

**HIT Privacy and Security Tiger Team**  
**Final Transcript**  
**March 19, 2012**

**Presentation**

**W**

All right, go ahead, Laura.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Good afternoon. This is Laura Rosas from the Office of the National Coordinator for Health IT, in for Joy Pritts. This is a meeting of the HIT Policy Committee's Privacy and Security Tiger Team, and I'll begin by doing the roll call. Deven McGraw?

**Deven McGraw – Center for Democracy & Technology – Director**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

**Paul Egerman – Software Entrepreneur**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Dixie Baker?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I'm here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Alice Leader?

**Alice Leader**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Sam Callahan?

**Sam Callahan**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Neil Calman? Carol Diamond?

**Rebekah Rockwood – Markle Foundation – Manager, Health**

This is Rebekah Rockwood. I'm joining for Carol.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Judy Faulkner?

**Judy Faulkner – Epic Systems – Founder**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Leslie Francis? Gayle Harrell?

**Gayle Harrell – Florida – House of Representatives**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

John Houston?

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

David Lansky? David McCallie?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Vern Rinker?

**Vern Rinker**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Wes Rishel?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Here.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Micky Tripathi? Latanya Sweeney? Okay, Joy Pritts will be joining the call later, and I'll give it back to Deven and Paul.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, go ahead, Paul.

**Paul Egerman – Software Entrepreneur**

Thank you very much. This is Paul Egerman. I want to say good afternoon or good morning to you and welcome you to our Privacy and Security Tiger Team. This is a group of individuals who are participating with the HIT Policy Committee and the HIT Standards Committee that meets periodically to give recommendations to those committees and ultimately to the National Coordinator. This meeting is a public meeting and I also want to be sure to welcome any members of the public who may be listening on the telephone or through the Internet. At the end of the meeting we will have an opportunity for public comment. Those public comments are extremely important to us, and so if you have any observations or reflections please be sure to make them to us at the end of the meeting.

Today's topic is extremely important. As you may know, as many people in the industry know, there has been recently issued a Notice of Proposed Rule Making, NPRM, related to Stage 2 of Meaningful Use, and what we will be doing today and in subsequent meetings is basically reviewing that NPRM. We will be talking about what is in the NPRM as it relates to the recommendations and discussions that this Tiger Team previously had, and what we will also be doing then is after we've had those discussions we will be making recommendations that will be carried forward to the HIT Policy Committee. We can't guarantee that there will be any recommendations, but I have a suspicion that we will have some recommendations. Basically the NPRM did accept many of the comments or recommendations that this Tiger Team and the Policy Committee and the Standards Committee previously made and so there are reasons to feel very good about our previous work. But there are also some areas where there are perhaps some ambiguities

or some places where our recommendations were not accepted that are important for us to discuss. That is what we'll be talking about today. Do you have any comments, Deven? Would you like to proceed?

**Deven McGraw – Center for Democracy & Technology – Director**

I think we can get started, although I may need some help advancing the slides. I'm pressing on the little arrow, I'm technologically deficient today, so can the folks from Altarum advance the slides for me?

**M**

Sure.

**Deven McGraw – Center for Democracy & Technology – Director**

Thank you. What slide do you have on your screen?

**Paul Egerman – Software Entrepreneur**

We have number three, "Scope of Discussion and Time Frames ..." –

**Deven McGraw – Center for Democracy & Technology – Director**

Thank you very much. It's not showing up on my screen, so I'll follow along in the paper. As Paul indicated, we have two rule makings that came out that are related to upcoming Stage 2, and they are proposed rule makings and they deal with both what are the meaningful use objectives that providers and hospitals are going to have to meet, as well as what are the technical specifications that need to be in the certified EHRs. And you'll see from this timeline that the MITRE folks did for us that we have this meeting today and another meeting on the 28<sup>th</sup>, and then there is a Health IT Policy Committee meeting on the 4<sup>th</sup> where we will be able to present any conclusions that we are able to reach as a Tiger Team either on this call or on the next call, but we also have a couple more meetings in April and another Health IT Policy Committee meeting on May 2<sup>nd</sup> that will allow us to bat cleanup on these issues and continue to talk about them.

In addition, potentially there is the Advanced Notice of Proposed Rule Making on Nationwide Health Information Network governance that may be released during the time period and we may need to use some of those meetings to begin talking about that rule as well. But of course we won't really know until that comes out, and we don't have any advanced notice of when it's coming. We will use the meetings that we have to get through the material in the two rule makings, which is pretty considerable. Next slide, please.

As Paul mentioned, our goal ultimately in our meetings is to reach agreement on comments that we want to suggest to the Policy Committee be provided on the proposed rules. Next slide.

As Paul mentioned, we have some victories here, and this is important and worth celebrating, I think. The recommendations that we provided, again, all of which were adopted by the Policy Committee dealing with the security risk assessment and the spotlight on addressing encryption at rest were adopted. Most of what we said on amendments was also adopted, and also most of what we said with respect to the patient portal or what's also been called as the view, download, and transmit functionality that's part of Meaningful Use Stage 2 also were adopted, but there were some that were not, and this is not an exclusive list here on the slide. The recommendation that we had on digital certificates, and specifically that certified EHR technology be tested for being able to accept digital certificates, was not part of the certification rule. Also, some of what we said on authentication for patient portals was not included in the rule, and again, it's not an exclusive list, but essentially as we go through each of our recommendations that were relevant to Stage 2 and talk about whether they were incorporated in either proposed rule making, we've done this in the order of taking the victory lap first, so we'll go through the things that we think were successfully included in the proposed rules and then we'll get to the material that we think was not dealt with, either not dealt with at all or not fully incorporated. So we'll get to that in some more detail.

And then there were some other issues that were not directly relevant to recommendations we made to Stage 2 but do have a bearing on Privacy and Security that we would like to talk about, in particular the changed approach proposed for Stage 2 with respect to whether certified EHR modules need to

demonstrate all of the privacy and security functionalities as part of certification. The approach that's being recommended for Stage 2 is different than in Stage 1 and also we think different from what the Standards Committee has recommended.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Deven, this is Dixie. I guess you know that the Privacy and Security Workgroup did recommend directly that each EHR module not be certified against all of the security requirements because ideally what you want is centralized, uniform security enforcement, security policy, and security capabilities across an enterprise. You don't want each EHR module doing its own thing. So that change was a direct response to our recommendations.

**Deven McGraw – Center for Democracy & Technology – Director**

Thank you for pointing that out. When we get to that in these slides I definitely would like for you to chime in on both helping me out with an explanation of what is the proposed new approach, but also providing some feedback on how consistent you think that is with what the Standards Committee recommended. Because one of the things that's going to be a little bit tricky for us as a Tiger Team to navigate is that we, by design, have both members of the Policy Committee and the Standards Committee and members of both the Privacy and Security working group of the Policy Committee and the Standards Committee in one Tiger Team so that we can benefit from one another's expertise. But ultimately this Tiger Team reports to the Policy Committee, whereas, the Privacy and Security working group of standards reports to the Standards Committee, and while we're all better served when our advice to ONC can be as consistent as possible and when the policy pieces and the technical pieces are informing one another, I think we also want to be careful to stay on the policy side with respect to our recommendations versus opining specifically on technical standards. But I think we'll be, again, very well served as we parse through this discussion in having the expertise in both camps, and, Dixie, I'll definitely look to you to help us understand where the Standards Committee came down on that issue.

The way that we're going to try to do this call today, which is a 90 minute call, a little bit shorter than our usual, is to first at least get through the explanation of what's in the two proposed rules as compared with what the Policy Committee, and on occasion what the Standards Committee had recommended. Rather than chunking this up into a discussion starting to discuss what our recommendations might be for each of these sections of the proposed rules, Paul and I are suggesting that we just initially get through an explanation of what we think and a collective agreement and all being on the same page about what we think is in the proposed rules as compared to what our recommendations were, and then start to go back through what we might want our recommendations to the Policy Committee to look like. That way we make sure that everyone is on the same page. I suspect that some of us have read these rules in detail but probably others of us on the phone haven't really had a chance to do that, and before we can really begin meaningful discussion as a group we think it makes sense for us at least all to be on the same page. Does that sound like a good way to proceed?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, terrific. All right, then we'll go to slide six, where again we're starting with our victory lap here and talking about the pieces dealing with the security risk analysis and the spotlight of encryption. This is a combination of how the Meaningful Use Stage 2 proposed rule approaches this, as well as the certification standards for Stage 2. Our recommendation requiring that the risk analysis that was required in Stage 1 also be continued in Stage 2 was adopted and similarly our recommendation that providers and hospitals address encryption for data at rest, not require encryption across the board but data at rest, but attest that they have addressed it consistent with the HIPAA security rule, including data in data centers and data in mobile devices. And in fact one of the things that is included in the certification rule is a demonstration of the capability to encrypt data in mobile devices when those devices are managed by the EHR technology if in fact the data remains stored on the device when it's turned off. Our recommendations with respect to requiring this focus on encryption of data at rest were included, and there was a little bit of additional emphasis in the certification proposed rule on making sure that the

encryption capabilities are extended to mobile devices when those devices are managed by the certified EHR technology. So I'm going to pause here to see if anybody has any questions or is disputing my explanation. These are long proposed rules, so I want to make sure that we've got it right here. But does anybody have any questions or think that I didn't explain this correctly?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

This is Wes. I have a question. The way I read the rule it says address in the sense that a HIPAA security standard is addressable, so it's not a mandate for requirement for encryption at risk of all devices involved in the EHR; instead it's a mandate to decide which, and a strong hint that if you decide it's not necessary for portable devices you're in deep doo-doo.

**Deven McGraw – Center for Democracy & Technology – Director**

Well, it's definitely not a mandate, and like any implementation specification that's addressable under the security rule if you decide not to adopt it you need to document that decision, and I'm sure Vern will correct me if I'm stating this, and deploy something else that will protect the physical security of the data that is ideally at least as effective, and again, documenting all of that. Vern, did I do okay with that, or did I completely screw that up?

**Vern Rinker**

No, that's accurate.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, thanks.

**Paul Egerman – Software Entrepreneur**

This is Paul. I think that Wes' comment is also correct, though, in terms of his summary.

**M**

Yes, and just for background –

**Deven McGraw – Center for Democracy & Technology – Director**

The deep part, again, it's –

**Paul Egerman – Software Entrepreneur**

I think he was just describing a metaphor or something.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Oh, the deep part?

**Deven McGraw – Center for Democracy & Technology – Director**

The doo-doo part.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

It could be a metaphor, but the important thing is that the distinction that we discussed in prior times about the difference between the data storage that supports the servers that are locked down in an operation center and the relative risks associated with devices that are carried outside of the fortress merit a different security analysis as opposed to a single approach to all devices.

**Paul Egerman – Software Entrepreneur**

Yes, and I think that's what's captured in the NPRM and I think that was also what we said in our recommendations.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I think so. There have been some people who have read the NPRM differently, but I think you're –

**Paul Egerman – Software Entrepreneur**

Well, it's an interesting issue. This could end up being one of the more controversial issues, because I think people will completely misunderstand what it says. But you actually did a great summary of it, Wes, and I have to say I'm really pleased with ONC and CMS for including this, because this is clearly where there's been confusion and it's actually something where we need to improve things.

**Deven McGraw – Center for Democracy & Technology – Director**

Does anybody else have any questions?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, I do. This is Dixie. The NPRM actually says not only to perform a security risk analysis and address encryption, but it also says "and implement security updates as necessary to correct efficiencies," and I don't see that on your chart.

**Deven McGraw – Center for Democracy & Technology – Director**

That's a good point, Dixie. We tried to do a little shorthand here. It's the same security risk analysis that was required for Stage 1.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I think they added, and I could be wrong, but I think they –

**Deven McGraw – Center for Democracy & Technology – Director**

I think it's exactly the same. You had to do updates and address deficiencies in Stage 1 as well.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, so the only thing they added was address encryption.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay. Well, I think that's an important piece, not just to do the security risk assessment but to implement the security updates.

**Deven McGraw – Center for Democracy & Technology – Director**

Point well taken, we'll add that back into the chart.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, thank you.

**Deven McGraw – Center for Democracy & Technology – Director**

Any other questions?

**Paul Egerman – Software Entrepreneur**

My only comment is, this is a point where we ought to be doing a virtual fist pump or something, a victory lap, because this is a complicated issue and our recommendations were accepted.

**Deven McGraw – Center for Democracy & Technology – Director**

So noted, we'll put that in the minutes. Let's move to the next slide, please. And I can finally view the slides on my screen. Here's another fist pump for my technical capabilities. On the issue of amendments, you may recall that we had a fair number of recommendations here that focused a lot on the capability of the technology to help providers comply with HIPAA and be able to respond to patient requests for amendment and to be able to move amendments or appended data if there was a dispute about data initiated by a patient forward to other providers. And we focused largely on what the HIPAA privacy rule already requires, but had some additional pieces to our recommendations as well, again,

including making amendments to a patient's health information in a manner consistent with their legal medical record obligations and again the ability to append.

Now, meaningful use doesn't really address this, because this is already a legal requirement that's going to apply through the HIPAA privacy rule. Mostly this was about making sure that the EHRs in certification have the capability to do this, and as you can see we got adopted in the proposed certification rule a requirement that users can electronically amend a patient's health record to reflect the original information but to clearly show the amendment, to append patient supplied information either in free text or scanned directly to a patient's record, or by embedding an electronic link and then enabling a user to electronically append a response. This is all, again, part of what's required to respond to an amendment request from a patient in HIPAA. And then here HHS actually asks for a comment on whether the technology should be required to be capable of appending patient supplied information in both free text or scanned format, or really only in one or the other, and when we get to that discussion phase we can talk about that. But in general we did get what we asked for included in the certification rule. Next slide.

The other piece of our recommendations on amendment dealt with the ability to then transmit amendment updates and/or the appended information to other providers to whom the data had been previously transmitted, and this was not addressed in the certification rule. So this may also be something that we may want to tee up for a specific comment, either to be addressed in this Stage 2 or in Stage 3. That, I'm going to stop here because those are all of the recommendations that we made on amendments and an explanation of what we got in either the certification rule or meaningful use rule. And so this one is one that we got 80% of the way there for what we asked for, but there still was a piece that was missing. Does anybody have any questions?

**Gayle Harrell – Florida – House of Representatives**

Deven, this is Gayle. Do we have any idea why they chose not to do that? I was surprised by that, tremendously, because certainly the additional information could be critical to anyone who has those records.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, it's interesting. Well, there's a lot in Stage 2 that really ups the ante on requiring the actual exchange of data and some fairly specific exchange requirements in Meaningful Use with respect to transitions of care and the use of a particular standard format, the consolidated CDA, for exchanging information about a patient for continuity of care or in care transitions. So certainly you could foresee that if the CCD is an update from a previously sent version, but that's not really an amendment, so I'm not sure, and I would open it up to maybe the standards members to see if this was a topic of discussion at the Standards Committee, or if you have any idea why this might not have been ready for primetime.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

This is David. I don't recall the specific discussions, but there's a tremendous amount of technical complexity to do this and an absence of widely supported standards to do it. So it may simply be a complexity issue, something that gets deferred to a later stage.

**Deven McGraw – Center for Democracy & Technology – Director**

All right, well let's put that in the queue for some later discussions, Gayle, and it may be that we need to do some inquiry off line before the next call to see, although David's explanation sounds consistent with my understanding as well.

**Gayle Harrell – Florida – House of Representatives**

Thanks.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay. Any other questions? The next set of recommendations deal with what we're calling patient portals but they're referred to in Stage 2 of the proposed Meaningful Use rule as the patient view, download, and transmit capability. There are a number of recommendations that we had around patient portals, in fact, these really take up the next five or six slides, so I'm just going to try to go through all of

them and then we can go back and address questions and make sure that I explained it properly. Initially, and we're on slide nine, we recommended that EHR technology have audit trails in these patient portals and be able to provide these to patients on request. And in the certification rules ONC has proposed that the EHR technology be certified to include a patient accessible log that tracks the use of the view, download, and transmit capabilities, and so we consider this recommendation to have been adopted.

The second recommendation is one where we said patient portals should include mechanisms that ensure that information in the portal can be securely downloaded to a third party authorized by patients. And what ONC said in the certification rule in response is that while they did not feel that they needed to include this as a specific additional certification criteria because of the technical implementations for secure download, and there are two transport standards for transporting data outside of an institution or a practice that are included in the proposed certification rule and that are in this document, that in terms of specifically requiring the certified EHR technology to demonstrate the secure download, ONC sensed that the technical implementation that we recommended was commonplace and ubiquitous and there would therefore be little value by adding these as criteria that would have to be demonstrated as part of certification. So this is something that we may want to talk about when we get to the discussion phase.

The third recommendation in the portal area is that patient portals have appropriate provisions for data provenance which can be accessible to the user, which in most cases would be the patient, both with respect to access and upon download, although actually the provenance would need to be able to be seen by anybody who the patient transmitted the data to as well. And here there are in fact some data provenance elements that are part of the consolidated CDA that I talked about just a moment ago, and so here we thought it looks like the recommendation was adopted, because there are data provenance elements that are included in the CDA, which is a document that the patient will have access to through the portal and will be able to download and transmit, a patient can download and transmit herself or she can ask for it to be directly transmitted to a third party. I think what kept us from doing the full-fledged fist pump on this one was that it wasn't entirely clear to us that the patient would be able to view the provenance data elements, but that may be an easily cleared up technical question.

The next recommendation on portals that was dealt with in one way or another in the rule is that we had said as a policy committee that certified EHRs should have a capability to detect and block programmatic attacks, or attacks from known or unauthorized persons, and this is with respect to unauthorized access to the portal versus unauthorized access to the provider or hospital EHR. This was one where the Standards Committee took a different view on whether this would be something that should be in the technology, concluding that the objective or measure did not align well with today's security technology and that we ought to reconsider this objective as something that should be guidance or good practice rather than one to be implemented and tested directly and certified EHR technology. I'm looking forward to hearing more from our standards colleagues about this during the discussion phase because I think that will be very helpful for us in understanding what would be the best recommendation that we could make here.

Still, on portals here's another one, we recommended that providers at least require a user name and password for authenticating patients for accessing the portal, and that this would be a minimum and that providers who want to should be able to offer patients additional security or potentially provide additional security for sensitive data. And here the Standards Committee also opined on this and in the certification proposed rule, though, what ONC said was that they did not include these additional capabilities in the proposed rule because, again, this is another one where they felt that the technical implementations are commonplace and ubiquitous and so there would be little value added to requiring them to be demonstrated as specific certification criteria.

Another one to talk about, and this is our last one on portals and this was our set of best practices on providing guidance to patients on how to use the view and download functionality appropriately. We specifically did not ask for this to be included in certification, nor did we recommend that it be part of meaningful use, but instead it was more of an overarching recommendation to ONC to put this out as a best practice. And there is a mention of it in the commentary on meaningful use for hospitals, but it doesn't really get very much emphasis here. And so one of the things we might want to consider is

whether there are some additional recommendations that we might want to make to ONC outside of the proposed rules that are currently on the table about how best to get this guidance out. So that's where we are for portals, and I'm going to stop and take a breath and see if I need to be corrected in any of my statements about what's in these rules, or if people have any questions.

All right, you all are following the rules very well today. It's hard not to talk about these immediately after summarizing them, but we just have a few more to get through. The next couple of slides deal with our – I need us to be on slide 14, please, there we go – our recommendations on patient matching, and specifically we had a lot of recommendations on patient matching that were not specifically targeted to the meaningful use or certification rules. But the ones that were targeted to certification are the ones that we really highlighted here, and primarily they dealt with ensuring that there were standard formats for the demographic data fields that are commonly used to match patients. Similarly, what should be the standard response when data is missing? Should there be U.S. Postal Service normalization to improve matching accuracy, and should that be added to the demographic standards? And then the last one on here is ensuring that in fact EHRs are tested to ensure that the transactions can be sent and received with the correct demographic data formats and that data entry sequences exist to reject values that are incorrectly entered. And what happened in the certification rule is that, and it took us a little bit of time to ferret this out, but essentially the consolidated CDA prescribes standard formats for the demographic data fields –

**M**

Excuse me. The slides are dancing around on various things. Can we get it to the page you're talking about?

**Deven McGraw – Center for Democracy & Technology – Director**

I'm sorry. We should be on slide 14.

**M**

Okay.

**M**

We're on slide 14 –

**Deven McGraw – Center for Democracy & Technology – Director**

Okay. So we're on slide 14 and where we, at least in our initial conclusions, and this is Paul and me with some assistance from the folks at MITRE who provide us with some backup, but we would love to get feedback on whether we're analyzed this right. But we have taken a look at the consolidated CDA and think that in fact our recommendations on standard formats for data fields use and matching are part of what is required in the document header for the consolidated CDA. Now, ONC has requested public comment on whether they should require that the technology actually be able to perform some type of demographic matching or verification between the patient that's in the EHR technology and the summary of care record that comes in as part of a care transition, or as part of coordinated care. It almost looked to me like what they were suggesting was should we test the ability of certified EHRs to be able to almost automatically perform the match of the patient record based on the demographic values in the CDA, so definitely something that I want to understand what they might be proposing here, whether we think it's possible.

Now I'm on slide 15, so with respect to our recommendations about standards, to specify how missing demographic data should be represented during exchange, the consolidated CDA does prescribe a series of null flavors, which I thought was an interesting way to refer to this, to designate missing information. And then there are some examples provided here in the matrix: NI for "No Information," and ASKU for "Asked but not Known." But whether this is as complete a recommendation, I see the MITRE folks helped us with this chart, these null flavors may be used to address the required fields but are not necessarily required to, and our recommendation, I recall, was tilted more towards requiring some standardization with respect to representation of missing data. With respect to our recommendation on USPS

normalization, in the consolidated CDA they do prescribe standards for entering addresses and zip codes, but it does not appear that they specifically took up our recommendation that there be normalization to USPS standards. But perhaps we're satisfied with the standardization of addresses and zip codes in the consolidated CDA and don't think that normalization is necessarily needed.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Question?

**Deven McGraw – Center for Democracy & Technology – Director**

And then with respect to this last one on 15 that certification criteria include testing of the sending and receiving of demographic data formats, it wasn't specifically addressed. So I'm certain that I probably messed this up. And I can hear Wes already in the background, so I'm going to stop here and call on him.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

You're awfully apologetic for a lawyer, Deven.

**Deven McGraw – Center for Democracy & Technology – Director**

Some of this is so new for me that I want to make sure that our understandings of what's in these rules is both right and commonly agreed to among ourselves.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes. So the top line, which has to do with the null flavors, null flavors are a term of Art in HL7 for explaining why missing data isn't there.

**Deven McGraw – Center for Democracy & Technology – Director**

Right.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

And the specific recommendations, just reading the words, it says "specify how missing demographic data should be represented," well, the null flavors do fulfill that requirement. I guess the question that's being raised, implied in MITRE is that it's treated as a best practice, the term "may," as italicized here, is a term of Art meaning it's a recommendation or a best practice rather than an absolute requirement. So if we have an issue it's do we want to be moved up to an absolute requirement, or do we want some allowance for judgment on the part of implementers. The corresponding problem is that people tend to certify for the least complex possible behavior rather than the best practice behavior.

**Deven McGraw – Center for Democracy & Technology – Director**

Right, so I think when we get to the discussion phase of this, assuming that folks don't have any additional questions, is in general do we think that the demographic values in the consolidated CDA do essentially incorporate the recommendations that we had on standardization of demographic data fields to enhance the probabilities of an accurate match? Or, did the certification criteria not quite go far enough, such as, for example, by not requiring the systems to be tested to accept these fields and to reject incorrectly entered fields, which might mean if you didn't use one of the null flavors and it was just blank that it might get rejected? But we should talk about that. I personally think this is kind of a confusing area, but does anybody else have any questions before we move on to the last two areas that we need to get through before we can throw this open?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Deven, I'll ask it now, it's a broad question and it may be relevant now, and maybe it should be deferred until later, but I think in our discussions way back when we made some of these recommendations, the ANPRM about metadata wrappers had circulated and was being collected, and I think some of the questions that you're asking here I think we've assumed would be addressed in metadata governance, or metadata ruling, which obviously has not happened yet. So I wonder if some of this is just being deferred until later, for example, digital signature of transmitted documents to prove they haven't been tampered

with, that's not mentioned, I think we discussed that, and there are some other things that were part of that metadata work.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

David, this is Dixie. We asked Steve that before and he said, the question that we asked, to be more specific, we specifically asked him would there be another NPRM on the metadata following on for the ... ANPRM, or whatever it was that came out before, and he said that the metadata would be incorporated into this rule. So I don't think there's a plan to have something in addition, he said, to metadata, and in fact it has been incorporated into this rule because the metadata recommendation was CDA headers.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Okay, but that doesn't address everything that was in the metadata like the digital signature and so forth.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

You're right. You're right. But I don't think, based on what they've told us so far, I don't think they're planning a separate metadata ruling.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Thanks, I had forgotten that.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, well that is good to know. Thank you, Dixie, for that information. All right, well we'll move on and we'll finish up the explanation of what's in the rule and then we can jump to the discussions. Can we go to slide 16, please?

Here was the one that I referred to earlier about the EHR modules potentially no longer being required in Stage 2 to each individually demonstrate that they can satisfy all of the privacy and security certification criteria, and that's what was part of Stage 1 rule, if it was impractical for them to have a certain privacy and security functionality or any of the functionalities and they could demonstrate that to the certifiers, or if they were part of a bundle of certified modules that made up one complete EHR and the privacy and security elements were taken care of by another module, that was another way that they could be excused from demonstrating the capabilities for all of the privacy and security functionalities. But they've proposed something different for Stage 2 and it sounds like it's more consistent with what the Standards Committee had suggested that they do, which is largely what they've said in Stage 2, is that the EHR modules do not have to demonstrate compliance with the privacy and security certification requirements that would apply to a complete EHR.

Now, there is a new concept in Stage 2 for certification, which is that base EHR, which is not necessarily a complete EHR but which has the required functionalities that all providers and hospitals must meet in order to receive their meaningful use payment, that base EHR payment does have to fulfill all of the privacy and security requirements required in certification. It's just additional modular technologies that you might purchase to enable you to meet a meaningful use criteria that might be applicable to functionalities that you need that are not necessarily part of the base EHR, although I must confess that I don't fully understand what is required to be in a base EHR since my reading of the rule says that the vendors can declare that they have a base EHR but I may have just completely missed something. So I want to pause for a moment and let Dixie chime in on what the Standards Committee had to say about this piece and whether the certification rule essentially adopts what the Standards Committee recommended.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Well, you've quoted there exactly what we recommended and the Privacy and Security Workgroup hasn't really reviewed this.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

So I really can't –

**Deven McGraw – Center for Democracy & Technology – Director**

Okay.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

But I certainly didn't come with the – I was just looking it up – I didn't have the impression that they just exempted the EHR modules. Let me explain the thinking behind what we recommended was that in an enterprise you don't want each application to separately implement security, authentication, and access controls individually. You prefer that each application would call a service, a common service so that security policy would be enforced consistently across applications instead of different mechanisms and different policies within each application. So that's what we were trying to get to. Before when they were certifying every module against every single security criterion they were basically coming up with sub-minimal solutions because they were encouraging this separation. We have not, as a team, discussed what they actually recommended.

**Paul Egerman – Software Entrepreneur**

Yes, and this is Paul. There's also a complicated certification issue for complete EHR systems that may be impacting this, if I can say this right, but a lot of people when they buy modular systems the way they'll do it is they'll buy a complete system from the vendor and they'll use everything except one module, for example, so everything, say, except emergency department, and the catch-22 that people came up with in Stage 1, which is that they bought a complete system and did not use the emergency department module of that complete system then the rest of the system really wasn't certified, because you can't really make it a set of modules because each module under Stage 1 had to have individual certification for security purposes, so it became somewhat awkward for the complete vendors who were trying to figure out how they can really get their systems certified. And so I don't know if I explained that in a clear way, but I have a feeling that certification issue also impacted this decision.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Actually that exact point was brought up at our standards meeting and Steve responded that that particular complication wasn't addressed. That challenge still exists.

**Deven McGraw – Center for Democracy & Technology – Director**

All right, well we'll be coming back to this one, I suspect, but we have two more slides to get through. Next slide, please, slide 17. On ePrescribing of controlled substances what we had said was that you're going to have eligible providers that are going to need to comply with the DEA rule regarding ePrescribing of controlled substances, and so therefore the certification testing criteria should include testing for compliance with the DEA authentication rule, which requires actually two factor not addressed in certification, and in Meaningful Use Stage 2 what they said was that there are still some challenges with respect to some more restrictive state law and the widespread availability of products that include the type of functionalities that are required by the DEA regs. And actually I'm surprised, this may be in certification and not in meaningful use, but between the two rules what ONC said was they didn't feel that this was ready to include as a requirement in certified EHRs, but they did encourage comments on the current and expected availability of these products and whether this could be required, I guess, in either Stage 2 or Stage 3.

Then slide 18, next slide, please, our recommendations on digital certificates, which we had a number of them, but relevant to these proposed rules we said that for certification, well, one, we said they should be EPs, eligible providers and eligible hospitals should be required to obtain digital certificates in order to effectively do secure exchange and that the certification process should include testing on the use of digital certificates for appropriate transactions, and this issue was not addressed in either rule.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Deven?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Again, I may be going too detailed, but I think the standards addressed for exchange, the specific standards, require the use of certificates embedded in the standard itself. So maybe it's incorporated by being embedded in the standard.

**Deven McGraw – Center for Democracy & Technology – Director**

Oh, in one of the two transport standards, is that what you're saying?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Right.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

For example, direct requires a digital signature on both parties, it's an organizational signature not an individual signature, but that was acceptable to all the parties that discussed it. And likewise exchange, the way you validate that you're connecting to a legitimate exchange node is through a certificate based verification step.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay, David, well, that's really helpful, because I clearly did not catch that. But if we think that that recommendation is essentially picked up by the adoption of the two transport standards, which are SNTP S/MIME and SOAP, right?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes, and more exactly the profiles that are specified on how to use SNTP S/MIME – well, SOAP is another question, let me put that off to the side because I think there's a problem with the way they wrote the reg on that, but let's just focus on direct for a second. The document that is cited specifically about direct includes a specification of how you must use a digital certificate organization identity. Dixie, are you comfortable with what I'm saying?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes. But what I'm thinking, David, is that having a digital certificate is one thing, validating the certificate and making sure that it's still current is something else that I don't think is incorporated in the standards.

**Paul Egerman – Software Entrepreneur**

Dixie and David, here's the way to look at this part of the presentation on digital certificates. What we're trying to understand is, is this a topic that we need to tee up for discussion for this group?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I think so. I think that the question of whether an EHR needs to validate a certificate before they can actually establish the connection or authenticate the entity, or whatever they're using it for, I think that that really is a policy question, as to whether they need to validate that, because the standards say you have to have the capability to check it, but the policy piece of it is do you have to check it, and then what do you do? That's –

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

To your question, Paul, I agree that we can discuss it. I'm not trying to say we shouldn't discuss it.

**Paul Egerman – Software Entrepreneur**

Okay, I'm just trying to understand whether or not what's written here is either accurate or ... accurate, it may not be worded exactly correctly, and that this is a topic that we need to discuss further because it perhaps may not have been addressed to the extent that we had expected, or we would have liked.

**Deven McGraw – Center for Democracy & Technology – Director**

Right. And we have it on the matrix as not being addressed at all, so David provided some helpful information then that we –

**Paul Egerman – Software Entrepreneur**

... information that may be addressed more than we realize.

**Deven McGraw – Center for Democracy & Technology – Director**

More than we realize, but maybe not as far as we may ultimately want to go, which is why we'll put it in the discussion queue.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, I think David responded directly and correctly to this question of whether this recommendation should be required to obtain. Yes, that's embedded in those standards. I think the policy question is, then what? Do you have to validate its currency? Those are the policy questions.

**Paul Egerman – Software Entrepreneur**

Okay, so those are helpful comments.

**Deven McGraw – Center for Democracy & Technology – Director**

Those are very helpful. All right, well we are at the end of our lengthy explanation of what we thought was in these proposed rules as compared to what we asked or recommended that ONC do, either as part of Meaningful Use or as part of certification, or in a combination of both. So I'm going to suggest that we just go back and work through these issues and see if there's something that we want to comment on and get as far as we can in the time that we have left before we need to break for public comment, and then we'll pick back up again at our meeting on the 28<sup>th</sup>. So if we can go to slide six.

**Paul Egerman – Software Entrepreneur**

Deven, the next slide, which shows ... right now, said "Other Issues."

**Deven McGraw – Center for Democracy & Technology – Director**

Oh yes, I didn't think we had any.

**Paul Egerman – Software Entrepreneur**

The question is do we want to ask the Tiger Team members if they had any other issues that they want to add to the agenda before we start going through these.

**Deven McGraw – Center for Democracy & Technology – Director**

Good point, Paul, thank you.

**Paul Egerman – Software Entrepreneur**

In other words, for those of you, probably most of you who have read the NPRM, are there any other issues that you would like this Tiger Team to address that we haven't gone through so far?

**Deven McGraw – Center for Democracy & Technology – Director**

All right, well, that's a relief –

**Paul Egerman – Software Entrepreneur**

Yes –

**Deven McGraw – Center for Democracy & Technology – Director**

... because I think we have a lot –

**Paul Egerman – Software Entrepreneur**

Okay, so we have a lot.

**Deven McGraw – Center for Democracy & Technology – Director**

... to discuss. Okay, let's then go to slide six. Thank you, Paul. This is the one where Paul suggested we take a fist pump, I called it a victory lap, again, this is related to the issue of the requirement to conduct a review of security risk analysis, and as Dixie pointed out, we'll add in the pieces that we didn't put on the summary slide, and that is to do updates and address any deficiencies that are identified as part of the risk analysis, and then similarly the recommendation that you have to address encryption and security functionalities for data at rest, including data located in data centers and data in mobile devices, and for each of these providers and hospitals attest that they have done so in order to meet their meaningful use requirement. And then related to that on the certification side, which we didn't cover as well on the chart, is the demonstration that the encryption capabilities extend to mobile devices when those devices are managed by the EHR technology and there is data that will remain stored on the device when it's not in use or turned off.

Is anybody uncomfortable with at least saying thank you for doing this, we pat you on the back, we think this is the right thing to do, obviously better phrased than that, but did anybody have any concerns about this or think that we needed to add something in recommendations? All right, well, that's terrific. So let's move to slide seven.

These next two slides are the ones dealing with amendment, and here, again, it's really wholly dealt with in certification and there are proposed requirements to certify EHR technology to ensure that information can be amended, that patients can submit information in the event of a dispute that can then be appended to the data, either in free text ... or in embedded links, and then of course if there's a subsequent response to the patient's appended information that that all can be included in the data that's in the EHR. And then subsequently we had a recommendation that those amendments be able to be transmitted, that piece was the one that was accepted, and then we have a specific comment that HHS is requesting on whether the technology should be capable of appending the information in both free text and scanned format, where really only one of these is a choice of the vendor. Gayle had already chimed in that she thought that the capability of being able to transmit the, I think we called it propagating the amendments and the appended information when we were having this discussion with the Policy Committee, that that capability was an important one but some uncertainties expressed by David on whether the technical capacity and the required accepted standards for doing that were in place.

So I'm just going to open it up for a discussion about what we might want to comment on in this area. For example, the basic question that HHS has asked, should the EHR technology be required to be capable of appending information in both free text or scanned format, or can the vendor choose one?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

It's not like me to express an opinion, but –

**Deven McGraw – Center for Democracy & Technology – Director**

Well, I was hoping somebody would. It was a little quiet out there.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes. I felt like I had to fill the void here.

**Deven McGraw – Center for Democracy & Technology – Director**

Everybody's on mute.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Right, yes, all shouting on muted phones probably. I would argue that we want to enable, if not require, that people be able to enter their proposed corrections through patient portals. Scanned or faxed documents is not the most convenient way to do that, whereas, typing into a text box in the portal and having that text be recorded with the electronic health record is. On the other hand, the workflow where someone sends a record to an eligible provider or an eligible hospital, sends a letter to an eligible

provider, an eligible hospital, is also an important workflow and therefore I would regard our recommendation as being we should support both.

**Deven McGraw – Center for Democracy & Technology – Director**

That sounds good to me.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

This is David. I think the complexity of supporting attachment of a scanned document to an existing document in the EHR system is pretty high. I don't know how widespread vendor capability is to do that, but it's certainly non-trivial to support a variety of scanning approaches and then embed that scanned data in a hard linked fashion to the document. I don't know exactly how our team feels about it, not that that matters, I'm just not sure. I just know that there's a fair amount of complexity there. So requiring it does have some significant cost. It may be costs that most people have already accounted for, but that to me is less of a difficult issue than the notion of notifying people downstream that the document has been amended. And in some cases that's not too complicated, if the physician knows that he's pushed a copy to someone he can just push the amended copy, but in an HIE like setting where an unknown number of people may have accessed it and downloaded their own copy of it into their own EHRs, keeping track of all of that would be quite challenging technically and that may be why that wasn't a part of what they required.

**Paul Egerman – Software Entrepreneur**

What you're saying right now, David, is they've delivered the scope to this one question that shows up on page 26 was it should be scanned format and patient supplied, or only one, and you're suggesting only one, did I hear you right?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Paul, I'm not ready to make a strong suggestion. I'm just registering that scanned is non-trivial. None of it's trivial, so maybe that's a moot point. I've asked internally for comments on this and I just haven't gotten them back yet, so I need to just sit tight for a while.

**Judy Faulkner – Epic Systems – Founder**

This is Judy. I asked internally too, and I did get some back, and the feedback I got was that both are okay to do and that there's going to be things that are going to come through in scans, such as a letter, that you're just going to want to add and that it's okay if the EMRs do support both. And the comment was made that they think a lot of the EMRs already do support both, so it might not be that hard, David.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes, I suspect that's the case. I'm uncomfortable knowing if the ability to support a scanned letter can be seamlessly and forever attached to the document that it's modifying, or if the letter just stands as a separate document. That's a technical detail I'm just not sure about yet. I assume they can be linked, but I'm not positive.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

This is Wes. Is the HIPAA requirement really narrowed down to just specific documents? As far as I know the requirement is, I think there's something wrong in my EHR and I have to be able to dispute it, not I think there's something wrong in a patient's summary and I have to be able to dispute it.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

This is John Houston. I think there are two issues at play here. One, I think that there's the technical correction, which I think is covered, A, under certification, which it sounds like we still need to be electronically able to update the information so that it's technically accurate; and B, really deals with the patient's views or perspectives on that mistake and whether there needs to be a rebuttal by the patient if the clinician doesn't agree with the patient's request. So I guess the question is, if we simply deal with A in terms of communicating A we're at least ensuring that the patient's information is accurate. So I guess then the other question is, okay, then if the patient doesn't believe that they still want rebuttal information

communicated, I guess that's less important to me in terms of ensuring quality of care because the clinician's already said that any changes are reflected in A, if that makes sense.

**Deven McGraw – Center for Democracy & Technology – Director**

Well, right, but, John, the way that we formulated the recommendation was to make sure that the EHRs have the technical capability to essentially allow providers to comply with their HIPAA privacy rule recommendations, which does require them to append data in the event of a dispute and then send it along to providers that they may have sent that data to. So we're not opining on whether we care or not about whether that can happen. It has to happen. And so our recommendation was that this technology ought to support that. And I think the question on the table was whether EHRs need to be able to demonstrate in certification two different ways to append data, in both free text and scanned format, or only one. And then I think the second question on the table is what if anything do we want to say about their being a certification criteria in either Stage 2 or Stage 3 about the ability to transmit this to providers that you know have received it.

**Paul Egerman – Software Entrepreneur**

And that's a good explanation, Deven. We're narrowing our discussion right now to should there be two methods, text and scanning, should we be requiring that in order to make amendments. In other words, can a patient come in and say, gee, here's some data, some test report or a letter or something that should be in my record that's not in the record, and in which case you scan it and you include it somewhere in the record. How you transmit it is a different issue. It's really an issue of required scanning, because presumably everyone can do the text stuff.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes, I think this is tantamount to requiring scanning, but it's hard to imagine a system that doesn't require scanning.

**Paul Egerman – Software Entrepreneur**

To put it a little more succinctly, required storage of a scanned something, document.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

You're talking about the state of healthcare IT today, Paul.

**Paul Egerman – Software Entrepreneur**

Yes. That's the question then. The sense I have is everybody is somewhat tentatively saying, yes, it should be both. Is that correct?

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Yes, from here too.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes, for the narrow point you've raised, yes, I think this discussion has hit on some other issues that may be valid for discussion.

**Paul Egerman – Software Entrepreneur**

Yes, when we get to transmitting them then it's a lot –

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

By the way, Paul, I apologize because I have ... on the brain right now so I was thinking of the transition side of things. My apology.

**Paul Egerman – Software Entrepreneur**

Well, the transmission is definitely a thornier issue.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

John also recognized the difference between a correction that's entered as a result of a patient dispute and a simple acknowledgement of the patient dispute, whereas, the decision is made not to correct it. When it comes to the state of having transmitted this information, there's a whole bunch of complexities around was the information sent in this document or that document, how many different documents did I send out that might have had this information that wasn't corrected, how many of those that I sent out were replicated and forwarded, there's a whole bunch of issues around the transmission part.

**Paul Egerman – Software Entrepreneur**

Yes, it's a thornier issue. But I think we have resolution, at least, of this question on this slide.

**M**

Yes.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, I think so too. And we can go back and revisit it the next meeting if folks hear otherwise from their colleagues or if we get something in public comment that makes us want to pick this one up again. But based on the knowledge that our Tiger Team members have today on our call it sounds like we're comfortable with both. But on the third question of transmission, let me –

**Paul Egerman – Software Entrepreneur**

Doesn't that come up in the next slide?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, it does, so we can go to the next slide, please. What we do have in Stage 2 for both meaningful use and certification are a requirement to transmit this summary of care document in the form of the consolidated CDA. How hard would it be if there was information on that CDA that needed to be updated to send a revised one that had the new information in it, and to have some data appended to that CDA if it's in fact one of those circumstances where there's a patient dispute about something in the CDA. Because the exchange requirements in Stage 2 are very much focused on the exchange of this consolidated CDA document, right?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I guess I just want to raise the issue that the documents, the various ways that data is transmitted, the CCD versus an op note, versus something other, don't represent the way the data is held in the EHR, at least we would hope that the EHR has a central store of data that is what they know about the patient and they package it up to produce various documents and send it out according to ... documents. So let's take a case where due to a patient protest we decided that the patient's not paranoid schizophrenic, they're mildly schizophrenic, that's a change in a problem, and it's a correction as opposed to an alteration, then there is the potential for the EHR having to know how many different documents it transmitted that information in and to whom they were transmitted, and let's leave it there. You can make it even more complex by saying and who might have retrieved the document as opposed to whom it was transmitted, but let's at least start with that. Is that a strong requirement on the EHR to be able to know which different documents were impacted by this correction or would have been impacted if the correction had been accepted?

**Deven McGraw – Center for Democracy & Technology – Director**

So it sounds to me that the technical issue that you all are raising is not one of whether there's a capability of transmitting an amendment or an appended piece of information, when you know a provider to whom you have previously sent it. It sounds to me that the requirement is you have to send it out to everyone you've sent it to even if you don't know who it is.

**Judy Faulkner – Epic Systems – Founder**

This is Judy. You can get some interesting recursion there, so A sends to B and C with interoperability; B and C sends to D and E and F and G; and let's say B and G also send it back to A, so you can see them going round and round.

**Deven McGraw – Center for Democracy & Technology – Director**

Right. But I'm trying to tease apart – what I hear is two issues, and I may be wrong about this. One is the issue of who got the original document that has either an error or the disagreement in it that we may now need to send a correction to, and the identification of where all those reception points might need to be, which may be impossible to know even with a really good audit trail.

**Paul Egerman – Software Entrepreneur**

Right.

**Deven McGraw – Center for Democracy & Technology – Director**

Versus the second issue, which is when you do know can you get the new information to the recipient in one way or another? And we may be able to dispose of the problematic part of the former if in fact what the privacy rule requires is send it to people that you know you already sent it to.

**Paul Egerman – Software Entrepreneur**

Right. But, Deven, I think Judy's comment is a good one, because either you pick up on Wes' example, where the amendment is they're changing something from moderate to mild, you send that downstream, and somebody downstream says no, it's not mild, it really was moderate, and then goes ahead and sends it back. It's sort of like what happens right now where you get these firestorm e-mails where everybody seems to want to say to everybody else something that is like you can't quite figure out what they're saying.

**Deven McGraw – Center for Democracy & Technology – Director**

Right, but I think we may be –

**Paul Egerman – Software Entrepreneur**

And you can't even keep up with the volume of e-mails.

**Deven McGraw – Center for Democracy & Technology – Director**

Right. And I'm not disputing that that is incredibly complicated, but I think we confined our recommendations to just what's required to be done in the privacy rule, and I'm not sure it scopes out that far.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

That definitely bears looking into, that is at this point now we're beginning to argue about facts. But it wouldn't be the first case that a requirement in the privacy rule, which sounded good in general, created difficulties in implementation. However, I do want to just make sure that we recognize that we cannot simply discuss this in terms of a document, that it really is in terms of data which may be encompassed in more than one document. We also may want to look at the current practices with regards to sending lab data, because there are a lot of pretty formal requirements with regard to updates there, and I think, and I'm speculating, that they're based on the order. So if so-and-so ordered this with a copy to such-and-such and you have an amendment, then you need to send it to who ordered it and to such-and-such. But that's different than saying, well, we don't know who such-and-such sent it to but we need to follow up. Is there an obligation, we're talking about a new obligation, which is dealing with an inbound correction from a third party source now, what's the obligation to forward that?

**Deven McGraw – Center for Democracy & Technology – Director**

All right, so I'm going to use the prerogative of the chair because we are running low on time.

**W**

Yes, five minutes, I've got to open the lines.

**Deven McGraw – Center for Democracy & Technology – Director**

But I think one of the things that we'll do is to investigate just what the current legal obligation is, because I think that we were very careful in how we put policy recommendations forward on amendments, and I

think it may be that that just didn't get reflected in the slide where we were attempting to be a summary. So we'll investigate that so that we can tee up this question with a little bit more focus.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

Deven?

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, but it's got to be quick, John. We've got to get to the comments.

**John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security**

This is basically to Wes' point. We're sort of throwing data over the fence here and I think we need to deal with the other side of the fence even before you talk about forwarding it to some other source, how is it managed, how does a provider even expect to have to insert the data into the receiving record, and how does a provider even know what to do with data once it's thrown over the fence at it?

**Gayle Harrell – Florida – House of Representatives**

Now, I just want to add that this is patient provided data, not the common facts from the different providers. We're talking about only patient provided data.

**Deven McGraw – Center for Democracy & Technology – Director**

That's correct. Thank you, Gayle. We have to move into public comment, so let's pause and let them open up the lines.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Operator, would you open the lines for public comment, please?

**Operator**

Sure. One second, please.

**Laura Rosas – Office of the Chief Privacy Officer, ONC**

Thank you.

**Operator**

(Instructions given.) We have one call.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay.

**Operator**

Carol Bickford, your line is open.

**Carol Bickford – ANA – Senior Policy Fellow**

This is Carol Bickford from the American Nurses Association. When you were talking about the items that an individual might submit for amendment or inclusion in their electronic health record you talked about limiting it to text and scanned content. What about those who might be bringing digital studies with them, for example, a CAT scan, or an MRI, that they have in their own custody? So I would encourage you to expand that discussion to be more than text and scanning.

**Deven McGraw – Center for Democracy & Technology – Director**

Okay. Thanks, Carol. That particular discussion was in response to a discussion teed up with that either/or phrasing from ONC in the actual rule, but it's a good point and we'll add it to the material that we have to discuss on our next call. I think we've got to close, because we're nearing the end of our time. We'll pick this discussion back up on our next call, which is on March 28<sup>th</sup>. In the interim if everyone will please do some thinking about which issues they want to make sure we try to cover in that next call, that

would be terrific. It may help us proceed a little bit more quickly, but in the meantime we'll also try to chase down answers to some of the questions that came up during the call today that we needed to get some additional feedback on, including understanding with a little bit more particularity what the requirements are on amended in the privacy rule.

Anything else, Paul, before we close?

**Paul Egerman – Software Entrepreneur**

Yes, great call. I want to thank all of you –

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, welcome back, everybody.

**W**

With a bang.

**Paul Egerman – Software Entrepreneur**

Thank you, Gayle, for the public comment also.

**Deven McGraw – Center for Democracy & Technology – Director**

Yes, thanks, Carol.

**Paul Egerman – Software Entrepreneur**

Carol, right.

**Deven McGraw – Center for Democracy & Technology – Director**

All right, everyone have a nice rest of your day.

**Gayle Harrell – Florida – House of Representatives**

Thanks a lot.

**Paul Egerman – Software Entrepreneur**

Bye.

**All**

Bye.