CENTERS FOR MEDICARE AND MEDICAID SERVICES
National HIPAA Security Roundtable
November 10, 2004
1:00 pm CT

Operator: Good afternoon, ladies and gentlemen. My name is (Tina) and I will be your conference facilitator today.
At this time, I would like to welcome everyone to the HIPAA Roundtable. All lines have been placed on mute to prevent any background noise. After the speakers' remarks, there will be a question and answer period. If you would like to ask a question during this time, simply press star then the number 1 on your telephone keypad. If you would like to withdraw your question, press the pound key.
Thank you.

Ms. (Holland), you may begin your conference.

(Elizabeth) Holland: Hello and welcome to the 17th National HIPAA Roundtable call. This call is being conducted by the Centers for Medicare and Medicaid Services or CMS, which is part of the US Department of Health and Human Services.

We began conducting these calls in March of 2002 to facilitate the implementation of the Health Insurance Portability and Accountability Act of 1996, or HIPAA. And more specifically, the Administrative Simplification provisions.

Today's call will focus on HIPAA security. We will begin with our first speaker Nathan Colodney, Director of the Office of HIPAA Standards in CMS.

Nathan Colodney: I'd like to thank everybody for joining us today. As the new Director of HIPAA Standards, I appreciate everybody joining this conference call to learn more about these Security rules.

The Security Rule is intended to ensure three main points -- confidentiality, which is who can see data; integrity, that is the information has not been altered or destroyed; and the availability of data -- that is that the information can be accessed when needed.

The HIPAA Security Rule compliance date is April 20, 2005, so it's rapidly approaching, as I am sure you all realize. We would like to make sure that all covered entities have this information, for which you are calling in today, to ensure that you are able to comply and provide the opportunity to ask (unintelligible) questions.

We have prepared a presentation to cover the basic principles of the Security Rule, and then the lines will be open to take your questions.

Today we are joined by representatives from throughout the various components of the Centers for Medicare and Medicaid Services to provide you with the most comprehensive answers and a wide range of perspectives.

(Elizabeth) Holland: Thank you.

Our second speaker today will be (Brad Peska) of the Office of HIPAA Standards.

(Brad Peska): Thank you very much, (Elizabeth).

I am (Brad Peska) from the Office of HIPAA Standards, and I'm responsible for providing information and security expertise within the office.

I'd like to take a couple of minutes to walk you through the HIPAA Security Rule. I want to review some of the general concepts that make up the Security Rule and then give you a high-level review of each of the standards themselves.

During this presentation, I'm going to be referencing material from the Federal Register version of the Final Security Rule and specific frequently asked questions (FAQs) that have been posted to the CMS web site on Security Rule topics. I think it's important to make sure everyone understands that the material that we're all working from is the Federal Register version of the Security Rule.

We're all working from the same starting point, and what I want to do today is go through that material with you.

As Nathan mentioned, covered entities have approximately five months until the deadline for security compliance, and that will approach rapidly. Covered entities must be in compliance no later than April 20, 2005, except small health plans, which must be compliant no later than April 20 of 2006.

We've structured the Security Rule to provide covered entities with the ability to meet the standards that have been included in a variety of ways. But it's important to lay the ground work of what the Security Rule covers within a covered entity. What information are we really referring to?

In the context of the Security Rule, we are concerned with electronic protected health information, or we may also refer to that has EPHI. And that is any

electronic protected information that a covered entity creates, receives, maintains, or transmits within their environment.

So it really covers the full range of electronic PHI that a covered entity may have.

In the general requirements section of the Security Rule, we require the covered entities, as Nathan mentioned, ensure a couple of key properties - the confidentiality, integrity, and availability of the electronic protected health information.

Briefly again, that's making sure the right people can see it from a confidentiality standpoint, and only the right people can see the information; making sure that the integrity of the information is maintained, that no one unauthorized alters or destroys that information; and maintaining the availability of it. Only the right people are able to see the electronic protected health information within the covered entity.

We also allow - or we also require covered entities to protect against reasonably anticipated threats and hazards to the security and integrity of electronic PHI in their environment.

We also require that covered entities protect against any reasonably anticipated uses and disclosures. And this is a direct tie-in with the Privacy Rule requirements that covered entities are already required to be in compliance with.

We also make sure that we are very clear that covered entities also need to ensure compliance by all members of the workforce, and that the workforce in addition to those individuals responsible for compliance activities keep the

covered entity in compliance. So there is also - there also needs to be inclusion of all workforce members.

We have allowed an additional level of flexibility, scalability, and technology-neutral themes within the Security Rule itself.

We understand that the covered entities that make up those that are covered under HIPAA itself are - vary in a wide range of characteristics. We have covered entities from small health plans with single physicians all the way to the largest health insurance employers covered entities out there in the industry.

And we realize that no single security standards are going to fit for all of those entities. So we have allowed covered entities to take into consideration certain factors that make up their environment when they are determining what security measures and how to meet compliance.

We address those in the Security Rule, and those factors include the size, complexity, capabilities of that covered entity, the technical infrastructure, the cost of security measures, as well as potential risks to the electronic PHI within their environment.

So we also knew that developing the Final Rule that we had to make the role of technology neutral. We are not in a position and the rule does not prescribe the use of specific technologies.

So what we have allowed covered entities to do is again determine what fits best for their organization and allow them to use technologies that will enable them to meet the rule while still allowing for future advancements in technology and future implementations of technology.

We also made sure that we were comprehensive in the standards. As you will notice looking through the requirements that the majority of them are not just technical in nature. They are policy, procedure, and process-related. And this ties back into the concept of being - of all workforce members within a covered entity assisting with compliance.

We also lay out the concepts of having standards and implementation specifications of the rule. All covered entities must meet the standards of the rule. And again, I will go through most of those standards today.

In addition, there are implementation specifications. Implementation specifications provide more detail of how a covered entity will comply with the standards.

We have also allowed as I mentioned the additional flexibility under the rule by making implementation specifications required and addressable.

As it sounds, all required implementation specifications must be implemented, but addressable implementation specifications require that a covered entity goes through an additional analysis of how they will implement the implementation specification in their environment.

It is important to note that addressable implementation specifications are not optional. There is a process that covered entities must go through to determine whether the specification is reasonable and appropriate for their environment.

And I want to briefly walk you through that process. We also described this in the rule itself.

A covered entity when addressing an addressable implementation specification, if that specification is reasonable and appropriate, the covered entity should implement it in their environment.

If the listed addressable specification is not reasonable and appropriate, the covered entity can implement an equivalent alternative measure that still meets the intent of the standard.

If the addressable specification as written or an equivalent alternative measure are not reasonable and appropriate for the covered entity, then the covered entity may not implement either the specification or an equivalent alternative measure based on the risk analysis and organizational factors that we described - the size, capabilities, complexity, cost of the covered entity.

So there is a process that you must go through when determining how to address the addressable implementation specifications.

We also made sure that the covered entities understand that there is a requirement to maintain compliance on an ongoing basis, to maintain the security measures that have been implemented for compliance activities.

The HIPAA Security Rule is an ongoing process within covered entities, and it's not just a one-time goal. We have included a standard for maintenance, as well as another standard that I will briefly go through for evaluation within a covered entity whereby those - these two processes, a covered entity can ensure compliance on an ongoing basis.

So I've mentioned a couple of the standards and the sections of the Security Rule, but I want to get into a little bit of detail on what they actually are and what the rule states.

There are six main sections in the Security Rule. We have just gone over the first section, the security standards general rules.

The remaining sections of the rule are the administrative, physical and technical safeguards, the organizational requirements, and the policies, procedures, and documentation requirements.

Under the Administrative Safeguards, which is Section 164.308 of the Security Rule, the first standard is the security management process. The security management process requires covered entities to implement policies and procedures to prevent, detect, contain, and correct security violations.

This is the standard that allows covered entities to shape their compliance program. In this particular standard, we have implementation specifications which are required.

A couple of those implementation specifications - risk analysis and risk management - really lay out the ground work for a covered entity's compliance program and decisions that they will make with compliance with the rule.

We do identify in recently published FAQs that risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the EPHI held by a covered entity and the likelihood of this occurrence happening.

Whereas the risk management process is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising the electronic PHI within its environment.

These are very important concepts, and as I mentioned do shape how a covered entity will comply with the rest of the standards in the rule.

The next standard is assigned security responsibility. All covered entities must have assigned security responsibility to an individual that is responsible for the development and implementation of policies and procedures required by the Security Rule.

We do have a discussion of the options that covered entities have in relation to this standard in the preamble of the Federal Register version of the Security Rule, but it is important to note that all covered entities must have a single individual with assigned security responsibility.

The next standard, workforce security, and the standard after that, information access management, kind of go hand in hand.

The workforce security standard allows - requires covered entities to implement policies and procedures to ensure workforce members have access to the electronic PHI in the environment while preventing those who don't have access from obtaining it.

The access requirements themselves are a part of the information access management standard, which requires covered entities to implement policies and procedures for authorizing access to EPHI that's consistent with the requirements that are outlined in the Privacy Rule.

And this is a specific reference to the uses and disclosures that the Privacy Rule requires covered entities to put in place.

Moving on, we also look at the next standard, security awareness and training.

As I mentioned, having the workforce members (be) in compliance and assist the covered entity with compliance is a requirement of the rule, and the security awareness and training standard really steps up that program, and it requires covered entities to implement a security awareness and training program for all members of the workforce, including management.

And it's very important to identify that even those individuals who may be responsible for certain functions in the environment in a management capacity also need security awareness and training.

The next standard, security (incidents) and procedures requires covered entities to have policies and procedures to address security incidents, and specifically the response and reporting of security incidents within their environment.

We also have under the Administrative Safeguards a requirement for contingency plans. The contingency plan requirement is a policy and procedure for responding to an emergency or other occurrence that damages systems that contain the electronic PHI within the covered entity.

This particular standard also has required and addressable implementation specifications that a covered entity must address when looking at the standard itself.

As I mentioned earlier, there is also a standard for evaluation. The evaluation standard requires covered entities to perform a periodic technical and non-technical evaluation of their environment in relation to the Security Rule, and then on an ongoing basis to respond to environmental or operational changes that affect the security of the electronic PHI.

And the final standard in the Administrative Safeguards section is the business associate contracts and other arrangements. This particular standard requires covered entities to have business associate agreements, much like the Privacy Rule standards for business associate agreements.

The standard was purposefully linked to that concept in the Privacy Rule, the details of which, of what the contract must have in it are covered in the organizational requirements section that I'll speak to later.

So those are the standards within the Administrative Safeguards portion of the rule.

At this point, I want to move on to the Physical Safeguards.

The Physical Safeguards, the first standard is facility access controls. This requirement is for policies and procedures to limit physical access to electronic information systems in the facilities in which those information systems are housed, therefore ensuring that properly authorized access is allowed to electronic PHI.

The next two standards, workstation use and workstation security in the Physical Safeguards section, require first of all for covered entities to have policies and procedures that specify the functions that can be performed on workstations and the manner in which those functions are performed, as well

as the physical attributes of the surroundings of a specific workstation or a class of workstations that have access to electronic PHI. Again, the key here being workstations that have access to electronic PHI.

And then the workstation security standard is the actual requirement for implementing physical safeguards for these workstations that access the EPHI.

The last standard in the Physical Safeguards section is device and media controls. Device and media controls requires covered entities to implement policies and procedures that govern the receipt and removal of hardware and other electronic media that contains electronic PHI in to and out of the facility.

This standard also has required and addressable implementation specifications.

Moving on to the Technical Safeguards section of the rule, it's important to note that there are also several FAQs that have been posted to the CMS web site that address various issues under the Technical Safeguards portion of the rule, one of which is does the HIPAA Security Rule mandate minimum operating system requirements for personal computer systems used by a covered entity.

And the answer to that question is no, given that the operating system could be one component of the information system, and the rule itself again allows the flexibility for covered entities to select a technology that best fits their organizational needs.

And considering that the operating system is one component of an information system with electronic PHI, a covered entity has the flexibility to choose how that information system will be implemented to meet compliance activities.

The first standard in the Technical Safeguards section is access control. And access control requires covered entities to implement technical policies and procedures for information systems with electronic PHI that allow access only to those persons or software programs that have been granted access under the information access management standard that we discussed in the Administrative Safeguards portion of the rule.

So this is the actual implementation of technical policies and procedures that perform access control functions.

We also see the next standard is audit controls. This standard requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

It's important to identify here that hardware, software, and/or procedural mechanisms can be used for a covered entity's compliance per the rule.

The next standard is integrity. This standard requires covered entities to implement policies and procedures to protect electronic PHI from improper alteration and destruction.

Again, this is in the Technical Safeguards section, but it is also a key property that we discussed in the general rules that covers all information, all electronic PHI within the covered entity's environment.

The next standard is person or entity authentication. This requires implementation of procedures to verify that a person or entity seeking access to electronic PHI is the one that's claimed.

This standard in many cases works with the access control standard in which a person or entity actually has procedures for authentication once they've been granted the appropriate access.

The next standard under this section, Technical Safeguards, is transmission security. This standard requires covered entities to implement technical security measures to guard against unauthorized access to electronic PHI being transmitted over electronic communications networks.

It's also important know with this standard that several FAQs have been published addressing the use of email or the Internet for transmissions of PHI within a covered entity, or into and out of a covered entity. What encryption really means in that transmission process, and if it is allowable to use those mediums for transmission.

And in general, when we talk about encryption itself, we further clarified in an FAQ that encryption is actually the method of converting an original message of regular text into encoded text whereby an algorithm or mathematical formula would be used in that process, making the information encrypted and so that there would be a low probability that anyone other than the receiving party would have a key or a code to access the information would be able to decrypt or translate that text into plain information that could be viewed.

In addition, we also identified that encryption is an addressable implementation specification in the Final Security Rule. This means as I mentioned before that covered entities must go through the analysis of whether encryption is the appropriate option, or if equivalent measures are needed when transmission of electronic PHI is taking place.

So the FAQ specifically addresses is mandatory encryption in the Final Security Rule, and the answer is no. Covered entities must determine what the specific instances and what methods will be used for protecting transmission security.

And since the encryption specification is addressable and that since we realize that there are no single interoperable encryption solutions for communicating over open networks currently in the healthcare environment, we felt that setting of a single standard for encryption would have placed an unfair financial or technical burden on some covered entities.

So again, we have allowed additional flexibility in the case of encryption, much like other areas of the rule.

We also make the distinction that the Security Rule does not expressly prohibit the use of email for sending electronic PHI, although there are many standards that come into play that a covered entity must review when determining if email will be a method of transmitting electronic PHI. The rule does not expressly prohibit its use.

And again, I would refer you to the FAQ on that specific issue as well.

As we move on to the next section, organizational requirements, this is where I mentioned before we have a link to the business associate contracts and other arrangements that we discussed in the Administrative Safeguards portion.

In this particular standard, business associate contracts and other requirements, the rule requires business associate contracts or other arrangements between a covered entity and its business associate or other

arrangements such as memorandums of understanding between a covered entity and its business associate when both organizations are government entities.

The next standard in organizational requirements is the requirements for group health plans. In this requirement, group health plans are required to ensure that the plan documents of the group health plan provide that a plan sponsor will reasonably and appropriately safeguard electronic protected health information that's created, received, maintained, or transmitted to the plan sponsor on behalf of the group health plan. And there specific requirements or implementation specifications that the plan documents must contain.

And finally, the policies, procedures, and documentation section of the rule has two main standards, the first being policies and procedures, which requires covered entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule, taking into account among other things the general rules of the Security Rule which cover the factors that make up the covered entity's environment -- the size, capabilities, complexities, et cetera.

And the last standard under policies, procedures, and documentation is documentation, which requires covered entities to maintain the policies, procedures, actions, activities, or assessments implemented to comply with the standards in written format -- which may be electronic -- and also provides required implementation specifications for the time limit, availability, and updates to that maintains documentation.

I think it's important to identify that as we have gone through, you know, relatively quickly these standards, again if you haven't downloaded a copy

already of the Security Rule, you can go to the CMS web site to do so. It's important to actually review this material for yourselves, especially those of you that are responsible for implementation activities and determine exactly what the rule is requiring of covered entities.

And considering that we weren't able to get into the direct implementation specifications, it is also important to not lose sight of the fact that there are additional requirements for covered entities that weren't directly discussed on the call today.

Overall we feel that through the Security Rule, we have provided covered entities with flexibility for implementation that best fits their environment. We feel that these standards identify business decisions that covered entities should make and we think are good business decisions for covered entities to make in relation to implementing a standard set of security practices for all covered entities.

And with that I want to make sure that we allow for time for questions and I'll turn it back to (Elizabeth).

(Elizabeth) Holland: Thank you, (Brad).

We will now respond to questions. Callers, please begin your question with your name and your organization. Now I'm going to ask our operator (Tina) to remind our audience of the procedure for asking questions.

Operator: Thank you.

Ladies and gentlemen, if you would like to ask a question, you may do so by pressing star then the number 1 on your telephone keypad.

And your first question will come from the line of Raynetta Adams.

Raynetta Adams: Hi. I'm from Delaware Valley Community Health in Philadelphia.

And I wanted to know if there was written presentation with this conference call, and where I could find it on line.

(Elizabeth) Holland: I'm just going to interrupt for - when participants here respond to the questions, please start with your name.

(Brad Peska): Okay.

In general, there's not a - sorry, this is (Brad Peska). I figured since I just spoke that maybe people would recognize the voice. This is (Brad Peska).

In general, there is not a direct written presentation, but the material that I'm using here is like I mentioned from the Security Rule itself as well as frequently asked questions on the CMS web site, the HIPAA Administration Simplification web site.

Raynetta Adams: Okay, thank you.

(Elizabeth) Holland: Next question please.

Operator: Your next question will come from Sebastian Sullivan.

Sebastian Sullivan: (Unintelligible).

Operator: Ma'am, I'm sorry. Your line is distorted.

Sebastian Sullivan: Okay, is that better?

Operator: No, ma'am.

Man: No.

Operator: If you are on the speaker phone, please pick up your handset.

Sebastian Sullivan: I don't have a handset.

Is there a place I could email the question?

(Elizabeth) Holland: Yes, you can. You can email the question to CMS and the address is askhipaa@cms.hhs.gov.

Sebastian Sullivan: Thanks.

Operator: Next we will hear from the line of Ron Giles.

Ron Giles: Yes, this is Ron Giles, Oncology Hematology Associates in (Evansville).

With the implementation of the policy, a part of the security is auditing. And is anything really stated as far as the length of time auditing files need to be saved?

(Brad Peska): That's a very good question.

At this time we don't have additional details about the length of time that audit information must be retained or even the detailed content of the audit material itself. I assume there will be additional questions on that.

I assure you that we do have this as an issue that we are actively working on for future clarification, which will probably come in the form of frequently asked questions again posted to the CMS HIPAA Administration Simplification web site.

Ron Giles: Okay, thank you.

(Brad Peska): You're welcome.

(Elizabeth) Holland: Thank you, (Brad). Next question.

Operator: Next is Chris Williams.

Chris Williams: Hi. I'm calling from Employee Benefits Institute of America.

And under the Privacy rules, conduits which would transmit PHI were carved out from the business associate category.

Considering that under security transmission is specifically one of the things that has to be taken into account and has to be protected when you're transmitting electronic PHI, I'm wondering if the same carve-out from business associates or conduits applies in security.

(Stanley Nachimson): Hi, this is (Stanley Nachimson).

And let me make sure that I understand your question and I think we can explain it.

I think what you're saying is that the (lines) themselves that carry the information, whether it's an Internet service provider or some private network were carved out, that those people were not to be considered business associates under the security - under the Privacy Rule so that business associate agreements were not necessary.

I think that's what you're referring to?

Chris Williams: Correct.

(Stanley Nachimson): Yeah.

And I think we would agree that these additional folks, the (unintelligible), Internet service providers would not be considered business associates nor covered entities under the Security Rule.

Chris Williams: Thank you.

(Elizabeth) Holland: Thank you, (Stanley). Next question please.

Operator: Your next question will come from the line of Jason Taule.

Jason Taule: Hi, how are you?

(Elizabeth) Holland: Great.

Jason Taule: The question is could you review for organizations that don't specifically fall as one of the covered entities what some of the criteria will be for the applicability of organizations and whether or not they have to comply with the rules.

(Brad Peska): That's a good question.

Covered entities under HIPAA and specifically (unintelligible) under the Security Rule are health plans, healthcare clearinghouses, and healthcare providers that transmit health information electronically in connection with the named transactions in HIPAA.

And I would refer you to the actual standards themselves to get further clarification on the definitions of those entities that I just identified.

And again, this is (Brad Peska).

Jason Taule: If we're definitely not one of them, but we're likely to be a business associate of those covered entities, even - I don't want to wait until I get specifications defining what security I must provide in order to satisfy their subject requirements.

Are you with me? If I'm a...

Man: Right.

Jason Taule: ...handshake away, should I basically be following this as though I were a covered entity?

(Crosstalk).

Man: If you are not a covered entity then your organization is not subject to the requirements of any of the HIPAA rules.

If you are a business associate, the requirements that you would have to follow would basically be spelled out in the business associate agreement that you would have if you are a business associate of a covered entity.

We have some general requirements for what has to be in those business associate agreements, but again that's a requirement of the covered entity to ensure that those are in the business associate agreements.

That's not the requirement of the business associate.

Jason Taule: Yeah.

I don't mean to press the point, but that - let me give you a specific example and maybe that'll help me clarify because, again I don't want to wait for them to dictate terms to me in three or four months from now and I've only got a month or two to respond.

Let's just say I ran the data center for a hospital. Obviously we're going to have as an outsider, as an outside service provider under a managed service contract. Clearly it's going to be a business associate agreement there.

Would we be expected to provide to HIPAA as though we were the covered entity?

Man: You know, in this instance I don't think we can necessarily answer the direct question of the contractual relationship there.

But I think it's important if you want to get a head start on the requirements themselves and what covered entities that must comply with the rule will have in their agreements...

Jason Taule: Okay.

Man: ...then you can look at Section 164.314 of the Security Rule, the organizational requirements, specifically the business associate contract and other arrangement requirements that fall into that section and probably get a little bit better detail there on what you would be expected to do as a business associate.

Jason Taule: Last follow-up I promise to that.

If we get the required business associate contract that spells out what we have to satisfy, but that doesn't come for several months, is there an additional timetable other than the April 20 deadline by which those at arms length have to comply?

(Stanley Nachimson): I - this is (Stanley) again.

Those at arms length, again business associates don't have any timetable to comply (unintelligible). The requirement and the timetable is on the covered entity.

So the covered entity is the one that's in some sense libel if their business associate doesn't comply by the appropriate compliance date.

Jason Taule: Can I get that in writing?

(Stanley Nachimson): Excuse me?

Jason Taule: I said can I get that in writing?

Okay, thank you.

(Elizabeth) Holland: Thank you. Next question.

Operator: Your next question will come from Scott Wright.

Scott Wright: Hello. This is Scott Wright from WellPoint Health.

I have a question under the Technical Safeguards, in particular the safeguard that is integrity.

It talks about a mechanism to authenticate EPHI, and again because this is under the technical area, although I recognize that it's addressable, my question is if you can give a little more guidance on what is expected here.

Man: Again at this time we can't give additional details on this particular standard.

I would say especially when you're looking at requirements or implementation specifications that are addressable, there are many options that you would have from a technical aspect for implementing.

And I'm not able to give specifics at this time because it would be deemed you know, something that covered entities would have to implement when in fact depending on how they chose to implement what their technical situation would be and their technical capabilities would be.

It may not apply to all covered entities, so it's just difficult for us to give an answer that wouldn't be seen as applying to all covered entities.

Scott Wright: I have - I can appreciate that view that my - I guess my concern is that when I look at the hundreds of thousands of transactions that happen in a large organization, looking at a mechanism that's going to be able to authenticate the - an electronic mechanism that would be able to authenticate that only those that are authorized to have made that transaction, it seems to be a pretty good-sized undertaking.

So I'll look back through my own organization and in the future maybe we'll get a little more specification on exactly what it is that we're supposed to do.

(Elizabeth) Holland: Okay, thank you. Next question.

Operator: Your next question will come from the line of Debbie Johnson.

Debbie Johnson: Yeah, actually I was looking on the CMS web site and found what I needed, so.

(Elizabeth) Holland: Great.

Debbie Johnson: Okay?

(Elizabeth) Holland: Thank you.

Debbie Johnson: (Uh-huh).

Operator: Your next question will come from Sheila Method.

(Elizabeth) Holland: Hello?

(Frank): Hi, this is (Frank) and Sheila from Memorial Healthcare in Owosso, Michigan.

My question has to do with authentication, and I think I know what your answer's going to be already - refer to the web site or whatever's reasonable and adequate. But I'll ask it (anyways).

Is there anything that describes password complexity or the amount of time that a password has - you know, can be changed and the regularity of password changes.

Any detail that we can, you know, use?

(Brad Peska): (Frank), this is (Brad Peska) again.

I'll answer your question a little more directly than the others in that the rule does not have specific requirements for password standards identified. This would be an area that - to getting kind of the other standard answer, this would be an area that you would have to determine based on other requirements or characteristics of your environment what those password characteristics would be. The requirement under - or the standard in the Security Rule is to have person or entity authentication.

So does that help at least a little bit?

(Frank): Not really, but it just seems like password complexity, it's pretty clear that there should be a minimum requirement of the complexity of a password. I

mean, I - just in certain environments I think you've got to have some complexity there. I mean, (unintelligible) some environments that (unintelligible) password that never changes is going to be adequate.

(Crosstalk).

Man: I would agree (Frank) that overall that that is a valid concern, and as an information security professional, there - you know, I understand the issues that you're identifying there.

But purely from a Security Rule standpoint, there are no specifics identified under the rule that relate to your question.

So that doesn't mean that you couldn't set your own -- and for that matter shouldn't set your own standards for a password complexity and password, you know, management and the password standard may be within your environment.

But it's not something that is mandated by the Security Rule.

(Frank): Okay. Thank you.

(Dan Jacobs): Can I do a follow-up question on that?

Man: Yeah.

(Dan Jacobs): This is (Dan Jacobs), with these people also.

Just the one problem that maybe some of us are hearing is on the one hand we are being told by supervisors or managers that to check this out, find out what the information is, and come back to them with what we're supposed to do.

When in actuality it sounds like reasonable and adequate and all of the rest of these themes, which really don't tell you anything is what you're saying, is standard.

So when we go back to our supervisors or managers, we can't really tell them concretely they want a minimum of this and a minimum of that, a minimum of the other thing, and then if we want to do beyond that we can, so that they can approach the board and say well this is what the standard is in order to do it, they've researched it and found out these are the costs that are associated with it.

Instead we're going back and saying we don't know, it's up to our discretion, we have no idea if we're going to be compliant or not, other than to say that we've done a reasonable and adequate job.

(Stanley Nachimson): This is (Stanley Nachimson), and I certainly understand that point of view and the necessity for you to go back to your supervisors or your board to explain what would be right.

The approach that we took for - in the Security Rule though is to place the responsibility about what would be right for your organization essentially on you.

The risk analysis that we talk about as a required implementation specification is really the basis that you'll use, and you can present to your management as to what needs to be done along with the other factors in your organization.

You've got the flexibility to make some decisions about what the minimum is right for you.

We were very uncomfortable setting minimums in a lot of cases because they might have been too cumbersome for certain organizations and not cumbersome enough for other organizations.

So it's very important that you look at the circumstances of your own organization and determine what's right for you. There is a requirement for authentication for example. There is a requirement for integrity, just to reference the previous question.

But it's important to look to see what is the best way for your organization to meet those requirements, as opposed to simply meeting an arbitrary minimum that we might have come up with.

(Dan Jacobs): It sounds like what's clear here is when we go through this process of determining what's reasonable and adequate that we better document our butts off so that when something - litigation does happen, we can pull out our documentation to show that this is how we figured out what was reasonable and adequate for our organization.

(Stanley Nachimson): I think that's accurate, and you'll note that we did state that documentation is a requirement in the regulation.

So you can certainly present that to any - to your superiors and say not only do we have to make these decisions, but it's clear in the regulation that the decisions that we make and the analysis that we do must be documented.

(Dan Jacobs): Okay. Thank you.

(Elizabeth) Holland: Great. Thank you. Next question please.

Operator: Next we will hear from the line of Camille Orso.

Camille Orso: Hello.

I'm not sure you're going to answer this question as directly as I'd like you to, but given that the state of outside user access auditing controls in the healthcare industry is pretty poorly developed, and we're looking at having many systems in any one hospital that have PHI within them, as we're trying to figure out what's a reasonable and doable approach, are there any resources in the industry that you would direct us to for advice on how to proceed?

(Brad Peska): This is (Brad Peska) again.

You know, overall - and we've made this statement in a couple of forums as well as we have in FAQ on the topic, in the past we've referenced specific documents, and there are some documents such as the NIST materials, the National Institute of Standards and Technology materials identified in the preamble to the Security Rule.

But in general, Health and Human Services, CMS, and the Office of HIPAA Standards don't endorse any specific external documents.

However, we identify that material from certain professional industry organizations, local groups that you may be affiliated with, or even information sharing between covered entities that are working towards compliance activities may be valuable for covered entities.

But there are no specific resources that we can provide you with. We do require that covered entities determine for themselves the value of any external resources, and again, you know, remind you that compliance is a requirement of a covered entity.

And just because you're using certain materials doesn't necessarily mean that you are guaranteed to be in compliance. It also doesn't guarantee that you'll be out of compliance either, but that's just an evaluation that each organization has to make for themselves.

But I will, you know, mention that there are valuable resources out there that you can use for compliance activities. We're just not able to directly identify them.

Camille Orso: Okay.

I guess another question is there are obviously many different kinds of things that you could audit, from, you know, system availability and performance through log on or attempts to get access privileges that are not appropriate to inappropriate use of within appropriate access privileges.

Is there any direction from CMS on where to put your emphasis?

(Brad Peska): Again, that's another good question. This is (Brad) again.

I think again the important thing to remember is that audit controls is one of the areas that I mentioned earlier we're still looking at providing additional clarification on, including what the content of the audits may be.

So at this time I'm not able to give you any more information, but I will assure you that we have this issue as one of the top priorities to try to provide additional clarification out to the industry.

We realize that this is an issue that many covered entities are dealing with, and we want to make sure that we provide you with a clearer accurate answer that's going to fit for the entities that, you know, are covered by the rule.

Camille Orso: Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Next we will hear from the line of Regina Hattman.

Regina Hattman: Hi. This is Regina Hattman from Ohio Valley Hospital. I'm near Pittsburgh.

And I have a question concerning workforce training. In the Privacy Rule, you're required to do it every three years and whenever the policy has changed.

What do we have to do as far as security?

(Brad Peska): That's another good question, Regina. This is (Brad Peska).

The requirement under the Security Rule itself for security awareness and training is for a covered entity to implement security awareness and training for all workforce members.

It includes addressable implementation specifications that provide additional content if you will, or considerations for the security awareness and training

standard. But we do not identify specific timeframes for the training to be performed.

There is a discussion of security awareness and training in the preamble to the Security Rule that will allow you to determine what works best for your environment as far as how often to provide awareness and training.

You can also note that the first addressable specification under awareness and training for security reminders requires periodic security updates to the organization.

So again, that could be - that could take on different forms for different covered entities. But we don't define directly what periodic is.

Regina Hattman: Okay. Thank you.

(Brad Peska): You're welcome.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question will come from the line of Ashley Akers.

Ashley Akers: Good afternoon.

Maybe this question has already been answered, but I just wanted to kind of clarify myself.

We are considered a business associate and we have contracts of course with our covered entities. But say they broke one of the privacy acts. Would we be as liable as they would, since we do have a contract?

Man: I don't want to address privacy violations because that's not - well, one that's not the topic of this call and number two, that's not the responsibility of CMS, so we'll assume that the talk about an alleged - a possible security violation after April 20 of 2005.

The covered entities are the entities, the organizations that are liable or are bound to follow the requirements of the Security Rule. Business associates are not.

The panel piece for violations of the Security Rule may be something that would be included in a business associate contract. It may not be.

But in terms of enforcement of the Security Rule, we would only enforce against the covered entity. And that enforcement might take the form of a discussion or an attempt to resolve the issue and not involve any type of financial or other liability.

It would - we've been trying to take a tack in the (transaction and code set) enforcement of trying to work out the problem through a corrective action plan or through a resolution before we would move on to any other measures.

So again, our enforcement of the Security Rule would be against the covered entity, not the covered entity's business associate.

Ashley Akers: Okay.

And what is the exact web site address for the Security Rule?

(Elizabeth) Holland: Our web site is www.cms.hhs.gov/hipaa/hipaa2.

Ashley Akers: hipaa2?

(Elizabeth) Holland: Just the number 2.

Ashley Akers: The number 2. Okay. Thank you very much.

(Elizabeth) Holland: You're welcome. Next question please.

Operator: Next we will hear from Pebble Pramann.

Pebble Pramann: Yes. Pebble Pramann from Shepard Staff Christian Counseling Center.

I know that with privacy we're talking about all PHI, security focusing in EPHI.

And - but in some of the other CMS-(Sharp) work group things they were talking about as we develop the security, we may also want to be developing the policy and procedures as it relates to other PHI and center PHI, corporate PHI, whatever you want to call it.

But anyhow, my question is in developing our security policy and procedures, do we need to isolate the EPHI portion of it? Or can it be in the policy and procedures manual for security alongside paper PHI security policy and procedures?

(Brad Peska): This is (Brad Peska).

In general in the rule, we don't require a specific way that a covered entity needs to document their policies and procedures. But there are requirements of course for the content that we discussed earlier.

I would say that if that is an approach that your organization feels is reasonable and appropriate and would work, that is a potential option for how you could manage documentation.

But there is no specific mandate of how that would be performed, so either of those options, whether it's addressing electronic along with or if it's keeping separate policies, if that's what works, it would be a business decision in that case.

As long as of course the covered entity is maintaining that documentation and making it available to the appropriate individuals when needed, et cetera, the things that we mentioned as part of the documentation standard itself.

Pebble Pramann: Right. Okay, thank you very much.

(Brad Peska): You're welcome.

(Crosstalk).

Operator: Your next question will come from Paula Ciotti.

Paula Ciotti: This is Paula Ciotti from Blue Cross Blue Shield of Rhode Island.

Both the Privacy and Security rules require that in order to disclose protected health information to a plan sponsor of a group health plan, the plan sponsor has to amend the plan documents with certain enumerated provisions.

The Privacy Rule also says that in order to disclose information to the plan sponsor, the plan sponsor has to certify that the plan documents have been amended.

There is no certification requirement in the Security Rule, so we - you know, is this an oversight or an intentional - you know, do we need to require a certification to have security language included in the plan sponsor's plan documents before we disclose EPHI?

(Stanley Nachimson): This is (Stanley).

No, there is no requirement in the Security Rule for that certification. Just the requirement that the appropriate language be in the plan documents.

Paula Ciotti: Okay. Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Lori Grudzien... Ma'am, your line is open... I'm sorry, she has withdrawn.

Your next question will come from the line of Michael Smith.

Michael Smith: Hello. My name is Michael Smith at Parkland Hospital. My question concerns the audit trail.

Within your document here it is stated that the audit trail does not - the Privacy Rule does not incorporate a requirement for an audit trail, but you do want us to provide accounting for certain disclosures.

The issue we have at Parkland is that we have several applications. The larger applications come with an audit function, but a lot of the smaller ones don't.

And so can we take a sampling to address this requirement?

(Brad Peska): This is (Brad Peska) again.

I think, Michael, it's important to make sure that we're making a distinction with some of the terms that you use there as well.

The Security Rule has a requirement - or a standard I should say for audit controls. The Privacy Rule has a standard for an accounting of disclosures. Those are two separate requirements within each rule.

So I'm only in this instance going to speak to the audit controls requirement itself, and as I mentioned it's not something that we can get into additional detail on.

But we will be providing an FAQ in the future that provides more details on the specific standard.

So I just want to make sure also that it's important to understand the - that those two standards, from the Privacy and Security Rule are separate.

Michael Smith: I understand.

(Brad Peska): Okay.

(Stanley Nachimson): And this is (Stanley Nachimson).

Let me just add to your comment that some of your systems might not have audit capabilities.

The standard for audit control allows not only all hardware or software solution, but it also allows for a procedural mechanism so if the system itself does not have the capabilities, you can have some sort of a manual logging or such that would enable you to keep appropriate audit controls on some of your systems that might not have the built-in capabilities.

Michael Smith: My concern over the audits is that that information may be deemed as discoverable and be called into some legal malpractice suits.

(Brad Peska): I - this is (Brad Peska) again.

I would agree that that could be a consideration, but again it's nothing that is directly covered by the Security Rule itself, and I don't think that we'd be comfortable trying to give you, you know, additional legal advice about the discoverability of these documents outside of the requirements of the rule itself.

Michael Smith: Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Greg Bee.

Greg Bee: Yeah, hi there.

This is a follow-up on the audit controls question. (Stanley) just started to touch on it, but I wanted to dig a little further about the procedural mechanisms specifically.

And I was trying to figure out what a procedural mechanism for running an audit would be other than self-reporting. And (Stanley), you just said something about manual logging. I wondered if you could elaborate on what that might entail.

(Stanley Nachimson): And I think your - you hit on it yourself. Some self-reporting.

Greg Bee: Okay.

(Stanley Nachimson): Or in the extreme, someone else noting that somebody happened to have accessed a system or printed out information from the system or put information into the system.

Greg Bee: Okay.

So for a - particularly small providers that didn't want to, or couldn't rather, afford more sophisticated keystroke logging software or what not, a system of manual logging or self-reporting could be sufficient.

(Stanley Nachimson): Possibly, yes. Again depending on the risk analysis and the other factors, you're absolutely correct.

Greg Bee: Okay. Thanks.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Darlene Jenkins.

Darlene Jenkins: Hello. This is Darlene Jenkins from Pulmonary Associates in Fredericksburg.

I'm not sure if my question is security or privacy, but I know at one point I heard or read that our medical records -- charts, et cetera -- needed to be locked.

And I'm wondering if this is the case and, you know, how - I mean, the office is locked at night, but how much further do we need to go with that?

(Brad Peska): This is (Brad Peska) again.

I think that the question that you have is probably more of a Privacy Rule question. The Security Rule again is only - only covers electronic health protected information within a covered entity.

So if your question relates to paper medical records, it would be a Privacy Rule-related question, and I would refer you to the Office of Civil Rights, who is responsible for Privacy Rule questions.

And they also have an extensive amount of FAQs and other guidance material on their web site that you can access.

But it sounds like you're speaking of paper records and that would be a Privacy Rule.

Darlene Jenkins: Okay. Thank you.

(Elizabeth) Holland: Thank you. Next question.

Operator: Your next question will come from the line Candace Gray.

Candace Gray: Thank you. I'm calling from Bay Care Health System in Florida.

Can you tell me if a business associate agreement that meets the Privacy Rule automatically meets the requirements in the Security Rule?

(Brad Peska): That's also a very good question. This is (Brad Peska) again.

We are actually also in the process of looking at some of the issues surrounding business associate agreement language, and at this time I wouldn't be comfortable saying it whether does or doesn't.

In some cases covered entities, you know, may have varying language that they use in business associate agreements that may be over and above the direct requirements.

But again I'll refer you to the organizational requirements section of the Security Rule. Again that's 164.314(a)(1) for business associate contracts and other arrangements, which does identify the content if you will that is required by the Security Rule.

Candace Gray: When I look at the language that was published by the government as far as the business associate agreement and I look at the requirements in both rules, to me I would say it would meet both.

But I was wondering if you (unintelligible).

(Brad Peska): (Right). And that's a good question.

I - we do - we haven't received that question before and that's why as I mentioned we want to make sure that we provide the best possible information to the industry on this issue.

And at this point we do need to look into this question a little further.

Candace Gray: Okay. I appreciate that.

(Brad Peska): Yeah.

(Elizabeth) Holland: Thank you. Next question.

Operator: Your next question will come from the line of Kevin Buhler.

Kevin Buhler: Hi. This is Kevin Buhler calling from CalOptima. My question is related to the addressable standards.

I know that we have the flexibility to determine whether or not an addressable standard should be implemented within our organization, and we must document that fact, or document the decision-making process that goes into that.

My question is regarding the documenting the decision process. Do you have any best practices or recommendations as to how something like that should be documented? And who - what kind of legal or outside consulting should be involved to review that decision-making processes.

(Brad Peska): You - this is (Brad Peska) again.

You have a couple of points in the question there. I want to start off though again just by making sure that we clarify the terminology that we're using in the Security Rule context. And I think you may have just have not used the right term.

But addressable implementation specifications is really what we're referring to, not standards. All standards are required. So again, I just want to make sure that for the rest of the individuals on the call that we make that distinction.

But we also - we have the requirement for policies, procedures, and documentation in the rule which do, as we mentioned before, require you to document certain activities -- assessments, et cetera -- within your environment in relation to compliance with the Security Rule.

Now, there are no specific requirements of how you actually document or what the best method is or what the content should be, other than what is required in the standards themselves.

So that is again the business decision that organizations should determine based on, you know, probably taking a good look at what they currently do with policies and procedures would be a good start.

In addition, you mentioned potentially needing other individuals external to your organization that would assist in activities. And again, that's a - that would be a decision that a covered entity may make if they feel that they would need that kind of assistance.

But there is no requirement to use any external organizations to assist you with compliance. Compliance is a covered entity responsibility. Not that you

couldn't choose to use external resources for those type of activities, but the rule does not require it.

Kevin Buhler: Great.

Do you know of any resources of sample justifications out there? Just example wording?

(Brad Peska): And again, we're not able to provide any specifics on where you would find specific information or language if you will that would apply to the Security Rule. We're just - we're not able to do that.

Kevin Buhler: Okay. Thanks.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question is from Mark Eggleston.

Mark Eggleston: Hi. This is Mark Eggleston from Health Partners. My question is regarding encryption.

I understand that the implementation specification for encryption, and I truly appreciate that it is addressable.

However, the standard for transmission security is not addressable. It must be met. In reading through that standard, I see that we must implement a technical security measure to guard against unauthorized access to EPHI being transmitted over electronic communications networks.

My question is if we do not, or we chose to rule out encryption, could you give me a very high-level example of something else we could implement to meet that standard?

(Brad Peska): Hi, Mark. It's (Brad Peska).

I appreciate the question, and again it's a very good question. I know you've done some good analysis on that.

But at this time, we're not able to provide any additional information again that's over and above what is in the rule itself. But being that encryption is an addressable standard, as you mentioned, there could be other ways, other equivalent alternative measures out there.

And this is another issue that we're looking at to determine if there is additional information that we can provide to the industry.

But as with some of our other responses, it is very contextual, based on again the covered entities that we have out there and we do have to make sure that any specific answers that we provide or alternatives that we identify are applicable to all covered entities.

Mark Eggleston: Thank you, (Brad). I'll look forward to additional guidance.

(Brad Peska): Thanks, Mark.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question will come from John Cody.

John Cody: Hi. John Cody from New York State Office for Technology. This is actually sort of a follow-up on Mark's question.

As an attorney, I'm appreciative of the way this Security Rule was drafted. I think it's very flexible. And from an attorney's standpoint, it's relatively easy to live with.

But there have been several questions that have been tending along several lines that have been pending for some time. I think in particular of the security incident question.

I had information from somebody at CMS a year ago of November 24 that an FAQ on security incident handling would be issued shortly, and also several mini-papers on the CMS web site of about four pages each, and then also 20 other FAQs. We did see about 13 FAQs in August.

But otherwise the other guidance has been fairly slow in coming. So I'm wondering whether there's anything still in the pipeline on security incidents first of all.

And then second of all in terms of enforcement, whether the slow pace of the guidance that's being asked for and issued from CMS will weigh in on in terms of the enforcement, which does take place after the compliance date, which is just five months from now.

(Brad Peska): John, this is (Brad Peska). Thank you very much for that question. And your question is also very, very involved and I appreciate the analysis there.

I think it's important to recognize that not to make light of the situation, but there - a year in some cases isn't necessarily a short or long timeframe when

you look at some of the issues that we have to take into consideration for all covered entities involved.

So I understand that, you know, that some of these topics may be slow in their release, but from an enforcement perspective I will continue to point individuals back to the fact that the rule has been published for over (a year-and-a-half) now, and the requirements of the rule are what our office will be looking at when it comes time for enforcement activities.

So I understand that additional clarification and guidance is looked at favorably and sometimes requested by the industry as a whole, but the standards are what they are, and we're all, again as I mentioned earlier, working off the same page.

So - and I'll reassure you that security incidents is a very high priority for our office. It's just - as I know you have identified in the past, it's not an easy question to answer as with other activities that we're dealing with.

So I just want to assure you that we are taking it very seriously. We're trying to get the information out as quickly as we possibly can. But there are a lot of factors that go into the decisions that we make, which again affect a wide range of entities out there.

John Cody: Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Nick Hernandez.

Nick Hernandez: Hi, yes. Rick Hernandez here with the Center for Radiation Oncology down in Florida. I've just got a quick one there for you regarding the training, the security awareness and training, kind of tagging off of the earlier things.

A simple question. I know here that looking at the paperwork that it - there was a - it was addressed whether or not someone here is kind of like a short-timer, as (unintelligible) talked about, a one-day thing.

Really my question is, is there any - I don't see a requirement that says like a timeframe when we get onboard a new employee, you know, he or she must be trained within a 90-day period or something like that.

Is that true?

(Brad Peska): Nick, that's a good question.

And, you know, I'll point you to the - there is some level of discussion in the preamble to the Security Rule. And I unfortunately don't have the direct reference for you.

But if you have the Federal Register version, I would take a look at the discussion of security awareness and training in the preamble.

And to paraphrase what the content is included in there is some covered entities expressed the need for orientation - for security awareness training during the type - orientation-type of activities and other organizations chose to do those types of training and awareness programs throughout on periodic basis, whether it's annually, biannually.

We don't have direct requirements that state exactly how or when this awareness and training must be performed other than before - at least once before the compliance date.

But those decisions on if it will be performed within 90 days or those type of considerations again are a business decision and should be based on potentially the way that you perform other training activities within your environment.

The rule, you know, doesn't - also doesn't say that you couldn't incorporate the concepts of security awareness and training into other training that you are performing.

Nick Hernandez: Yeah, okay. That's where I thought and that's some of the things I was reading. Thanks. I appreciate it.

(Brad Peska): Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Beth Rubin.

Beth Rubin: Yes, this is Beth Rubin from Dechert.

I just wanted to follow up on something that John Cody mentioned. I think this is what he was getting and - when he talked about the definition of security incident.

And that is that I'm having trouble and the whole negotiation of business associate agreements is being slowed down because of the definition of

security incident, and particularly the fact that the word “attempted” unauthorized access is included in it.

The word attempted is the problem. I’m being told repeatedly by area expert security people that you can’t possibly monitor all unattempted - I mean all attempted pings on a system.

And covered entity security experts tell me that they don’t want to know about attempted unauthorized access. They only want to know about successful unauthorized access.

So I’m just wondering when we’ll get that guidance.

(Brad Peska): About - this is (Brad Peska) again.

I do again understand the need to get some of this material, but I will again stress the importance of making sure that we make a decision and provide guidance that’s going to allow the industry again to best meet compliance for what’s reasonable and appropriate in their specific environment.

So I will again reassure you that this is at the top of our list of guidance - or FAQs I should say is a better way to put it -- FAQs out to the industry.

Beth Rubin: Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question comes from Ruth Homuth.

Ruth Homuth: (Unintelligible) we do our computing with Siemens Corporation on an RCO basis, which means our files with all our electronic health stuff is really stored on the mainframes at Siemens.

From what I can read in the law, they are really not a covered entity because they are a provider of basically computing capability. What would we need to have from them, since that's where most of our EPI is stored, in order to meet the compliance with the law?

(Brad Peska): That's a very good question.

I think in this circumstance what you're referring to would be a business associate relationship, so I would point you in the direction of looking at what is a business associate. There is a definition of what is a business associate in Section 160.103.

Ruth Homuth: Well, we know that we would need an agreement like that.

But we were wondering since that - now they are storing all our EPHI, do we need something from them like what their disaster recovery would be, what their backups are, what they're actually doing to protect the information up there and their access to it and all that good stuff.

(Brad Peska): You know, I would say from - again, from a Security Rule standpoint, there are some requirements, and you probably have picked up the reference and stuff that we've been pointing to for what the content should be.

So you know exactly where the requirements themselves are, Section 164.314, the organizational requirements, business associate standard.

But I would say that in general when you're looking at your overall compliance program, there may be issues that you look at which are outside of the Security Rule requirements themselves that as a business decision you would chose to find out what those particular plans would be for that business associate so that, you know, it could be a part of your contract itself.

But it - those specifics that you've mentioned are not identified in the business associate agreement directly.

Ruth Homuth: Thank you.

(Elizabeth) Holland: Thank you. Next question please.

Operator: Your next question will come from Randall Patton.

Randall Patton: Yes, this is Randall Patton from Pleasant View Retirement Community in Pennsylvania. Two full question.

The first -- have specific, defined penalties been brought out for noncompliance, number one. And also, who specifically within the federal government will be the overseer for enforcement?

(Stanley Nachimson): This is (Stanley Nachimson).

The - your first question about penalties, the overall penalties for noncompliance for violations of the HIPAA Administrative Simplification standards were specified in the law.

Again, at least for non-privacy provisions, they were - its $100 per violation of the standard per incident, up to $25,000 per year per standard.

That being said, the details about how those would be computed have not yet been - have not been issued. We've got some plans to issue proposed rule that talks about the details of enforcement probably some time next year.

So can't answer the exact question about how penalties will be computed.

The responsibilities for enforcement lie with the Department of Health and Human Services for privacy complaints. That's the responsibility of the Office of Civil Rights.

And the other Administrative Simplification provisions for transactions and code sets, which we're already enforcing, for the upcoming security provisions and the upcoming identifier provisions, those would be the responsibility of the Centers for Medicare and Medicaid Services.

Randall Patton: Okay. Thank you very much.

(Stanley Nachimson): You're welcome.

(Elizabeth) Holland: Thank you. I think we have time for one more question.

Operator: Your final question will come from the line of Kelly Beard.

Kelly Beard: Hello. This is Kelly Beard with Willamette Valley Hospice. I have a question about alpha pagers and two-way pagers and if those are included in the Security Rule.

(Brad Peska): Kelly, that's a good question.

I would refer you to the definition of electronic media, which identifies certain devices as being covered in the definition of not only electronic media, but also therefore being electronic protected health information.

So I would point you to - let me give you the exact citation here for that definition. That would also be in 160.103, the general administrative requirements of - it's listed in the beginning portions of the Final Security Rule.

And there - that's where you'll find the definition of electronic media that would allow you to make that determination.

Kelly Beard: Okay, thank you.

(Brad Peska): Thank you.

(Elizabeth) Holland: Okay.

Before we end, I have several announcements.

First I'd like to announce that we have another roundtable scheduled for Wednesday, December 15 at 2 o'clock pm Eastern Time. That roundtable will focus on the National Provider Identifier, or the NPI. The call-in number for that call is 1-877-203-0044, and the conference identification number is 1598382.

More information on HIPAA can be found on our web site, which is located at www.cms.hhs.gov/hipaa/hipaa2. We do plan on posting a transcript of this call and posting information on future calls on or web site.

If you do have additional questions, please email them to our electronic mailbox, which is located at askhipaa@cms.hhs.gov.

And we'll now conclude with some final words from Nathan Colodney.

Nathan Colodney: I'd like to thank all of thank all of you for joining us today, as well as (Elizabeth), (Brad), and (Stanley), who are members of a team working very hard at CMS to address your concerns.

I believe that your participation today is indicative of the interest in the industry in understanding the rule and complying with it. To that end, I would highly encourage you to use the available resources (Elizabeth) cited.

As the April 20 deadline approaches, I hope you view the rule as not really a regulatory requirement, but an opportunity.

With this, I'll close this roundtable today and encourage you to participate in future roundtables. Thank you.

(Elizabeth) Holland: (Tina), could we get a final count of participants?

Operator: Two-thousand-thirty.

(Elizabeth) Holland: Thank you.

Operator: Thank you.

Ladies and gentlemen, this does conclude today's teleconference. You may all disconnect.

(Elizabeth) Holland: Thank you.

Operator: Thank you. Have a good day.

(Elizabeth) Holland: You too.

END