HIT Standards Committee
Privacy and Security Workgroup
Clinical Operations Workgroup
Transcript
August 8, 2013

Presentation

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Good afternoon everyone. This is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Privacy & Security Workgroup and the Clinical Operations Workgroup. This is a public call and there will be time for public comment. Please remember to state your name when speaking as the meeting is being recorded and transcribed. I'll now take roll? Dixie Baker?

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

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Walter Suarez?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
I'm here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Chad Hirsch? Dave McCallie? Ed Larsen? John Blair? John Moehrke?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
I'm here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS – Senior Director of Privacy and Security – Healthcare Information & Management Systems Society (HIMSS)
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Sharon Terry?

Sharon Terry, MA – President and Chief Executive Officer – Genetic Alliance
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Peter Kaufman?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
He's here; he just stepped away for a minute.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Thanks Dixie. Tonya Dorsey? Leslie Kelly Hall? Mike Davis? And for the Clinical Operations Workgroup, Jamie Ferguson?

Jamie Ferguson – Vice President, Health Information Technology Strategy and Planning/Fellow – Kaiser Permanente/Institute for Health Policy
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
John Halamka? Martin Harris?

W
Dr. Harris will be joining shortly.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Thank you. Chris Chute?

Christopher Chute, MD, MPH, DrPH, FACMI – Professor – Mayo Clinic College of Medicine
Present.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Donald Bechtel? Liz Johnson? John Klimek? Joyce Sensmeier? Kevin Hutchinson? Cris Ross? Becky Kush? Wes Rishel? Dan Vreeman? Stanley Huff? Marjorie Rallins? Floyd Eisenberg? Jeremy Delinsky?

Jeremy Delinsky, MBA – Senior Vice President, Chief Technical Officer – athenahealth, Inc.
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Kim Nolen?

Kim Nolen, PharmD – Medical Outcomes Specialist – Pfizer, Inc.
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Jay Crowley? Karen Trudel? Nancy Orvis? Terrie Reed? Clem McDonald? Marjorie Greenberg? Kevin Brady?

Kevin Brady – Group Leader, ITL Interoperability Group – National Institute of Standards and Technology
Here.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
And are there any ONC staff members on the line?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Debbie are you there?

Debbie Bucci – Office of the National Coordinator
I'm here, sorry, on mute. Debbie.

Michelle Consolazio – Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Okay, thanks Debbie. And with that I'll turn it over to you Dixie.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay. Thank you. Thank you all very much for dialing in to today's call and we'd like to welcome the Clinical Operations Workgroup into this. The Privacy and Security Workgroup was assigned a task early this year to review the digital signature plans that CMS was putting into place for electronic submission of clinical documentation or esMD. CMS gave a very good and insightful and thorough overview of their plans at the July Standards Committee meeting and following the meeting, I suggested that – to ONC that we might want to involve the Clinical Operations Workgroup in this – in hearing about esMD. There were – it was the last presentation of the day, but even then, there were quite a few comments and questions.

So, I think you'll find this presentation very interesting. One of the questions that was raised at the Standards Committee meeting had to do with alignment with the DEA plans for digital signatures, so I've asked Debbie Bucci from the ONC to do a comparison and she, after our presentation from CMS, she'll go over that and then we'll open the floor for a full discussion. I'd like to thank Melanie Combs-Dyer and Bob Dieterle, as well as Debbie Bucci for their work and for participating in this meeting. And Bob, please forgive me for probably slaughtering your last name. Jamie, would you like to say a few things?

Jamie Ferguson – Vice President, Health Information Technology Strategy and Planning/Fellow – Kaiser Permanente/Institute for Health Policy
Sure. Well thank you Dixie and thanks for putting this together, I certainly appreciate it. I think you know that in the Clinical Operations Workgroup, we have, for a long time supported, strongly supported the use of digital signatures, first on the CCD and then on the other CDAs for health information exchange, and so I think we're very interested in understanding some of the nuances and differences for the esMD project as well as the comparison with the DEA. So, I'm very interested and just want to be appreciative and thank you for putting this together.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Thank you. Walter, did you have comments?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Yeah, thanks. Yeah Dixie, thank you and thanks all of you for joining us. I think the only comment I wanted to make is one of the key points around this topic is the level of granularity at which the signatures are to be applied. And the interdependency between the signature and the various content elements of the message when messages contain different types of sources within the message, different physicians for example, or a physician and another provider, the content of those two or three are included, then how does one attach a digital signature at that granular level within the electronic document. So that would be one of the more interesting aspects of this project, I think.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay. Thank you, and I know that you're also doing some work in the NCBA – that's related to this as well, so we'll be interested in hearing your observations in that area.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Thanks.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
And with that, can we advance the slides? And I should also mention that I did get an email from John Halamka, who is telling me that he was not available today, so, I've already talked about what the agenda is, so let's just move on to Michelle – or, not to Michelle, to Melanie.

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services

Thank you Dixie. This is Melanie Combs-Dyer. I am the Deputy Director of the Provider Compliance Group in the Office of Financial Management at CMS and I'll be walking through the first few slides about our Electronic Submission of Medical Documentation project and then turning it over to Bob Dieterle, who is our esMD Initiative Coordinator, who will talk a little bit more about the author of record work that we're doing in our esMD Workgroup. Next slide. And one more slide please.

What we're about in my part of CMS is all about improper payments. We hire a bunch of contractors to look for improper payments, and there are quite a few of them in Medicare. Because the Medicare Fee-for-Service Program receives over four million claims every day, and most of them get paid before they get stopped, there are lots of improper payments. And so our Medicare contractors, called Medicare Administrative Contractors or MACs, Recovery Auditors or formerly known as RACs and the other contractors send out documentation requests. And there are between one and two million requests that are sent out each year and most of these contractors currently receive the responses to those documentation requests from doctors and hospitals and suppliers in paper form or through fax. Next slide please.

So we created esMD, the Electronic Submission of Medical Documentation. Next slide please. That's it. Because before esMD, providers, again the Review Contractors, the little red box there, would send out documentation requests through the US Postal Service to the provider and the provider would mail or fax back the medical record. But when we got to Phase 2 of esMD, which started in September of 2011, we were still delivering the documentation requests by postal mail to the providers, but the providers now have a third option. They can mail back the medical record, they can fax back the medical record or they can esMD it back. And at some point, maybe 18 months in the future, we hope to be able to deliver those documentation requests electronically as well. And that's what we call Phase 2. Next slide.

So the goals of the esMD Program are to reduce administrative burden for the provider, as well as for the Medicare Contractor, to reduce improper payments because we will be able to be more efficient in the way that we do our reviews, and to move from a post-payment audit world to more of a prior authorization or a pre-payment review world. To do that, we need to be able to move from a paper to electronic way of talking between the review contractor and the provider, and we need to replace the wet signatures with digital signatures. And finally we need to migrate from unstructured data to structured data. Next slide.

So this is a picture of what we are eventually envisioning as our esMD system. It has our review contractors in those red boxes in the upper right hand corner, and it has the providers, the doctors and the hospitals, over there on the left. Today, only the doctors and hospitals represented in the lower left hand corner, who are connected to a Health Information Handler, an HIH, to gain access to a connect compatible gateway, can communicate with the CMS connect gateway. Some day we at CMS may build a direct gateway or put in place some kind of an EDI translator, so that we can accept medical documentation in other forms, but today, we only accept it from a connect compatible gateway to our connect gateway. Once we receive it in the Baltimore Data Center, we strip off the security wrappers and we then deliver it to the requesting contractor. Next slide please.

What this represents is the full flow of electronic medical documentation requests. Remember today, we only have paper medical documentation requests going out and providers are able to send in responses to those paper medical documentation requests through the esMD system. That's represented by the third box on the right which is labeled as esMD Phase 1, that's in place today, that's where we are. But where we want to be is we want our contractors to be able to send electronic medical documentation requests to the providers. But before we can make that happen, if we want to stay compliant with FISMA, the Federal Law that requires us to protect patient's PHI, we have to have providers register to receive eMDRs, and to do that registration, they will have to send in a transaction that gives us their digital certificate and tells us which HIH they want us to send their PHI to. So what's represented there in box 1 and box 2 we call esMD Phase 2. And that's what we are really going to try to work hard on over the next 18 months. Next slide please.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Can I ask a quick question?

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
Sure.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Just a very quick on this eMDRs. This is – originally this is – or currently a letter with some information about the situation, right? I mean, we received this claim, we paid, we are looking for the following additional information. Are those done with a basic content elements of the eMDRs or are they more complex documents?

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
No, you got it exactly right. Today they might be onesy, twosy letters, one letter requesting one medical record or they might be one letter requesting the following ten medical records or the following 200 medical records. What we envision in the future is a structured eMDR and Bob can talk about this in a minute, I think our esMD Initiative Workgroup has already developed the transaction, the standard for the transaction, the data elements that need to be included. And it would be one transaction, one eMDR requesting one medical record and so it would contain the necessary pieces of information for the doctor or the hospital to identify that patient, find their medical record for that date of service for whatever the procedure was or whatever the service was, so that they can then submit it into the esMD system. Did that answer your question?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Yes, thanks so much Melanie. Thanks.

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
Okay. So I think we're at slide 10 and I will turn it now over to Bob Dieterle, our esMD Initiative Coordinator. Thanks Bob.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
All right, thank you very much Melanie and thank you Dixie for the opportunity to present. What I'm going to do is walk the transition from the esMD Phase 1 and Phase 2 Programs, if you will, into the digital signature environment, because I know that's the topic of our discussion for today. So looking at the overall workflow for esMD Phase 1 and Phase 2, and looking at the surround of the things that we have to have to make digital signatures work, our user story basically has all of the actors, and that would be the providers and the intermediaries such as the HIHs or the payer contractors or the payers with a digital identity, the ability to sign using a digital certificate.

We have a registration transaction, that Melanie's talked about, that has to be signed by the provider, which then gives us the right to send out a signed transaction requesting documentation. The expectation for Author of Record Level 1, and we'll talk about that in a second, is that this bundle of documents coming back will also be signed. As a bundle now, not authentication of individual documents necessarily, that's Author of Record Level 2, but the ability to sign the bundle, to indicate that this is being submitted in response to a request. The payer or the payer contractor in our case the esMD in Baltimore in the Data Center would go and receive that returned document set and validate all of the artifacts related to the digital signatures. That would also be true of the transaction to register. Next slide please.

So as we look at the flow internally within CMS, we have the transport and the connection to the front end that Melanie went over, using Connect Today and over time, migrating to not just connect, but Direct and X-12. And then on the back end we have all of the transaction processing side and the place that digital signature sit in is right here in the middle, the ability to validate both the signature or integrity of the – for identification of the individual, as well as possibly provenance of the document and the integrity of the transactions or documents. Next slide please.

The series of definitions, for those of you who are not real familiar with digital signatures, that are important, and I'm going to go through these this time. Identity is really a set of attributes that uniquely describe a person or legal entity within a given context. Identity-proofing is the process by which a CSP or registration authority collects and verifies the information necessary to establish the identity. A digital signature is a cryptographic transformation of data, the important part is in red, that provides a mechanism for verifying origin, authentication, data integrity and signatory non-repudiation. Data integrity is a property that the data has not been altered, in this case, since it was signed.

Non-repudiation, the important part of this is it's a service that allows for a third party to verify the signature and the integrity. And that is verify it without resorting to additional things such as system insulation, audit logs, transaction logs, all the things that might be required for other forms of signatures or attestations. And then finally the delegation of rights that we will talk about is the ability to assign the authority to sign a digital signature from one person to another, to assign that right. And while that might be done through a legal document, in our case we're looking for a cryptographic solution to that so that we can validate it and it also provides equivalent electronic non-repudiation. Next slide please.

We broke our Author of Record work into three different phases. The first phase was focused on making recommendations, establishing the standards for how you create digital signatures, and we'll talk about that in a second, as well as the ability to sign the transaction and the ability to sign a bundle of documents. We've already done that, all of the implementation guides are already created, they're posted out on the S&I Wiki. We're focusing on – as well as the white papers, and we'll talk about those in a second. We're focusing on the Level 2 right now, which is to sign an individual document. We have an eventual goal of being sign individual contributions. We can talk about why that is a goal as opposed to something we're pursuing right now and it's tied heavily to the availability of standards that would allow it and the work that would be necessary to put them in to certified EHRs. Next slide please.

So we had three sub-workgroups work on the various aspects of a digital signature. One working on identity proofing, what are the standards for that, what are the issues and gaps. Another working on digital credentials, how are they created, how are they transmitted, how are they managed, how do you access them. And the third working on signing and delegation meaning what are the specific standards and artifacts that need to get created to instantiate a digital signature, either on a transaction or inside of a document or attached to a document and also to be able to go and do this cryptographic delegation of rights. Next slide please.

And oh, by the way, there are three white papers out there on the S&I Wiki that address those three issues. I'm going to go through the summary of them here. So for identity proofing, and we looked at a series of standards that could have been useful to us. The ones we finally selected as being appropriate were the Federal Bridge Certificate of Authority, it's 509 certificate policy, the FICAM roadmap and implementation guidance and the NIST SP-800-63-1, which talks about electronic authentication guidelines. Because we are dealing with fiduciary responsibility, fiscal responsibility and medical legal signatures, we decided as a workgroup, that an in-person identity proofing was both appropriate and also a requirement for identity proofing an individual or an organization.

That left us with FBCA medium as the lowest bar that was reasonable, and it also makes provision for an antecedent event that could be used, so for example, if the identity proofing is being done as part of credentialing, that credentialing process could be the antecedent event. Federal Bridge has some very specific requirements there for antecedent events and we have to work within that, or at least work with it as we think about how we go and approach identity proofing. Next slide please.

So broadly the recommendations are to identity proof compliant with FBCA Medium Assurance, that requires an in-person or acceptable antecedent event. We must include the verification in the case of CMS, of the NPI, so that if you are signing as a biller, meaning you have delivered a service and you'd now like to get reimbursed for it, the NPI should be part of that certificate. There will be others that will have certificates that we'll sign that will not necessarily have NPIs. And we also made the provision because our workgroups were open to all payers, that it could also be an alternative provider ID. So there are providers that have IDs that are not NPIs that wind up billing other, whether its commercial or Medicare.

We tried to establish a concept of a single identity proofing as being appropriate for all issuance of credentials at or below that level. And I know when we go through Debbie's work, we'll talk about the potential implications of that. But the idea is that one identity proofing event could then be used to issue Author of Record signing credentials, it could be used to issue credentials for Direct, for example. Maybe over time, and we'll talk about this when Debbie goes through it, maybe for DEA and we looked at the idea of trying to federate the process of identity proofing, so that we're not limited to just those CA's that do identity proofing, but we could use a federated environment that takes into account the natural interactions that happen in healthcare. For example, as part of credentialing, as part of licensure, as part of the normal HR functions, so the things where people are in-person and available and can present credentials, there's no reason why, with appropriate policy and accreditation, those couldn't be used for identity proofing. We have a list of gaps here that are virtually all policy-related. And these would be the policies necessary to implement what I just described. Next slide please.

As we look at standards for signing credentials, ultimately it came back to Federal Bridge 509 Certificate Policy, to FICAM Roadmap and recommendations are that this is X509 version 3 signing certificate with a non-repudiation bit set and that would be used to sign all AoR transactions, bundles and documents. We looked at the issuing, meaning credential issuing issues and our recommendation is that these be issued only by CA's and CSP's cross-certified with the Federal Bridge or they're one level down subsidiary CA's. It resolves a bunch of issues when we start to go and have CA's, sub-CA's to sub-CA's. Providers must authenticate to a signing module at least one additional authentication factor. So this is two-factor authentication to be able to sign. We had some issues related to long-term validation because signatures on these documents will survive, or need to survive well beyond the lifetime of a typical credential, and so long-term validation was an issue. We think we have the answers to that by using the

XAdES-X-L standard. Next slide please.

And finally, as we look at the instantiation of these signatures, the standards that we looked at were again FBCA 509 Certificate Policy, we looked at the FIPS standards for 186-3 for digital signatures, we looked at XML DigSig and XAdES from W3C. We looked at the OASIS SAML assertion as a way to deal with the delegation rights. So again, all standards-based approach to managing the artifacts from signing. And ultimately recommend the digital signature is an XLM DigSig standard embodied within the XAdES-X-L for documents, it doesn't have to be X-L for transactions necessarily, which then provides for the ability to have data integrity on the message or the document, the time stamps, role, long-term validation, etcetera. And then using the SAML Assertions 2.0, we can satisfy all of the delegation rights issues. We have a gap that we have looked at how we fill on validation of these delegation of rights. We have an approach that we'll use as part of pilot, and that is to validate the assertion at the time it is used. And we can talk about that or we can read it in the documents. Next slide please.

This is just an example in a transaction of how signing works. And what happens is, you take the portion of the transaction you wish sign, you compute a hash or digest over it, which takes that entire message and converts it into a shorter string. The characteristics of that string are that it is unrealistic for that string to have been created from any other message, and that message cannot be used to recreate the string. That digest is then signed or encrypted by the private key of the holder. That public certification, which is the other half of the PKI certificate the public keys that are available for decryption is sent along with the message.

So you'll have the message, you have the encrypted hash and you have the public keys as part of the public certificate. The receiver then goes and can validate the certificate to verify that indeed it was issued appropriately by an appropriate trust anchor or appropriate authority, that it has the appropriate content, for example validates the NPI of the sender, and it is currently valid. And then what they do is they will decrypt the hash using the keys that were sent, computes the hash on the message and by comparing the two, you can do two things. You can verify data integrity and you can verify that the holder of certificate signed that message. And this is true of documents also. Next slide please.

This is broadly the environment we're working in for the Determination of Coverage issues, and this is where we're starting to look at now, how we require, in a standard format, information that is necessary for anything from prior authorization to pre-payment review, to post-payment audit. And all of these little documents floating around on the screen here, between the licensed clinical medical professional and the physician and the specialist or the service provider and the payer are all places where we need to be able to prove the provenance of the document and the information it contains. Next slide please.

I want to separate Author of Record Level 1 from 2 because it's important as we go forward in the conversation. In Author of Record Level 1, we are assigning a bundle of documents for the sake of submitting them in response, for example, to a Request for Documentation an eMDR, Electronic Medical Documentation Request. So we're still using a 509 signing certificate, FBCA medium. We are using a different structure to store the XAdES standards signatures and that is the IHE Digital Signature Standard and the reason for that is, we may wish to sign multiple documents for the sake of submission, not for the sake of a provenance of the document itself. And we also would use SAML Assertions to delegate that right to a third party if necessary. So the environment is, they're creating these in response to a request, they're being validated upon receipt. There is one signer and one signer only on the entire bundle of documents. And the delegation of rights is used to establish the right of the submitter to submit. Next slide please

As we go to Author of Record Level 2, we have a different set of requirements. These are now digital signatures on documents for provenance, both clinical and administrative. We're focused on administrative but they could be used equally for clinical validation of provenance of declaration of provenance. We have a need that they meet the requirement for what we're calling encapsulated non-repudiation meaning, what is contained in the document is sufficient to validate the signatures on the document and the integrity of the document itself. The second one is, signature needs to be applied at the time of document creation, modification or review. In the case of CMS administrative requirements, it has to be applied prior to claim submission. Multiple signatures may well occur on the same document, we have to make provisions for that.

Certificates must be validated at the time they are used, and the reason for that is because this document may have to go and exist for many, many, many years, as many as 21 years, we can't be assured that the information to determine that the certificate was valid at the time it was used is available at the time we need to validate the signature. So we're looking at the need to do that long-term validation at the time of signing. We need a support of validated delegation of rights assertion, we talked about that. We need to have signature and delegation of rights that must travel with the document, this can't be held somewhere else in a practical sense, both for access and for the ability to manage it long-term. The signature has to be bound to the document for the lifetime of the document, that's a similar statement to 6, but not quite the same and we want something that supports a transition from unsigned to signed documents over time. In other words, we want these to be backward compatible. Next slide please.

So as an example, we could approach this two different ways. The upper flow here shows a document where the signature is internal, and as long as that process of making that signature internal allows for backward compatibility, all the recipients continue to receive those documents. In this case we're talking about a CDA or a CCDA. If we sign this externally, now we have additional artifacts that have to travel with that document. For example, the signature on the document, a delegation of rights and the thing we ran into is the recipient then, if they don't know what that means, and that will be the vast majority of them once you can initially sign, they will either discard the signatures in which case the document will now be unsigned, or possibly worse, in fact, we would argue worse, they'll discard the entire transaction because they won't know what to do with it. Next slide please.

So what we've done is, we've worked with the structured documents group at HL7 and we've identified a way that within a CDA we can actually sign the CDA itself, and John Moehrke was helpful in putting this together as were the other members such as Bob Dolin and Austin Chrysler, in helping us to understand how we can add in what's called a signature text element or attribute as part of a participation occurrence in the header of the CDA. And that can contain all the artifacts that are necessary to both sign and, where necessary, convey a delegation of rights. And since it is in the header and its part of the standard structures and part of the rim element, it applies equally to a structured body and an unstructured body. Next slide please.

So we look at the flow that happens in a provider environment. The provider has an encounter with a patient, maybe more than one provider in the same clinical setting. They use their EHR and the EHRs forms and template to record the information. That information is stored in the EHR database. Next slide please. At some point that information is then moved into a CDA, in other words, a CDA is created from it, okay, and it may be structured, such as an operative note, or it may be unstructured. And in the case of a structure, the CDA sections and entries are populated or appropriate null Flavors are used to indicate that the data's not available for that particular section, template or entry template. Next slide please.

When the provider's ready to sign, they can potentially sign with one session, multiple documents. They practically should review each one and indicate they're ready to sign it, but one authentication to a signing process should be sufficient for them to go through and sign multiple documents. What's happening during that signature process is things like long-term validation and universal time are being captured, the digest is being created over everything other than the legal authenticator and authenticator, because those are the places where these signature elements will be stored and will get updated. And they then write the signature back or the signing module writes a signature back into this signature text element. Now that can be done on more than one document in one session by a provider and more than one individual can't sign the same document. And as we indicated here, authentication is acceptable by two-factors, something you know, something you hold, something you are, etcetera. Next slide please.

Right now this will be an HL7 ballot, the part that we talked about on how to include a digital signature in a CDA document, for the September ballot cycle for HL7. It is being sponsored by the Structured Documents Workgroup, co-sponsored by Security and Attachments and has RMES or the Record Management Evidentiary Support Workgroup as an interested party. We are finishing it, we've posted on the ListServe this week, the I'll say semi-final draft. The effectively final draft will be posted on Monday for comment before it is approved for ballot. We should be approved for ballot on the 15th and start the ballot process on the 16th. Next slide please.

So, in summary, the Author of Record work is identifying best practice for establishing identity of providers. That includes identity proofing of all participants, individuals and organizations, managing credential lifecycle, especially with attention to private keys, Digital Signature Standards and Delegation of Rights Standards as part of all of this establishing the identity of the providers for the sake of provenance on transactions, bundles, documents. And we're addressing the Author of Record requirements, which we've talked about, and we're defining requirements for structured documents that include digital signatures for proof of provenance. I think that's the end. Next slide please. Yes.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Thank you Bob and Melanie both. We really appreciate this and that's a great overview of what you're doing. I'm sure we have a lot of questions, but I would like for Debbie to briefly go through the comparison between the esMD signatures and the DEA requirements before we break it open for full discussion, because she may be answering some of your questions through this. Can you do that Debbie? Are you there? Are you on mute?

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Yeah, I am on mute, do you hear me now?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Yes, thank you.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
So hopefully I can answer some, and before I get started, I wanted to thank Bob Dieterle. He worked with me on making sure I was accurate on the esMD comparison, so as we go through to make it just side by side, hopefully they are meaningful. Next slide please. So what focused on, I spent a significant amount of time looking at the DEA regs and focusing on the DEA website and what I thought we were focusing on was the DEAs electronic prescription for controlled substances, which provides practitioners with the option of writing prescriptions for controlled substances electronically. But even as of yesterday, what I really think is – we're looking at two systems within DEA and I don't have a slide for it. And the other thing that you need to take into consideration is DEA's controlled substance ordering system, which allows for the secure transmission of ordering Schedule 1 – require for 1 through 2, but scheduling 1 through 5 controlled substances. Next slide please.

So in the side-by-side, I'm just going to briefly go through to have time for discussion. I just want to highlight that – and focus on the DEA side, that on the DEA side, everything starts with a DEA registration which is a form 223. Everyone needs to have that license or that registration for either prescribing or ordering prescriptions. There is – when you go to the – using the DEA's CSOS system, you delegate a coordinator that manages because you have a 223 form for each location that you have, and then on top of that, you need another form, electronic representation of actually order, which is the DEA 222.

The applications must have a third party certification program and they do have a delegation via power or attorney, through DEA. So verification of the DEA form is – can either be for hospitals, you can delegate by hospitals or government agencies or – health services or to an individual. The total numbers of individuals is 390,000 – providers it's really more for the EPCS, but the larger group is, there's over 800,000 – of steps between manufacturers, distributers, retail pharmacies, authorizing institutions and other registers. Next slide please.

So the CSOS certificates are equivalent to an FBCA Medium level of assurance and they can, according to their policy as of February 2010, can be used for other applications. The certificate again is issued to each location and it is typically operated under the authority of DEA. DEA did that specifically because they wanted to quickly be able to revoke a certificate at any location where possible. It can be renewed for a maximum of up to six years, can be renewed for two times and there are some general, as you see, when you looking across for esMD, that they're generally aligned where you can validate the order, verify – checking and because it's issued by the DEA, there's only one single trust anchor that you need to worry about. Additional verification is that they check for the DEA, they actually include the DEA 223 number actually into the certificate itself. Next slide.

So essentially the e – I don't want to go into authentication, but, certificates could be used for either authentication or signing, specifically for the EPCS, it is actually the application that signs on behalf of the prescriber. It could be that it – you may use a digital certificate and it may be passed on as – for the evidence of the information or either they would send a data file instead. It's really up to the prescribing application to do that. But essentially it is signed and the responsibility is to the prescribing application. And within that, you can sign one application at a – you may sign many prescriptions for one patient, but it must be done one patient at a time. The retention of the application orders and linked records are for two years and FBCA retention records retain for a max of 10 years 6 months and then again, they do have the – of delegation of rights via power of attorney to the DEA registrant, and also so for hospitals again and agencies may delegate as well. Next slide. I think that's it.

And then this was more presented by CMS and Bob, did you want to present this piece or – ?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services

Yeah, I'd be very happy to. We looked at the DEA interim rule when we started the work on Author of Record and we tried to understand how we could possibly work with the work that they had done on digital signatures. And it wasn't particularly clear to us what they were going to finally require. If we look at the Final Rule, it appears that we may be able to use their identity proofing process for both individuals and organizations, where organizations are identity proofed, as the basis for issuing Author of Record certificates. That would assume that they are acceptable for Federal Bridge Medium Assurance certificates under – for the cross-certified CAs that we would use.

I'm less comfortable that we can reuse their certificates because they have some very specific requirements as far as embedded information, as do we. Possibly as we move forward in the future, longer term, we could create common certificates that have all the information necessary for either application as either specific information or OIDs on the certificate that would allow us to go and share the certificates, assuming that's appropriate. The other thing that we want to address is over time, we should have a common certification audit process for signing applications so that we're assured that the signing applications meet the requirements – the Federal Bridge requirements for either software or hardware signing applications. Questions? Is that what you wanted me to present Debbie?

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator

Yes, that's it and I think that's the last slide. You can go to the next slide, but I think that's it.

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

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Is it under ten minutes Dixie?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
I just put your definitions in there Debbie.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Okay.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Well thank you. Now Debbie, I remember you and I had some exchanges about this, the CSOS certificate can't be used for signing prescriptions, right, it can only be used for ordering drugs.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Exactly. It cannot be used, it can be used for other applications, but it cannot be used, exactly. And the other thing is, Level I substances, you can order, but you cannot electronically prescribe, but you can subscribe Level II through V through the EPCS.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay. All right, let me open it up for questions to either Bob, Melanie or Debbie.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
This is Peter Kaufman. I think many on the call know, but some people may not know, that I was kind of instrumental in working through the EPCS stuff and also working with NIST on generating 863-2, which I was a little disappointed wasn't mentioned. There was a little confusion with the last three slides Debbie, but the confusion between pharmacy ordering and prescribers, the stuff was accurate was there, but it was kind of...for somebody who didn't know, I think they might have been a little lost between the thing about ordering controlled drugs and ordering Schedule I-V and prescribing. You can't paper prescribe Schedule I's either, but the prescribing of only Schedules II-V. But let me talk quickly about 863-2, which was submitted for comments in February and the comment period closed March 4.

During the meeting I sent an email to NIST to try to find out where things stand on that, but the difference between 63-1 and 63-2 really comes down to 5.3.2 in the document, which allows hospital Medical Staff officers to do identity proofing for their physicians. Because the credentialing process at a hospital is actually as much or more than Level 4 generally is, so they should easily be able to safely do a Level 3 credential for two-factor authentication. That is in 863-2 and I'm not aware of any negative public comments on that, so I'm assuming it'll go through with the Final Rule and I'm hoping you can update the requirement for 863-1 to 863-2, so that hospital Medical Staff officers could do the identity proofing for their credentialed providers.

The only other thing that I wanted to say was – is there – or it's really a question, was did this take into account the NSTIC and the Identity Ecosystem Steering Group working to make a digital signature that will be useful across the board rather than having different digital signatures for different processes in healthcare? I've often called for a single digital signature, and not just for physicians, but all the way down the road, to different levels of medical providers – healthcare providers, so that everybody would be signing things digitally. And now I will put myself back on mute.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
So, this is Debbie. You're absolutely right that I do have the CSOS system mixed up with the EPCS system because until literally last night it – I did not realize that I was looking at two separate systems, one for ordering and one prescribing. And it was when we were focusing on just the digital signature aspect is where it finally came to light, thank you Dixie. And as far as authentication, there are separate certificates and separate message use for authentication versus the certificate, and in this case, the DEA – can be used for other FBCA Medium applications. Now whether – it did not specify whether it could or could not be used outside the DEA, but their certificate policy was very neutral on that. So it is moving towards an NSTIC type of way where one credential could potentially be re – one certificate for signing could be reused, as Bob suggested in his slides.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Keep in mind that the DEA doesn't actually require the doctors or the pharmacists to digitally sign. They do need to use a two-factor authentication, but the vendor in both ends can do the digital signature. The DEA does have a method of sending electronic prescriptions digitally with a digital signature on both ends, but as of yesterday at the NCPDP meeting, nobody is actually sending any prescriptions for controlled substances that way, although I hope, as providers start getting digital signatures, that'll actually start becoming something that's used.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Yeah, this is Bob, let me just comment on one thing Peter. At the time we put the white papers together, which was the source of the information going into these slides, 863-2 did not exist. We're happy to update it because it's important to point out that the changes that were made in 863-2 are absolutely in line with the recommendations we'd made on federation of identity proofing.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
You're welcome.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
What about his question about NSTIC, Bob? Did it take NSTIC into account?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
We had discussed NSTIC. The question was how to look at that as an ultimate instantiation of a digital signature process and it was, I'll just in motion, and probably still is in motion. We don't have an objection to it, but we need something that has good, strong basis for meeting both FISMA and HIPAA requirements, especially as we see in 800-66. I don't really have a basis for saying we could or could not use an ultimate NSTIC approach, other than to say I don't think it's quite ready.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Well – so Bob, this is Debbie, and also in the white paper for the digital credential piece, it does recommend using an authentication, as you mentioned in your slides, if you authenticate to the system before you're actually doing the signature. And I'd like to make the clarification on – for the prescribing, a provider authenticates to the system, they use that as a signing, but it's actually the application that is signing the prescription, it is an authentication event. So, it's not apples and oranges in the way that they're actually doing it.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
I think we could see something like NSTIC as an authentication approach, meaning the ability to authenticate to a signing module where you then have access to a 509 signing certificate. We're certainly open for that approach; we were very silent on ultimately the method that we require for two-factor authentication.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
The DEA doesn't say that end-users can't do a digital signature and then have the vendors send it on to the pharmacy under the non-digital signature system, it's just easier to have them just authenticate instead of digital signature. But I think digital signature would be better.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Actually, the DEA regulation says you must use an e – a certified signing application to do it; you must go through that if you're going to do it –

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Right, but the vendor can do that, the vendor can be the certified digital signature; the end-user does not have to have their own digital signature that they're sending through to the vendor for the two-factor authentication.

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
Okay. So a provider authenticates to the system and the system can sign on behalf of the provider –

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Debbie, I think you make too much of that. I know you said it before, but every digital signature is always signed by software, by definition it is; I think that's all its saying in that regulation. It's just saying the software signs it and that's always the case. Do we have questions or comments for anybody else, from others in the group?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Yes Dixie, this is Walter, I have a couple of questions. So this is a very comprehensive and impressive body of work really. It is also, as I see it, quite complex and the question I have is are there any products currently capable of performing or meeting all these Author of Record identity proofing, digital signature, the bundled document level, delegation of rights requirements? That's the first question, are you aware of any products? The second one is what is the timing for implementation of these various requirements? And then the third question is, what do you see the additional load to the systems, when you put all this digital signature elements behind the system, how much load to the system that carries, particularly as the data is packaged into a CDA perhaps and then unpackaged later on? Do you see a major load into the system? And then my last question and these are very quick, I suppose, short questions, but the last one is really, what's the cost? What to you estimate to be the cost for providers to implement this?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Good set of questions Walter. First, there are no products that do it all, but there are certain instantiations that do a large part of it. The delegation of rights is the piece that is really the exception. For example, the DEA – sorry, the DOD and the VA currently use PIV Cards to do exactly what we're talking about here or PIV-I cards. The DEA, through the signing modules, are doing exactly the same thing on transactions, or at least a very similar thing on transactions. The parts that are new in what we did is to create a method for a delegation of rights that could be cryptographically verified. It uses SAML Assertion; is the SAML Assertion used for something like this, yes, but not specifically this. It uses a brand new construct on the CDA that did not exist before that is to take a RIM element and allow us to embed a digital signature. So, the answer to your question is yes and no, pieces of it currently exist, pieces of it do not.

As far as the implementation time, we're looking at, as Melanie said, moving into this gradually over the next 18 months or so on esMD Phase 2, with the assumption that over some period of time, documents will migrate as capability exists in EHRs from unsigned or electronically signed to digitally signed. We don't have a schedule on which that has to be implemented. In fact, the way esMD works, you always have the option of submitting outside of esMD, including on paper or through the mail or by fax. So we don't have a drop-dead deadline, if that's what you're asking, we do have a try to start the process over the next 18 months in pilots and go into production at the end of that period of time.

As far as load on the system, gathering this information and signing given PKI is not much of a load, quite candidly and at the rate – an approach we're taking it's going to be one, at least in an ambulatory environment, it's one signature per patient visit, which isn't a large overhead. If we had the opportunity at some point to move to individual contributions and signatures at the time of actions, that'll have a different challenge, but we're not ready to do that yet. The technical underpinnings don't even exist within the EHRs or in the standards to do it.

As far as cost, the cost for certificates is going to be reasonably nominal. The work that we've done with the various cross-certified CAs say that as long as the identity proofing becomes part of another process like credentialing, they believe that a reasonable cost. For the volumes we're talking about will be on the order of single digit per year per certificate, even if we don't get quite to there, it's a nominal cost given the benefit. As far as the signing modules, like any other piece of software, once they're created and certified, it depends upon what the vendor's going to charge for it or the service.

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
And this is Melanie; I'll just jump in on the timing. The good news is that we are not operating under any statute that says we have to do this by a certain point in time. The bad news is that I'm starting to hear some rumblings from our Office of Inspector General suggesting that perhaps there's more that we can do in this space, audit logs of EHRs and verifying who's signing the medical records that our contractors are auditing. So, while I don't think we need to rush, I think we need to continue to step forward at a deliberate pace and show that we are making progress on this front.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Great. Thank you so much for those answers, very informative. Thank you.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
I'd like to ask a question kind of jumping on to Walter's, the last question I guess it would be. The certificates used for the Direct messaging protocol are not cross certified with the Federal Bridge so will this result in a new requirement that Direct certificates be cross-certified with the Federal Bridge?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
This is Bob, I'll try to answer that, and the answer is no. The requirements for Direct are unique to Direct. They are primarily related to identity proofing endpoints, so the ability to determine that a message is going to a specific endpoint, in particular for CMS, under the requirements for FISMA and HIPAA, we need to make sure that the PHI we send out is going to the person or the organization we expect it to go to. That's a different requirement and bar, or at least is potentially different requirement and bar than we have for the medical-legal requirements and fiduciary requirements related to these digital signatures on documents and transactions.

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

Debbie Bucci – Office of Standards and Interoperability – Office of the National Coordinator
This is Debbie and because of the HISP to HISP, you could not use the same certification for non-repudiation and – .purposes, so it would have to be separate.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
That's not true Deb, these would be separate certificates regardless.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
This is John Moehrke. I definitely support that. A certificate would be issued for specific purposes and these non-repudiation certificates have to stand for a long time were as SMIME certificates need only protect the message. They generally are issued for different purposes that would be part of the certificate purpose.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay, are there other questions?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
This is John Moehrke again. I guess I'd just like to – I really liked the way you went through and did compare the DEA and the esMD certificate needs. I think those are appropriate things to potentially try to bring together over time; I think Bob, you mentioned that at the end. I do want to echo some of the earlier discussion that the actual workflow involved in the DEAs signature use is very different. The content is different, it's a message versus a document, it's a different reason and such. The question that I still am not sure I heard answered was, have you addressed the issue of where the trustable time stamp comes from? In your case, you are certainly trying to cover for risks that lead to fraud for non-repudiation, and therefore you really need a trustable time. I'm not sure where you addressed that.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
You mean the time stamp itself?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Correct. How do you know that the signer didn't backdate it or post-date it?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Well I think the two possible solutions for that John, one is in the process of certifying signing modules, to the extent those are certified to go and grab universal time and use it appropriately we may be able to rely on that. And the alternative is to do what the industry's done elsewhere, which is to use a time stamp service. Those are the only two that I'm aware of. I would prefer that we find a way in the former, because it doesn't require an additional service.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Okay.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Does that make sense or did you – were you asking –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
I – no, I totally agree. Generally, it gets less as a known risk that you follow up with if there's suspicion through audit log analysis, but the two technology solutions you've come up are also brought forth.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Okay.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Dixie, can I make one more quick comment? This is Peter Kaufman.

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

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
Okay, I knew we were running late. I think they mentioned earlier about the certificate price getting down to single digits may be reasonable for the price from the authorities to the – whoever's passing out the certificates, but I think it's unlikely they're going to get anywhere near that in terms of the cost to the end user. They'll probably be well into two digits and some vendors will have them at three digits, because somebody's going to need to pass these out. So I think that we don't want to be in the position of saying that these are really going to be cheap; they'll be relatively inexpensive, but they're not going to be at the level that's recommended for bulk.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
When this presentation was given to the Standards Committee, I would say the preponderance of comments and questions had more to do with the impact on operations than it had to do with security. Do any of you from the Clinical Operations Workgroup have questions here?

Jamie Ferguson – Vice President, Health Information Technology Strategy and Planning/Fellow – Kaiser Permanente/Institute for Health Policy
Well, this is Jamie; I do not have any questions at this time.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Others? Well, let me ask an operational question myself then. Today, when CMS goes to a hospital, let's say, or a doc – or a clinic and asks for this additional documentation as part of their audit, I would imagine that the person that does the work is probably a records person, probably not the doctor at all, right? Do you envision that – it seems – well, it seems to me like with this – these requirements in the digital signatures, that these will be more likely – these requests will now be more likely to involve the physicians themselves in responding to the requests. Is that what – do you envision that this will impact the doctor's normal wor – activities and workflow, or do you think it would just – can be implemented without too much of an impact?

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
This is Melanie, I'll go first and then Bob can chime in. I think we have to design it in a way that puts minimal change or impact on the normal flow of the physician or the clinician providing patient care. I continue to believe that there will be ways that we can capture the signature, for example, at the end of the visit or at the end of the procedure or whenever the physician is writing up the note or entering the data. And that weeks or months later, when the document is actually requested by the Medicare Review contractor, the appropriate audit logs or documents or CDAs or whatever needs to be gathered up, packaged up and sent, can be done either by the records managers, front office clerk or maybe it can become more automated, as we move forward. Bob, does that sound right to you?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Yeah, the intent of this Dixie is that, and let's just take an office visit. At the end of the office visit, when the provider is done and the documentations complete, they would create the CDA that's a representation of that visit and they would sign it. That then is the information that's necessary on a Request for Documentation; there's nothing more to do, it's all there. So that's the goal that we have. Now longer term, when we start to look at issues like, signing while you do orders, etcetera, we're not ready to do that. The technology just doesn't exist to do the digital signatures at that level, and the primary reason is that when you sign something, it can't be changed, so we'd have to have a persistent representation. Now there are standards that are emerging that might well go and address this, such as FHIR, but we're not ready to turn that into an operational requirement.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
I guess to follow up on that – this is Walter, is I actually interestingly enough went to a medical appointment this morning. And so went through at least five different providers from the nurse that took my vital signs to the physician that examined my knee to the x-ray technician that prepared me for and took my x-ray to the lab technician that drew my blood and did all the...so all these are providers that have recorded something on the visit. And granted each could be considered a different visit, right, my provider who saw me, then the lab, then the x-ray, all these – so all these will be adding different information into the record and different source really or different providers that would be signing off that component. And then all that gets pulled out and aggregated or combined into a CDA document at a later point that is perhaps in the future needed to be submitted, right, to CMS for post-statement audit. At this point, if I understand correctly, the expectation is that each of the individuals that provided my care and touched my record, put something on my record, are not going to be expected to digitally sign the participation they had in that record. But that at the point of aggregating the data into a CDA to be submitted to CMS for post-statement adjudica – audit, that aggregation of that CDA, there will be just one signature representing the individuals that put together the CDA or the organization from which the CDAs coming from?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Well – this is Bob. It's a good question. The view at the moment is that to the extent there's more than one legal signer or authenticator of the information contained in that CDA, then there would be more than one signature. And provisions have been made for that by allowing those signatures to go into the participant constructs in the header. So a CDA could be signed by an unlimited number of individuals. The problem we work with at the moment is that the contributions are not necessarily fully identified within the CDA itself, nor are they fully identified, necessarily, anywhere else. That's going to have to change over time, but that's part of the work that we're doing as part of the esMD Determination of Coverage work – Initiative. And so we don't have an answer for all this, we know we need to be able to sign it, we don't necessarily know exactly when everything's going to be created and signed nor exactly how many signatures will be required.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
This is the practicing physician Peter Kaufman as opposed to the Informaticist, Peter Kaufman. I think it's going to be a while before we get physicians like me to digitally sign our notes at the time that they're created, although if we can do them in bulk and do them at the end of the day, one digital signature for all the notes, I think it will be more likely. But then the labs come back a couple of days later and I don't think you're going to get physicians to digitally sign all their labs off. The lab would digitally sign the records before they were sent out, possibly, but I could see possibly having a digital signature for the labs separately by the practice clinical person who is sending them off to Medicare, and they would be digitally signed, but not by the physician. Would it be possible to be sending several documents, each individually digitally signed, all CDAs to Medicare or do they want them bundled into a single CDA where it will be complicated signatures where the physician would have signed the visit note and a staff person would have signed the laboratory records?

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
This is Melanie, I'll start that answer, and then I'll turn it over to Bob to give more details. It really depends on the policy surrounding that particular service. For example, I believe that there are some lab tests where the CMS policy says, in order to be covered by Medicare, the lab results need to be noted or signed in some way by the physician. Now the physician could do that in a number of ways – out the lab results and putting a wet signature on would be one way, perhaps someday, putting a digital certificate signature on would be another way. Writing a progress note and saying I noted the labs and they're all within normal limits, blah, blah, blah, that would be a third way, whether that's done paper or electronically.

For other items and services, there is a different workflow. For example, for power mobility devices, the order has to be written by the physician, signed by the physician, sent to the supplier. The supplier has to initial that and then send back something called a detailed product description. The physician must then sign or initial the detailed product description and all of those documents, the order, the progress note and the detailed product description need to be sent to Medicare. They can all be separate documents, but they all have to be signed and dated today in wet for – wet paper format, even if it's coming in by PDF, but I can envision a day somewhere down the road where each one of those documents might be signed electronically. Bob, do you want to add to that?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Yeah, we're not trying to mandate one of anything. We firmly believe that documentation for a hospital encounter, potentially for a physician office visit that includes procedures and other things, there may be more than one CDA that gets generated and signed. That's not the goal to dictate the number; it's more to establish the process. And so I think over time, what you're going to see is that the number of documents that gets created will reflect the workflow that exists for that particular practitioner and particularly for their specialty.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
But the physic – .

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
And this is Me – go ahead.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
– I was going to say that the physicians are currently with electronic medical records, signing those labs that come in, but they're doing a one-factor authentication with a NIST Level 2 certification. That should still be appropriately acceptable if an office staff member says, the doctor signed this with their lower level authentication and I'm signing it digitally with a two-factor authentication to NIST Level 3. That's what I'm saying you should have an allowance for that, that it may be a multiple level signature by different people to allow it to reach the level where it's non-repudiable to the office staff person, but that the doctor's not required for every lab that comes in, to do a NIST Level 3 two-factor authentication signature.

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
This is Melanie and I will just point out what today's policy is at CMS for signatures. We have very detailed policies that go for pages in our manual, about pen and ink signatures. If it's legible, if it's illegible, whether it has to be dated, whether the credentials have to be listed after the signature, on and on and on. We have about one line for what to do with a digital or electronic signatures and that is, we say we defer to the judgment of our individual Review Contractor. Well that worked okay a couple of years ago, but now Review Contractors are saying, hey, what should we accept as an okay signature, digital signature. We get this PDF, it's got a bunch of numbers, it says digitally signed by Dr. Smith, MD, is that a valid signature? I have emails and letters coming in from doctors, hospitals, and other providers all the time saying, hey, we're putting in place in a new EHR system, what do we need to make sure we put in place for our electronic signature, for our digital signature. I don't have a way to answer those questions now, because we defer to the contractor and their judgment, but I need to get to the place where I can put out a policy. And that's part of what Bob –

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst
I'll be happy to drive the half an hour to help you when you want to do it, just get in touch with me and Peter Basch will come too, he's just across town.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Yeah, let me just say, we're – our focus on this is to not just establish a non-repudiation signature, it's also to make sure that it fits reasonably within a provider's workflow, whether that provider's in an office or a hospital. If it doesn't, we're not accomplishing our purpose of simplifying the administrative requirements here. So, our goal is certainly to work with provider organizations to make sure that the implementation of what we're doing fits into their operational environment in the best way possible.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Yeah, this is John Moehrke. I think one of the other ways to look at this is I think you're looking for just the legal authenticator in digital signature form, not necessarily digital signature on contributor or author or predicate. So, that may be another way to deal with this and you can then represent the initials, which effectively it's an initials if you're just saying, yup, I got the lab report in without actually doing a digital signature on it. So, there are some workflow issues there that can mesh with the technology.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Well I thought Author of Record meant that it had to be the person who actually delivered the service, not just as an authenticator, but actually the person who –

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Well, that's the question, right?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
I hear three levels that CMS is working on, the bundled document –

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

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
– all the way down to the individual contributions.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
– right. And the individual contribution is the person who performed the service, right?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Yeah, but that's like Phase 3 or Phase 2, way into the future, it's more like a hope than a – or an expectation rather than a really this is – we are going to get there by this time, is my understanding. At this point is –

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
I'd like to hear what Bob says.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Sure.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
As I said, we do not see the standards nor the technology to allow us to take it down to the level of every time an action is performed that is signed digitally. We just don't have that ability.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Well that isn't what I was asking. I was asking, you Bob mentioned that you saw them kind of signing off on a visit, a complete visit, right? And the per – and what John Moehrke said as a legal authenticator, the person who signed that wouldn't necessarily be the doctor – a – one of the doctors who participated in that visit, it would just be somebody signing off that I put all these things together. Is it a legal authenticator or is it the signature of the person who delivered the service?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Those are two separate statements. If it's going to be signing on the CDA for the work that was done, it would be the provider that actually did the work, the one that's taking legal responsibility for it.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
That's what I was asking about, right –

Melanie Combs-Dyer, RN, MS – Deputy Director, Provider Compliance Group, Office of Financial Management – Centers for Medicare & Medicaid Services
But, but, this is Melanie. Sometimes the coverage requirements go further than that. For example, the blood work that Walter had done this morning had to be signed by the lab, but also had to be s – well, he may not be over 65, so he may not be on Medicare yet, but if he was a Medicare beneficiary, he may have had to have had his physician somehow note those lab results. And we would not cover it in Medicare if it was ticked for review, unless the lab signed it and the physician made note of it.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay, that's really what I was asking. It sounds like, yeah, it's a medical person that signs it, not just a legal authenticator like a –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Yeah.

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

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
But the legal authenticator can be the doctor, it's just the physician deems that the doctor is not attesting that they are the author of all of the things in the document, they are attesting that they have put this document together.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
It's sort of the difference between slide 25 and slide 27 of the deck. Slide 25 looks at the documenting encounter component and all the various people that are involved in the signing of the various parts of that document encounter. And then slide 27 talks about the signing of the CDA, which is the entire document.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Well remember, we're allowing, and we've done with the CDA – this is Bob. We've allowed them to have multiple signatures. So for example, if this were an operative procedure that had co-surgeons on it, they would both sign it. If this –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
At the CDA level or at the inside the template level?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
At the CDA level.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Oh, oh, okay. So at the CDA level, there's – you said it I guess, there's an opportunity to, at the CDA level, have multiple signatures.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
Yes.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
But how do you know which signature goes with which component inside the CDA?

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
That's where we have a bit more of a challenge, and I've been trying to work with Bob Dolin on that, and it may be something we resolve in the future –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Okay.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
– where we have the signatures going on where you're claiming the role as part of your signature. And eventually what we do is we make sure that every contribution, for example, entry into a section – a section level template, entry-level template, also have a contributor to them. We've got some work to do we're not there yet.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Yeah, the other model is that each of those contributions are published as a document and has the appropriate signature on the document.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
And that is correct.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Essentially if you tear apart a paper workflow, that's often times how the paper workflow is viewed.

Robert Dieterle – esMD Initiative Coordinator, Signature Consulting Group – Centers for Medicaid & Medicare Services
And there's nothing in the design we're creating that would prevent that either.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare
Right.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay. Well, I notice we've actually gone one minute over so; we need to wrap this up. I want to thank once again Melanie and Bob and Debbie for an excellent, excellent session. So we really appreciate it. With that, I think that we will turn this over to public comment if there are any and then we'll sign off. So –

Public Comment

Rebecca Armendariz – Altarum Institute
If you would like to make a public comment and you are listening via your computer speakers, please dial 1-877-705-2976 and press *1. Or if you are listening via your telephone, you may press *1 at this time to be entered into the queue. We have no comment at this time.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates
Okay. Than – my thanks to everybody for dialing in and to our participants. Have a good one.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente
Thanks.

Public Comment Submitted During the Meeting

1. When a provider signs off on their notes at the end of a visit could the digital signature of the CDA happen concurrently? This would prevent additional steps for providers at the time of CDA request via esMD.