue for a second, only because I want to remind folks a bit about where we sit vis-à-vis the Security Rule and the relationship of meaningful use to the Security Rule and the prev – and what CMS, as essentially the regulator who makes the final determination on meaningful use objectives has previously stated about the relationship between HIPAA, the regulations and what they're willing to do in meaningful use. And one thing that they've been very clear about is that they do not want to use the meaningful use program as another policeman for compliance with the Security Rule. They have been willing to highlight a few existing Security Rule provisions, in their current form, as a mechanism of shining a spotlight and a way to put some emphasis on Privacy and Security in the meaningful use program. But I do not see how us sort of diving into building a better mousetrap on compliance with the intricate – in some detail of the Security Rule is ever going to pass muster with either the Policy Committee or with CMS. So it feels like it's not a productive use of our time to necessarily be considering a recommendation that essentially we couldn't get enacted.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

Yeah, I think we –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

And that sure makes sense, I mean, we don't even have an apparatus at the regulatory level in the meaningful use program that could make judgment calls on this.

Judy Faulkner, MS – EPIC Systems – Founder and Chief Executive Officer

I don't disagree with you Deven. In my mind it left meaningful use and it went just simply to how do we help these folks.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, it did. But then hence the reason why I'm trying to focus us on the topic – the thing that we can solve, is if there's something else we want to shine a spotlight on.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Deven I think, I understand your refocusing and agree, but I think there's a general observation here that may be useful to us, which is that whatever we're talking about probably looked very different at the level of practices that are aided by RECs and ICs and the larger organizations and it may be hard to come up with a unified approach.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah, no, I mean I don't disagree with that at all, or any of the points that have been made, I'm just trying to steer us in a direction of something that's within our purview to recommend.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Good job, herd the tigers.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

This is Dixie and I would draw Wes' attention to the slide that clearly says that 47 or 59 providers didn't do risk assessment, which says to be we're not talking about just Level 4, we're talking about all levels. And I, for one, would be for strengthening the meaningful use requirement for risk assessment or maybe making it more succinct or maybe taking – using some of the ideas Judy mentioned, rather than adding additional burden. Because I think adding additional things to it is only going to water down what's there.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems

Hmm.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Well at a minimum I would say that the notion of dropping risk assessment in favor of another item sounds premature.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Good point Wes. Okay. You won't – agreed. But I too am – have my eyes wide open on that risk assessment figure Dixie, but I'm struggling with what else with meaningful use tools we could do to elevate the attention on it, to have it done more consistently and I think I worry that just a mere reiteration of it –

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yeah – we need to refine it.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

But in what way?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

I don't know. Maybe we need a smaller group to just figure –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Well that's not –

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

I'm going to make a radical proposition here. I mean, just personal experience, my wife has a friend who's a nurse at our local community hospital who basically shuts up when I come into the room because she knows I do something about HIPAA somewhere.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I have that problem too.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

She stops talking about work, right. And this is a small hospital and I am not sure that training, it's the lack of training rather than the quality of training that is the issue, at least until you get down to the REC level –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Right.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

– and I'm not sure whether we have an instrument that's not – I mean, our instruments are pretty blunt here, in terms of getting to the quality of training or the degree that it's matched to the actual policies implemented in an organization, that seems like a pretty difficult thing to measure. So, I am tending to feel that we should either just decline to add something to Stage 3 or look for some way, given our – that policy is the skilled use of blunt instruments, we should look for some way to create more attention – shine a brighter light or a more focused light on security assessments.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

I like the sound of that Wes. I mean, we're not – I'll do another check-in with folks on the timing of when we need to bring forward our final recommendations to the Policy Committee for a Meaningful Use Stage 3 discussion, but my recollection is we have some time here. Does anybody from staff want to correct me on that?

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

This is MacKenzie Deven. Meaningful use is planning to do an update in August and then do their final in September. So, if you want to sync up with them, you have time.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

If not, I mean, if you want to do it earlier, then there would obviously be the July Policy Committee meeting.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay. So, here's a thought. We have time on this. And there's been desire expressed to try to do some more deeper thinking on what we might do to shine a brighter spotlight on this risk assessment issue and tackle it a little better, even given the blunt instruments that we have. And I personally like the idea of sort of gathering a small group of folks together who want to help dive into this. I'll take any volunteers who want to fess up on the call that they'd be willing – that they'd like to be involved in that exercise. The process would be, of course, that the small group would report their findings or make some recommendations to the Tiger Team and then we would consider all of that in whatever we would decide to put before the Policy Committee. And again, we have some time on this. We wouldn't even ask you to report back by May 20, because I think we want to start digging into this non-targeted query model issue then. But we could be doing a couple of things simultaneously. How does that sound?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Yes.

Wes Rishel – Gartner, Incorporated – Vice President & Distinguished Analyst

Good.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Okay, then that's what we'll do and we'll aim to spend some time in June, whether it's at our first June meeting or our second June meeting, coming back to this question after we've done a little digging. I am very interested in trying to think creatively about what we might be able to do here, it sounded like Dixie was as well. Other folks can either chime in now or just send me an email and we'll get some help from staff and the MITRE team too. And we will do the outreach to CMS as well on what they've been doing to look at audits of meaningful use, if they are in a position where they can share some of those results, it might be interesting to learn that. We can talk to the RECs

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Is that – is Elizabeth CMS?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner

Oh good, good. I can –

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

So I think that that's how we'll handle this. And this has been a really good discussion everyone, I think. And David thank you – Holtzman, thank you very much for this information. Our eyes are wide open now. What we're going to do about that, we're not quite sure, but we're going to see if there's something more creative we can do. Does anybody else have any thoughts on this that they want to chime in on before we move to public comment.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

So Deven, this is MacKenzie. I just wanted to make sure I have it straight. Are we going to go ahead and pursue a transmittal letter with the first two scenarios definitely?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yes.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

And then wait on the third?

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

Yes. And we actually had already begun to work on a draft of that with MITRE MacKenzie, so if you want to – we'll send that to you, unless you would prefer to write one yourself.

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

No, that's fine, you can just send me a draft.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

We'll do that. Any other thoughts from team members? All right. Thank you everyone. Great call. We'll – MacKenzie, you want to open up for public comment?

Public Comment

MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act Program Lead

Sure. Operator, can you please open the line for public comment?

Caitlin Collins – Project Coordinator, Altarum Institute

If you are on the phone and would like to make a public comment please press *1 at this time. 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. We do not have any comment at this time.

Deven McGraw, JD, MPH – Center for Democracy & Technology – Director

All right. Terrific. Thanks everyone, have a good rest of your day and talk to you in a couple of weeks.

**MacKenzie Robertson – Office of the National Coordinator – Federal Advisory Committee Act
Program Lead**

Thanks Deven and Paul. Thanks everybody.