CENTERS FOR MEDICARE AND MEDICAID SERVICES

Moderator: Karen Trudel
April 13, 2005
1:00 pm CT

Operator: Good afternoon. My name is (Michael). And I will be your conference facilitator today.

At this time I would like to welcome everyone to the Centers for Medicare and Medicaid Services 19th National HIPAA Implementation Roundtable conference call.

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. Dr. Harper you may begin your conference.

Harper: Thank you Mr. (Paris). Hello everyone. It's my pleasure to serve as your Moderator.

And I also want to welcome you to the 19th National HIPAA Roundtable call.

This call is being conducted by the Centers for Medicare and Medicaid Services or better known as CMS which is part of the U.S. Department of Health and Human Services.

We began conducting these calls in March of 2002 to facilitate the implementation of the Health Insurance Affordability and Accountability Act of 1996 or HIPAA, and more specifically the administrative simplification provision.

Today's call will focus on HIPAA security. After we hear from our speakers we will have time to give you an opportunity to answer many of the questions that you have on your mind.

I'm also happy to announce that we do have a new Director of the Office of HIPAA Standards and CMS. It is Mr. (Tony Trenkle) spelled T-r-e-n-k-l-e. He had hoped to be with us today but he is not able to be in conference right now.

But I want you to know who he is and that he has had an extensive and successful career in electronic commerce and a great understanding of electronic initiatives.

I'm sure at some point you're going to have the opportunity to meet with him or to speak with him on a conference call.

Now it is my pleasure to introduce our first speaker who is Mr. Stanley Nachimson, Senior Technical Advisor of the Office of HIPAA Standards.

Mr. Nachimson.

Stanley Nachimson: Thank you very much Dr. Harper. Good afternoon to everyone. I'm very happy to have you all with us today.

This is a very opportune time for this roundtable since the compliance date for the HIPAA Standards is April 20, 2005, a week from today for all covered entities except small health claims. This teleconference will provide an opportunity for you to ask and for us to answer any of your last minute questions regarding the HIPAA Security Standards.

As you all know by now the security rule is intended to insure three main points in relation to Electronic Protected Health Information. First, protecting the confidentiality of that information meaning who gets to see the information.

Secondly, protecting the integrity of that information, ensuring the information has not been altered or destroyed.

And thirdly, ensuring the availability of Electronic Protected Health Information so that it can be accessed when and where and by who needs the information.

In writing the rule we divided the security safeguard into three main categories. Administrative safeguards, physical safeguards and technical safeguards.

We provided guidelines in the rule for business associate agreements and organizational requirements.

Well I'm sure you all have a lot of questions today so let's get started with our presentation and then you'll have your opportunity to ask questions of our folks here.

Thank you again for joining us today.

Harper: Thank you. Our second speaker it will be Brad Peska, Security Specialist of the Office of HIPAA Standards.

Mr. Peska.

Brad Peska: Thank you very much Dr. Harper.

I want to take a quick minute to expand on a couple of points as Stanley mentioned.

And then give you a quick overview of our current Federal Register Notice which addresses our enforcement procedures for all of the non-privacy regulations under the HIPAA Administrative Simplification.

So I want to do that and of course make sure we have enough time to address some of the questions that the group has here today.

As Stanley mentioned the security rule really is focused specifically on the Electronic Protected Health Information within a covered entity.

And just for a quick review covered entities are health plan, healthcare clearinghouses, and certain healthcare providers that perform electronic transactions that have been adopted the Secretary under HIPAA.

So when we look at this specific information and the protections that we have to place on EPHI specifically protecting against any reasonably anticipated threats or hazards to the security or integrity of information protecting against reasonably anticipated uses of the disclosures not permitted by the privacy rule the protections for confidentiality, integrity, and availability that Stanley mentioned as well as ensuring workforce compliance.

All of these things are coming to the conclusion here when we look at the compliance date for the rule.

But I do like to make sure folks also understand that when we look at the April 20th compliance date that it's really the beginning your ongoing compliance initiatives for the security rule.

And what I want to do is make sure that we give you somewhat of a view into our procedures for how we will continue to make sure through the enforcement process that covered entities are in fact maintaining their compliance with the security rule standards and it's implementation specifications as they've been laid in the final security rule which was published February 20th of 2003.

For those of you who have had access to the Federal Register Notice which is titled the Procedures for -- I'll get you the -- the Procedures for Non-Privacy Administrative Simplification Complaints under the Health Insurance Affordability and Accountability Act of 1996. I would encourage you to download that information from the CMS HIPAA Administrative Simplification website which I'm sure we'll give you many times today.

But that's www.cms.hhs.gov/hipaa/hipaa2. We have a link to this Notice that you can download. It was published on March 25, 2005 a couple of weeks ago.

And I want to make sure that I give you a high level of the points that are outlined in this Federal Register Notice.

But specifically as we look at the security compliance date and how we will move forward with the enforcement process all of the comments that we're making here apply to or I should say, all of the comments I'm making today come from this Notice which really sets forth the procedures for how individuals may file with the Secretary of Health and Human Services and therefore CMS has also a set of standards a complaint of noncompliance by a covered entity with certain administrative simplification provisions that we address as of the non-privacy regulations in this rule.

Those specifically are the Transaction and Code Set rule, the National Employer Identifier rule, the Security rule, the National Provider Identifier, and the National Plan Identifier. Each of these rules are at various stages of either final publication or proposed publication or under development.

The procedures outline the any person that believes that a covered entity is not complying with these provisions may file a complaint with CMS. Now truly any person that wants to file a complaint can do so via one of our two methods.

The primary method is the ASET system which is the Administrative Simplification Enforcement Tool which we call ASET. That application allows you to file electronic complaints to CMS Office of HIPAA Standard. The web address is http//htct.hhs.gov.

This application is the primary means not only of submitting complaints on the HIPAA Non-Privacy Regulations but also for allowing complainants to receive some level of status and to allow our office to manage complaints as well.

In addition you may file complaints via paper. We have a complaint form that is also on our CMS HIPAA/HIPAA 2 website that will allow you to submit complaints that are referred to as the non-privacy complaint.

And you can mail them into the address that's identified in the Notice which is Centers for Medicare and Medicaid Services, HIPAA TCS Enforcement Activities, P.O. Box 8030, Baltimore, Maryland 21244.

And I will reassure everyone that any complaint for an active regulation that OHS is enforcing can be submitted to this address even though it has a specific TCS identifier in the mailing address. You can submit any complaint including identifier and security to this mailing address.

When can you file?

In general CMS for each of the published regulations will not accept complaints until on or after the compliance date for the specific Administrative Simplification Provision in question. OHS of course has been enforcing transaction and code sets since October 16th of 2003, and the Employer Identifier since July 30th of 2004.

And we can add to that list the security rule which we also clarify in this Notice. We will be beginning accepting complaints via the two methods that I just mentioned on April 21, 2005 which is next week.

At that - on that date we will begin both with our updated paper complaint form and updated electronic submission being through the ASET system which will allow individuals, any individual to file complaints with our office.

Complaints that are submitted must meet certain criteria.

They must be filed in writing either paper way - either on paper or electronically.

They must describe the acts or omissions believed to be in violation of the applicable provisions, the Administrative Simplification Provision.

They must provide contact information for both the individual filing the complaint, the complainant, and the covered entity that was the subject of the complaint.

And it must be filed within 180 days of when the complainant is knew or should have known that the act or the omission that is the subject of the complaint occurred unless CMS waives this 180 day timeframe for good cause shown.

In general, our procedure is after we receive the complaint, we conduct a preliminary review of the complaint to determine whether it is complete and appears to allege a compliance failure with an Administrative Simplification Provision.

And typically it will proceed as follows.

CMS will acknowledge the receipt with an acknowledgement letter that is usually sent within 14 calendar days which can either be electronic or a paper letter.

If the complaint is complete and appears to allege a failure to comply we will notify the complainant the complaint is accepted for processing and further review.

But of course acceptance of the complaint does not mean that there is a determination a compliance failure has actually occurred.

In all cases, CMS reserves the right to reject certain types of complaints. And if there is any additional information that is required for us to make a preliminary determination on a complaint we will contact the complainant to obtain that additional information.

CMS also reserves the right and may close a complaint if it does not actually state a claim upon which our office can act.

Complainants may withdraw complaints at any time upon notice that CMS requires.

And even if a complainant withdraws their specific complaint against a covered entity CMS may still determine that it must continue with its investigation of the alleged noncompliance activity in the complaint.

In general, a complaint can be withdrawn before the investigation has occurred and may also be re-filed.

But we do identify the complainant and we will notify complainant that if they withdraw a complaint that they do need to be aware of the 180 day resubmission timeframe of when the act or omission actually occurred.

And the same procedures would apply here that we could waive that subsequent 180 day period.

Once we receive the information and we have determined that there is a need to continue with an investigation of the alleged violations in the complaint CMS will contact the covered entity that is involved. And will advise them that a complaint has been filed.

And will inform the covered entity of the alleged compliance failure. At this point we will work with the covered entity to obtain voluntary compliance.

CMS will ask the covered entity to respond to the alleged compliance failure by submitting in writing one of three items, either a statement demonstrating compliance, a statement setting forth the basis for disagreement with the allegations, or a corrective action plan.

We will allow the covered entity to respond to this request within a reasonable timeframe which is generally 30 days to respond to our request if they submit one of those items. We may for good cause shown extend that 30 day timeframe for a response.

But it is on a case by case basis and at CMS's sole discretion.

A covered entity that disagrees with the allegations should set forth and document to CMS the actual compliance status and then what respect it believes that the allegations may be factually incorrect or incomplete, the

allegations of course within the complaint. And identify why it disagrees with the alleged actions or failures to act may constitute a failure on their part to comply.

Upon receiving this information CMS will - may communicate further that it needs additional information either from the covered entity or from the complainant.

And we also may request the opportunity to interview any knowledgeable persons or review additional documentation or material that's needed to continue the investigation process.

We will allow a covered entity at any point to amend or supplement its response and to propose voluntary compliance and corrective action plan. We may require modifications in some cases to the terms of the proposed corrective action plan from the covered entity as a prerequisite to actually accepting the corrective action plan.

If the corrective action plan is accepted by CMS, CMS will actively monitor the plan and will require the covered entity to periodically report progress towards compliance.

As we move through the investigation process we move to actually resolving and closing complaints. If the covered entity is able to comment to voluntary compliance, CMS will notify the complainant of this action by mail or electronically. But the covered entity has to come into voluntary compliance.

CMS will make reasonable efforts of course to secure a response from the covered entity to the allegations especially in relating to keeping it with the theme of voluntary compliance.

However if a covered entity either refuses or fails to provide us the information that's sought, we do have the ability to issue investigational subpoenas and other activity.

But we do like to continue to promote the voluntary compliance approach. And if by some chance there was a violation of finding that is finding of a violation that existed the Secretary has the ability to pursue other options such as but not limited to several money penalties.

In all cases we will notify all parties to the complaint as appropriate that the complaint has been closed and the resolution has been reached.

As this applies to the security enforcement approach I mentioned the security rule is one of the non-privacy regulations that is identified in this Federal Register Notice, so all of the activities and statements that I've made do apply to our enforcement approach for the HIPAA Security Rule as well as the transactions and code sets and identifiers.

I do want to make it clear to folks listening in today that the compliance date for the security rule is still no later than April 20th of 2005.

And we do have procedures in place that will allow us to begin enforcing the security rule on April 21, 2005.

We expect this to be a primarily complaint driven process. And as I mentioned CMS will focus on obtaining voluntary compliance from covered entities through this process.

We have also realized through this process and through the correlations that exist between the HIPAA Privacy and HIPAA Security Rule that there is much enforcement coordination also needed between CMS and the Office for Civil Rights.

Currently we have teams from both agencies working through HIPAA Security and Privacy Enforcement issues. We've been able to share experiences and insight from our respective enforcement processes the history that our office has had with transaction and code sets along with OCR's experience with the privacy rule.

We've been able to establish a good working relationship that primarily focuses on how we will move forward with and handle any complainant that has alleged a violation of both the security and/or the privacy rule.

We expect that many complaints may focus on specific overlaps between the rules.

But we are also exploring the potential that some issues may involve - may allege allegations - may allege violations of the rules that do not specifically overlap but do have to be handled by the respective organizations.

In time we will continue to evaluate the effectiveness of these processes and refine them as necessary.

But we also have mechanisms in place not only to enforce the security rule but also to look at the overlaps and other issues that result from the HIPAA Privacy and Security Rules.

I do want to also make sure that everyone continues to be aware of the other outreach activities not only these roundtables, but the CMS website where we post additional FAQs. They clarify specific issues related to HIPAA security and the other provisions that our office enforces.

And we will continue to provide additional FAQs and information. And we anticipate of course continuing to publish this type of information even after the compliance date the same way we've done the transaction and code sets, and that OCR has done with the HIPAA Privacy Rule.

This type of clarification, the FAQ clarification, continues to provide the information the covered entities need to maintain their ongoing compliance program with the security rule.

And as we see advances both in technology and in operational issues there will be additional correlations that we need to make between other future technologies or activities and the security rule.

So we will continue to post additional FAQs even past the compliance date to maintain and to allow covered entities to maintain their compliance status.

I also want to alert everyone that we will have a HIPAA Security Series of Educational Papers that is being posted to the website as well.

We are at various stages of posting the material which is a set of seven papers that address areas from the Security 101 which is currently published through all of these safeguard provisions, the administrative, physical, and technical safeguards as well as a paper on organizational policy procedures and documentation requirements.

And a few papers that are specific to certain activities, the risk analysis and risk management approach or the basics I should say, of risk analysis and risk management, and implementation for the small provider.

These papers will be published to the external website. And we will make the appropriate announcement both on the website and to our Outreach Distribution List which I will also encourage you to sign up for if you have not already where you will receive not only the latest information in the form of FAQs or educational papers but also notifications of outreach activities such as this conference.

I will also encourage you to submit questions to our Ask HIPAA Mailbox where we are able to provide in some cases very direct answers in other cases answers that require more in depth analysis that in many cases turn into FAQs.

And that address is askhippa@cms.hhs.gov.

I want to make sure that everyone also understands there are more - we see the security rule in many aspects here. And I want to continue to encourage you to look at the larger impacts of the security rule in your organization.

And leave you with a couple of closing comments. Compliance with the security rule should mean more than just meeting a regulatory requirement. Compliance with the security rule makes good business sense.

Compliance with the security rule should encourage organizations to make security part of normal everyday operations within their environment.

As we move forward security and privacy issues will be key issues for the healthcare industry especially as we begin to look at new initiatives such as the electronic health record and the exchange of information across the nation.

I encourage you to continue to maintain your compliance with the security rule and leverage it to be much more than just the regulatory requirement.

I thank you very much for your time. And at this point would like to turn it back over to Dr. Harper.

Harper: Thank you Mr. Peska for that very comprehensive presentation. And I think that you have set the stage for people on line to be able to ask the questions.

And Stanley I want to thank you for the information that you gave at the beginning.

So I think we have a frame of reference now for our questions.

And Mr. (Paris) now will you give us the information relative to the callers to be sure that they give us their names first and their organization, and then to ask the question.

Operator: At this time I would like to remind everyone if you would like to ask a question please press star then the number 1 on your telephone keypad.

We will pause for just a moment to compile the Q&A roster.

Your first question comes from (Donna Benjamin).

Harper: Miss (Benjamin) your question please.

(Gregory Grannon): Actually this is (Gregory Grannon) sitting with (Donna Benjamin) at Delta Dental Plan of New Mexico.

And my question is two part, one, is there any accommodation for whistleblower anonymity in filing these complaints?

And two, if so, how are you going to sort out nuisance complaints maybe from one competitor trying to involve another competitor?

Thank you.

Brad Peska: Very, very good question.

Harper: State your name, please.

Brad Peska: Sorry, this is Brad Peska answering the question.

A very good question, the first part of it, yes. We do allow anonymity for whistleblowers.

But we allow for the anonymity when we are looking at post filing issues and correspondence between our office and the covered entities involved. We do apply a question which we allow complainants to answer yes or no to whether they want their information shared to the other parties involved in the complaint.

An answer to no, would allow us to treat that information differently from a normal complaint.

In response to your question about filings from competitors, I mean we need to look at every complaint that comes in on a case by case basis and make sure that the information that is submitted is looked at by a point of view of both the complainant and the covered entity that is involved. That all parties involved are both included in the discussions and that we are sensitive to the needs of both parties as well.

So if we have situations where there were multiple complaints by competitors, etcetera, we would take that into consideration.

But at the same time we need to make sure that every complaint is handled as it is submitted to us and that we are able to follow through with the allegations into the investigation stage for any complaint that we receive.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Deborah Keyslick).

Miss (Keyslick) you're line is open.

(Deborah Keyslick): Hello, thank you. I wondered what - kind of a follow-up on the last question with respect to those individuals who file a complaint and who are not concerned about anonymity.

Will CMS consider providing the covered entity with a copy of the complaint or will you just forward the information about the complaint as you see fit?

Brad Peska: Our process is to notify the covered entity of the allegations within the complaint.

If it, you know, if there was a situation that arose where we would have to provide specific details of a complaint we would have to look at that issue separately.

But our process is to, if you will, summarize the allegations within the complaint to notify the covered entity of the allegations. But not necessarily share the entire complaint file, if you will, with that covered entity.

(Deborah Keyslick): Thank you.

Harper: You're welcome. Next question, please.

Operator: Your next question comes from (Sundette Acrayha).

(Sundette Acrayha): Hello?

Harper: Hello.

Man: Yes, yes.

(Sundette Acrayha): I was talking about - you all - this is actually is a request more related to the - you all got information on individuals who participate in the converse, I guess the attendees.

And I was just wondering what that information is being used for. Is it to - maybe you can answer that for me, you know, got like the names and organizations that assist callers.

Or how does that information get used and why's it being used? I was just wondering that.

Harper: The information is used to let us know whose speaking and the people who are on line who are speaking.

(Sundette Acrayha): Oh, okay.

Harper: And to tell us which organization. Otherwise we don't use the information.

(Sundette Acrayha): For any other purpose.

Harper: No.

(Sundette Acrayha): Oh, okay. I also had another question. There was a video put out I think awhile back, a HIPAA 101 video.

And I wanted to know are you all planning on putting any other videos out for - related to HIPAA as far as like for - that could be used for training or for other resource? I thought that was very - a very good thing that you all did that resourceful thing, putting out a video relating to new standards. It would be like for the (NPI) or new standards that are going to come out in the future.

Harper: (Unintelligible) question.

(Sundette Acrayha): Or the security one or anything related to.

Harper: Mr. Nachimson, are you going to answer it?

Stanley Nachimson: Yeah, I think we had someone from the (NPI) outreach group.

(Helen) Dietrick: Yeah, this is (Helen) Dietrick. I'm with the (MBNPR) right not and we are in the process of developing a CD Rom.

And I think there might also be another product without audio, just a video product on how to fill out the application that will be coming shortly.

(Sundette Acrayha): Okay, I think that would be wonderful for - how would that be available to covered entities to access?

(Helen) Dietrick: Well we have a number of ways of distributing it.

Are you a provider?

(Sundette Acrayha): Well, I work for a healthcare organization.

(Helen) Dietrick: Okay, we intend to distribute it to healthcare organizations, providers, to the provider associations.

I guess if you send me your name I can make sure you get a copy.

(Sundette Acrayha): Okay, that would be wonderful. I could do that.

(Helen) Dietrick: I'm at hdietrick@cms.hhs.gov.

(Sundette Acrayha): Could you repeat that again? H…

(Helen) Dietrick: H Dietrick, D-i-e-t-r-i-c-k.

(Sundette Acrayha): D-i-t-r-i-c-k?

(Helen) Dietrick: D-i-e-t-r-i-c-k.

Harper: Dietrick.

(Sundette Acrayha): Dietrick, okay, at?

(Helen) Dietrick: CMS.

(Sundette Acrayha): CMS.

(Helen) Dietrick: Dot HHS.

(Sundette Acrayha): Dot gov?

(Helen) Dietrick: Dot gov.

Harper: Thank you very much.

(Sundette Acrayha): Okay.

Harper: Next question, please.

Operator: Your next question comes from (Alex Brainskono).

(Alex Brainskono): Hi. I work for (Scripps).

And I have a two-prong question.

Number one, how will the HIPAA Security Rule complaint process differ from the HIPAA privacy complaint process?

And part two, would you kindly point us to the CMS site where you have the information that you covered prior to the question and answer session on the complaint process?

Thank you.

Brad Peska: Sure, this is Brad Peska.

To answer your second question first, the CMS website is www.cms.hhs.gov/hipaa/hippa2. On that main website you will have a link to the Notice which you can go to that will specifically pull up our Federal Register.

And for those of you who may be a little more savvy in searching the Federal Register publications, it can be found at 70 Federal Register, pages15329 through 15331.

But that's the specific Notice that I was referencing which is titled Procedures for Non-Privacy Administrative Simplification Complaints under HIPAA.

To your first question, we expect the processes for enforcing the security rule and the privacy rule independently will be maintain moving forward.

And there - for the most part those processes are very similar. What we have done in relation to potential issues where you see both the privacy rule and the security rule issue we've been able to coordinate some of our activities to continue to promote what we call one HHS view towards the complaint management process whereby our office and the Office for Civil Rights will

coordinate very closely when it's appropriate to efficiently and effectively manage the HIPAA complaint process.

I will tell you that in general if there is specifically a security rule only complaint that we are addressing with a covered entity the process that we manage is, you know, independent and, you know, can purposely be independent of the OCR Privacy Rule process.

But I will tell you in the grand scheme of things our processes are very similar.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Alea Guys).

(Alea Guys): Hi, we're calling from New Mexico also.

One of our questions comes up in an interpretation of some of the policies. Specifically, you know, in a large metropolitan area we are split down the middle as far as the interpretation of encrypting and outgoing email that contains EPHI.

One large organization can make the statement that it's not appropriate. Another one is. So we're stuck in the middle.

Are there any particular guidelines? And how do we resolve an interpretation that is somewhat defined by community standards?

Stanley Nachimson: Hi, this is Stanley Nachimson.

And as we've done with a number of items in the security rule there are some implementation specifications that we made addressable. We left the decision as to whether or not to follow that particular implementation specification to the individual entity based on their particular needs, requirements, and their situations.

Within any community still the choice of whether or not to encrypt that information is left to the entity. So it is quite possible that one organization may choose to encrypt information that they deal with while and another organization for one reason or another chooses not to encrypt.

There are no specific guidelines that tell an organization exactly when they should or should not encrypt that information. That choice is left up to them, again depending on their risk analysis and the situation within that organization.

So if you are dealing with both those organizations you will have to deal with both those situations.

Harper: Thank you. Next question, please.

Operator: Your next question comes from (David Edmunson).

(David Edmunson): Hi, my question's a little bit more fundamental since we've found ourselves having applicability to the security rule. We're a health plan provider only because we're self-insured.

And so I'm having difficulty finding anywhere on any regulatory site even yours the definition of personal health information such that I would be able

to determine whether or not the premiums that are paid for the health plan are considered personal health information.

So if you could guide me to some place that gives either examples or specific wordage that tells me that that plan payment information is PHI or not that would be really helpful.

Stanley Nachimson: This is Stanley Nachimson. And let me at least provide you a guide as to where to go.

In our regulations, the Federal Register Regulations on HIPAA we have a general section on definitions.

And 160.103 where health information is defined, and it talks about - and the definition means any information oral or recorded in any form or medium that is created or received by a healthcare provider, health plan, which it sounds like it applies to you, health authority employer, etcetera, etcetera; and relates to past, present, or future physical or mental health, condition of an individual, provision, or healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual.

It sounds very much to me like the benefits that you're paying premiums that are being paid may be considered health information.

But it will depend on whether or not you are sending that information as a health plan, receiving it as a health plan, or sending that information as an employer.

Employers are not considered covered entities and therefore are not covered by the requirement of HIPAA.

Brad Peska: And this is Brad Peska. I'd like to add to what Stanley was just stating as well that you may want to look to the website for the Office for Civil Rights as well.

They do provide additional clarification and in many cases around the privacy rules listing of data elements which are considered protected health information or PHI under their rule.

So I would encourage you to go to the Office for Civil Rights that site as well and check with some of their both educational material as well FAQs.

(David Edmunson): Okay, because basically we've gone down the road of saying we're an employer and we lost that battle.

And so yeah, from my way of thinking in the IT organization, you know, it seems pretty obvious to me that any amounts of money paid would be considered PHI based on that definition you read from 103.

But it would be really helpful because, you know, that determines whether or not we have more in scope applications, processes, activities as opposed to just providing, you know, details on the personal health conditions and payments for services by doctors, etcetera.

Brad Peska: This is Brad Peska again. Can we, if you don't mind, get your information and follow-up with you on this issue?

(David Edmunson): Sure.

Harper: Give us your telephone number, please.

(David Edmunson): (858) 5.

Harper: (858).

(David Edmunson): 523.

Harper: 523.

(David Edmunson): 6680.

Harper: 6680.

Thank you Mr. (Edmunson).

(David Edmunson): Thank you.

Harper: Next question, please.

Operator: Your next question comes from (Angela Kinoff).

(Angela Kinoff): Hi. I'm calling from (Sparrow)'s and I have a question regarding the required implementation specification for audit control.

My understanding or interpretation of that is to be able to determine the - any time a patient record is accessed by individuals.

However in our varied applications that we have a lot of the vendor systems do not provide this ability even post "HIPAA upgrades." They still haven't

provided the full functionality as I would see that, you know, other than going to other systems which, you know, would be extremely difficult.

How would you view that from an enforcement standpoint our inability to completely track all accessed patient records within electronic information systems?

Brad Peska: Thank you for your question. This is Brad Peska.

The other control standard if, you know if you read very literally requires hardware - requires a covered entity to implement hardware, software procedural mechanisms to record and examine activity and information systems that either contain or use EPHI, Electronic Protected Health Information.

The rule does not provide the specific as to the level of detail or the capabilities within information systems. We do however want to provide additional information to covered entities to clarify this requirement in more detail.

I will tell you that we will look any complaints that may be received for any of the standards or implementations specification on a case by case basis and look at all of the facts presented which may include the technical capabilities of the information systems that a covered entity currently uses.

If you also look to the general requirements in the security rule where we describe the flexibility of approach the covered entities may take we do allow covered entities to look at a number of factors when determining what security measures to implement within their organization and that will apply to audit controls as well.

And one of those is the technical complexity and the current information system infrastructure that will be used within the covered entity. So we will look at all of those issues if a complaint was filed in relation to this type of an issue within information systems.

(Angela Kinoff): I understood the complexity and all that to be more for the addressable.

So also for the required if we have systems and, you know, we've done full risk assessments if we work with the vendors and they do not now and at this point do not have plans on addressing this and making it so we can audit it to the field level, at this point do you feel that might do diligence?

Stanley Nachimson: This is Stanley. Let me just add that I think the level of activity is really what you're looking at in the audit control.

And that's a determination that you would have to make for your organization based on your risk assessment and your capabilities.

The list that Brad gave does apply to even implementing standards. But I think your risk analysis would determine the level of audit control that you need to maintain.

And if your current systems do not have the level of audit controls that you think are necessary to maintain adequate protection for your information, then you will need to look at some additional systems for it.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Barbrianne Wade).

(Barbrianne Wade): My question actually was the - an exact piggyback to the former question.

We are actually a business associate, a vendor to hospitals. And we are having a lot of difficulty providing view level audit control across the board in the system that we provide.

However we are able to provide levels of audit control that monitor logins, access to the information, as well as attempts on the information just not exactly what was viewed.

And each facility, each covered entity that we deal with has different levels of expectations of how this rule should be addressed.

How should we handle that as a business associate?

Harper: Thank you for your question.

Stanley Nachimson: Yeah, this is Stanley.

And I would say as a business associate you need to look at the individual situation that each covered entity finds themselves in and what their particular requirements are. The level of auditing in one entity may need to be much more detailed than that in another entity depending on the risk analysis that's done.

We don't envision it be the security rule implementation is a one size fits all process.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Mimi Hart).

(Mimi Hart): Hello. My question would be well first of all our frustration. We're having a lot of difficulty implementing in the Biomed area. There's a lot of equipment that contains protected health information that my Biomed people tell me has no business having some of the technical security mechanisms that you guys have listed such as user IDs.

And I'm also having a lot of problems with foreign vendors who don't seem to, you know, are not familiar with HIPAA.

Do you have any recommendations in this area?

Harper: We're having a little consultation here in the room. We'll be with you shortly.

Stanley Nachimson: Again, in general in dealing with the medical equipment that you'd have to take a look again at the risk analysis and the situation, the technical capabilities of that equipment to see if things like individual user IDs are particularly relevant in those situations.

In terms of vendors that are not familiar with HIPAA, I don't want to - I don't think I want to comment on that.

Harper: Any other comments from Miss (Hart)?

(Mimi Hart): And I'm not bashing vendors. I'm just saying that there are a lot of my vendors that are foreign vendors in Europe and in Asia and they don't seem to have the knowledge of the HIPAA regulation so it's a real fight to get things implemented.

Brad Peska: This is Brad Peska speaking.

A lot of the issues in that respect are probably more appropriate for contractual discussions and not, you know, specifically to the rule.

Although we will continue to take these questions and look at them in more detail and determine if we can provide a more specific answer.

But also in reference to the biomedical equipment discussion, it is also a topic that we're looking to provide more clarification in the future on to give you some more specifics around the implementation of the security rule in relation to those kinds of devices.

(Mimi Hart): Great. And then…

Harper: Karen, did you have any advice for us, Karen Trudel?

Karen Trudel: No, I think Brad just made the point that we are looking at the issue of the Biomedical devices and do need to talk to the Food and Drug Administration about that as well.

But we are looking to provide some more guidance.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Connie Hine).

(Connie Hine): Hi, thank you. My question is actually relating to business associate agreements for the HIPAA Security Regulations as opposed to the privacy regulations.

Most of the requirements that are outlined in the security regulations are very similar to what is required by privacy.

However if you go through and look word by word there are some minor differences.

I was just wondering I had heard at some point that you all may be issuing some additional guidance perhaps another template like you did for privacy for business associate agreements.

Or do you all consider at this point that what people have in place for privacy is acceptable for security or how is that going?

Brad Peska: This is Brad Peska speaking.

If there are business associate agreements or contracts in place for privacy rule implementations that address the requirements that are outlined in the security rule, then there wouldn't be additional updates that would be needed to those agreements.

But the security rule requirements do as you mentioned identify some of the same activities but there are some additional items that need to be included per the security rule language.

We are looking at both providing additional information about the business associate agreement content and will continue to look at the potential to provide additional template language in the future.

(Connie Hine): Okay, thank you.

Harper: You're welcome. Next question, please.

Operator: Your next question comes from (David Markent).

(Dave Markent): Yes, my question was answered before. It was with regard to the biomedical equipment.

Is that definitely in scope requiring a risk analysis, you know, things like storage devices on Cat Scanners, MRIs, and screens that view the patient health information?

Brad Peska: This is Brad Peska. I'll direct you to the definition of Electronic Protected Health Information which will really give you the clarification of whether those systems do need to be included.

But I will tell you that with that definition including both electronic storage media and electronic transmission media the Biomedical equipment, if it contains Electronic Protected Health Information as defined by HIPAA, would be subject to and of course is - presides within a covered entity it would be considered an information system with EPHI and it would be subject to the security rule within that covered entity as part of it's overall information systems.

Harper: Does that answer the question for you?

(Dave Markent): Yes, thank you.

Harper: You're welcome. Next question, please.

Operator: Your next question comes from (Tom Hood).

(Carrie Alexander): Hello. This is (Carrie Alexander) in (Tom Hood)'s office.

Are your risk analyses always going to be complaint driven?

And if not, do you have a time line?

Stanley Nachimson: I'm sorry, I didn't quite understand you.

The question is our enforcement process always going to be complaint?

(Carrie Alexander): Is your risk analysis always going to be complaint driven?

And if not, is there a time line that you can provide us with?

Brad Peska: This is Brad Peska speaking. I want to make sure that we clarify a couple of points in your statement.

The risk analysis is a required implementation specification and the security rule that all covered entities must implement. In general, risk analysis is a process that you must perform.

But it's a very specific requirement of the security rule.

The enforcement process that I described earlier that I mentioned is primarily a complaint driven process. It refers to the process by which our office accepts processes, investigates, and resolves complaints in relation to the HIPAA Administrative Simplification Provisions that I discussed earlier, one of which being the security rule.

So I just want to make sure we clarify the concepts there.

But to focus specifically on the enforcement piece, at this time we do - we will have a primarily complaint driven enforcement process.

But we do also have the ability if needed once we become aware of certain actions that may be a violation of the rule to look into those additional actions or activities as well.

But right now our preferred and our current approach is a primarily complaint driven process.

Does that help answer?

(Carrie Alexander): Yes, it does. Thank you very much.

Harper: Thank you. Next question, please.

Operator: Your next question comes from (Jim LaFonto).

(Jim LaFonto): Hi, this is Penn State Hershey Medical Center.

The security rule says that it obligates a covered entity to make sure that business associates are able to comply with the security standards.

And in the commentary around that standard from the Federal Register there are suggestions that we might - a covered entity might want to do more than just have verbiage in a business associate degree.

I've actually heard some colleagues say that they think that we should require maybe (SAS-70) results or that we should require internal documentation policy and procedure from vendors or even one suggestion that we should acquire or contract for rights to audit the vendor ourselves to make sure they can comply with the security standards. We're getting pushback from vendors on that as you might expect.

And I'm wondering what are the trends that you see, what are covered entities requiring from business associates as a demonstration that that business associate can comply with the security rule?

Brad Peska: Sorry, this is Brad Peska.

At this time, you know, we are not able to discuss, you know, specifics of other covered entities business associate agreements or trends primarily because we, you know, are usually not a party to those discussions.

But I will tell you what the security rule requires to be implemented by the compliance date.

If there are other negotiations or contractual issues or obligations the covered entities are looking to apply against their business associates, it would be items that would be outside of the security rule and really outside of our direct responsibilities.

Not that a covered entity can pursue those types of things through contracting processes. But that doesn't apply to the security rule.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Emma LaGrand).

(Emma LaGrand): Hello.

Harper: Miss (LaGrand)?

(Emma LaGrand): Yes, I have a question regarding the password.

Could you tell me how many characters are required, and how often should the password be changed?

Brad Peska: This is Brad Peska.

The security rule does not require specifics as to the format or makeup of passwords or the frequency of change of passwords. Those are all items that would be business decisions of the covered entity.

As Stanley mentioned earlier a lot of these decisions will be based on the risk analysis of the covered entity.

And it's very - it's specific business considerations that will drive the types of decisions like the makeup of a password or how frequently it's changed. The security rule does not provide specific details.

(Emma LaGrand): Thanks.

Harper: You're welcome. Next question, please.

Operator: Your next question comes from (Mark Thompson).

(Mark Thompson): Hi, good afternoon guys.

It's (Mark Thompson), Western United.

I'm curious. Are you going to provide like a (visual) diagram in regards to how your network should look on the backend in terms of hardware?

Brad Peska: (Mark), this is Brad Peska.

We do not plan to provide any detailed either architectural or other diagrams of information systems or security models that's outside of the responsibilities and actions that we will perform in our office.

So to answer more directly, it's no.

Harper: Thank you.

(Mark Thompson): Okay, thanks.

Harper: Next question.

Karen Trudel: Dr. Harper?

Harper: Yes.

Karen Trudel: This is Karen Trudel.

Could I add something?

Harper: Sure.

Karen Trudel: I'm hearing a consistent theme here of people asking for specific guidance.

And I want to explain why it is that we are not providing this kind of guidance. We very distinctly made a decision, a conscious decision, in devising the security standards in the first place in the proposed rules, to allow covered entities as much flexibility as we possibly could.

So that each covered entity can make its own decisions about what the best security measures are for its own circumstances which again reduces the cost and the impact of implementation.

So the fact that there isn't specific guidance on what people's networks should look like, what should constitute a password, how often it should be changed, we deliberately did not provide that level of specific requirements because we want to give covered entities the ability to have some leeway to make their own decisions.

Now that being said, there are I'm sure a number of industry best practices and it's appropriate to look at those in determining what a covered entity wants to do.

But I wanted to make it clear that most of the people who commented on the final rule considered this lack of specific guidance to be a definite advantage.

Harper: And thank you for that historic reticulation and it's always good to sort of look at from someone's (side) so one will know where one is going.

Thank you very much.

Next question, please.

Operator: Your next question comes from (Robert Quong).

(Robert Quong): Hi, this is (Rob Quong) from (Alcon Scientist).

Actually kind of a two part question, the security rule requires that business associates contracts have very specific language that incorporates the security rule provisions.

However there is no requirement or it looks like from the regulations that there's no requirement that data use agreements have specific security rule language.

And I wanted to see if this was the correct interpretation of that.

The second part of my question is actually involves one of the very specific provisions about covered entities, you have the report to covered entities any security incident of which you become aware.

And if you look at the definition of a security incident it's fairly broad. It covers successful and attempted attacks on information systems.

And based on the potentially high volume of attempted attacks just as an example if you use a professional hosting company they may very well be attacked a thousand times in an hour, you know, on their systems.

What's the expectation of actually reporting all of these attacks especially since the actual language and the regulations don't really specify a reasonableness standard for reporting security incidence? It says that you really have to report any security incidence.

Thanks.

Brad Peska: This is Brad Peska. Thank you very much for your question. That is very well thought out.

To answer your first question, the security rule does not address data use agreements.

So I think the answer to that question is yes, the business associate contracts must have the required language. Data use agreements are not addressed in the security rule.

The second, to your second question we are providing and have, you know, continued to promise additional clarification on security incidence and how it shows up in several forms throughout the rule. We hope to publish that additional clarification very shortly although I cannot give you a specific date.

But in general our additional clarification in the form of FAQs that will be released will address both the security incidence within a covered entity within the business associate agreement and within the group health plans planned documents.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Lela Pronshook).

(Lela Pronshook): Thank you. We have had our question answered.

Harper: Thank you. Next question, please.

Operator: Your next question comes from (Julia Norris).

(Julia Norris): Hello.

Harper: Hello.

(Julia Norris): Hello. I have a question on the security series on the physical safeguard, that's Paper 3.

And on the Item 3, access control and validation procedures, one of the sample questions is do the procedures identify individual's roles or job functions that are authorized to access software programs?

Since this is under physical safeguards I'm wondering if this is about access to CDs or backup tapes that contain software programs or access to equipment that contain software programs.

I'm just not sure how to handle that one.

Brad Peska: This is Brad Peska.

Specifically to that question is addressing the requirement under the physical safeguard standard. The addressable implementation specification for access control and validation procedures which at the end of that addressable implementation specification identifies that - what is also if reasonable and appropriate required to have control of access to software programs for testing and revision purposes.

So that's what that question is really addressing is the access control and validation procedures addressable implementation specification under the physical safeguard standard.

Harper: Does that answer your question?

(Julia Norris): No. I could, I mean I can see that - I mean are you talking because this is under physical access.

Programs usually exist in electronic form.

Brad Peska: Right, this is Brad Peska again.

To be more specific, yeah, it would be to the physical safeguard characteristics of controlling access to those.

(Julia Norris): That would be?

Brad Peska: Programs or systems.

(Julia Norris): But when it talks about testing or revision that's usually - that's something you do electronically not physically. So that's where I'm kind of hung up on that.

And so if it's just access to the media that contains the programs whether that's a hard drive and a server or a CD or whatever, I can handle that. It's the part about the testing and revisions. Because if you…

Harper: Why don't you give us your number and we'll call you. Give us your name and your number.

(Julia Norris): Okay, it's (Julia Norris). And my number is (954) 847-4083.

Harper: Staff will get back with you.

(Julia Norris): Thank you very much.

Harper: Thank you. Next question, please.

Operator: Your next question comes from (Beverly Dennis).

(Beverly Dennis): Yes, basically I understand the audit trails for the business associates. And I understand the risk analysis that we are required.

But my concern comes with if we do everything that we're supposed to do here, have the business associates sign our contracts and then also them giving us information that they're doing their part and that we can trust it, and I know ignorance is not acceptable in the eyes of the law, but the bottom line is are we going to be responsible if someone complains on something out of our office that a vendor or business associate did and we got all the information from the beginning that they were going to go by the HIPAA rules and regulations, are we going to be responsible still?

Brad Peska: This is Brad Peska.

I'm sorry, go ahead.

Harper: We're having a little consultation in the room.

Stanley Nachimson: Okay, I'm sorry. This is Stanley.

We actually addressed I think your question in part of the regulation where it says that a covered entity is not in compliance if the covered entity knew of a pattern or an activity or practice as a business associate had constituted a violation unless the covered entity took reasonable steps to cure the breach or end the violation.

So if you've taken the necessary steps of contacting your business associate and getting (it right) and you believe you need to assure that that business associate is reasonably protecting the information and something happens unrenowned to you probably would not be held at a compliance again unless you knew that there was a problem or should have known about that problem.

(Beverly Dennis): So we would have to document everything and that would be like a due diligence. And then we would be an exempt.

Stanley Nachimson: Sure, you've got it.

(Beverly Dennis): If we did as much as we could do to correct the problem and still followed up and documented everything indicating, you know, the persons that we spoke with so that would be a due diligence and we would be exempt if we did everything we possibly could.

Stanley Nachimson: Now I can't guarantee that you'd be exempt.

But those are the reasonable steps that you would take. And I'd also refer you to that section in the regulation. It's 164.314 under the business associate contracts or other arrangements.

(Beverly Dennis): Can you give me that number again, please, you went kind of fast.

Stanley Nachimson: Sure. It's 164.

(Beverly Dennis): Uh-huh.

Stanley Nachimson: Point 314, organizational requirements, the first standard business associate contracts or other arrangements.

(Beverly Dennis): Okay. Thank you.

Harper: Thank you Miss (Dennis). Next question, please.

Operator: Your next question comes from (Phillip Toll).

(Phillip Toll): Yes, I need to get some more clarification on the systems requirement. It's been asked. And you leave us in the dark on this one I think.

And it's related to if our systems do not meet the requirements of a regulation but the vendor has stated that they will sometime in the next 12 months.

Come April 21st, do we need to implement any alternative procedures or can or will you accept the fact that we did our due diligence, the vendor has documented that they will comply?

Harper: We're thinking at the moment.

Karen Trudel: This is Karen Trudel. Can I add a point while you're thinking up there?

Harper: Yes, thank you.

Karen Trudel: It seems to me that having a vendor tell you that they're not compliant is certainly an indication that the covered entity realizes that there's a compliance issue.

So I would say that whether the vendor says they're going to be compliant later or not what you need to do as a covered entity is to try to find some other way to address the shortcoming. There's not necessarily a single way to fix the security problem.

And if there's a problem that the vendor has inherent and it's technical, perhaps there's an administrative or a physical safeguard that you can put in place to mitigate all or part of that risk.

Harper: We thank you.

(Phillip Toll): I understand what you're saying. But put yourselves in our position. We have maybe a system that has 500 users.

Are you saying we could implement a manual type procedure to record who accesses the medical record?

But you can see how inefficient that process would be. It would not guarantee even close to 100% accuracy if whether people follow procedures.

I understand where you're coming from. But you also have to put it in a business perspective. We think we've identified. We've done our risk analysis. Our vendors have been contacted. Our vendors have given a positive response. They say, "We will fix this."

But we're just concerned about, you know come April 21st for three or four months if we have a gap here will you say to us, "You did not comply with the regulation."

Or will you accept the fact that we did our due diligence. There is a solution coming. And that's satisfactory.

Karen Trudel: I'm certainly not going to make that statement. No.

Stanley Nachimson: And this is Stanley.

I'd also like to point out that you - if you've identified a risk and vulnerability, I don't think the statement that, we'll fix it in a year, is necessarily a good solution to that.

The alternative solutions as Karen mentioned I think are very important.

Brad?

Brad Peska: This is Brad Peska.

I think also from a historical perspective we do need to look at the fact that the standards of the security rule have been out and in a proposed format since 1998 and have been in proposed or have been finalized in a final security rule

for over two years now as we near the compliance date from February 20, 2003.

So I also want to make clear that there is a long history of these requirements. And the anticipation of both the final rule and now the compliance date for covered entities.

Harper: Thank you very much. Next question, please.

Operator: Your next question comes from (Dennis Lockhorn).

(Dennis Lockhorn): Hello.

Harper: Hello.

(Dennis Lockhorn): I have a question and I'd like some clarification on what I perceive as a conflict in the rule.

And it has to do with the general requirements of the security rule where it says a standard adopted in such and such regulation includes required implementation specifications, a covered entity must implement the implementation specification.

Now must is a pretty strong word, and I've heard guidance today talking about required standards that says you can adjust that based on risk.

So how do you adjust the part in the rule that says you do it on risk versus this must?

Brad Peska: This is Brad Peska.

The compliance of the security rule does require implementation of all standards and implementation specification.

When you get into the security measures is what I think we've been referring which are identified in the flexibility of approach in the general rule section where we identify that a covered entity may use any security measures that allow them to reasonably and appropriately implement the standards and implementation specifications.

So we're not making the statement, and I definitely want to clarify and thank you for the question and allowing us the opportunity to clarify, that we're not making the statement that it is optional or that you can choose not to implement a standard or implementation specification.

But there is that flexibility of approach section the ability to use the factors which makeup the covered entity one of those factors being the potential or the probability and criticality of potential risks to EPHI as a factor when you select which security measures to implement in order to comply with the standards and implementation specifications.

(Dennis Lockhorn): So a follow-up then. A rough example, we'll use the personal entity authentication. That's a required standard or specification.

And, you know, we've got 100, 120 applications roughly with patient information.

And some of them are relatively new with relatively good security built in. Some of them are old. Some of them are very little used.

Across the board it's very difficult to say in all systems we have person or entity authentication.

So how would you address that type of scenario?

Stanley Nachimson: I think what we're saying is that in your more sophisticated systems as an example, that have the built-in authentication procedures you met the standard for those systems.

And those systems which may not have any type of authentication procedures built-in you've got to determine an appropriate way for those systems to meet the standards for personal or entity authentication. Whether that's some sort of front end or other procedure we're not going to specify.

But that - the way that you meet that standard it's up to you for each individual system, but you have to have personal or entity authentication for each of your systems.

And that, you know the technical piece is the easy one. You know, the password, the biometrics those things.

Some of the old systems that don't have that built-in and are not even network based some of them are relatively ancient. You really struggle to find anything to - any tool to use on these systems.

And yet you can't just chuck them.

(Dennis Lockhorn): Could you do that with policy then or? Give examples.

Stanley Nachimson: Let me give you an example of a program that you say is not network based.

In other words that perhaps resides on one individual machine or another individual's machine.

(Dennis Lockhorn): Yes.

Stanley Nachimson: The access to that system to that machine is based on hopefully a password for that individual user.

So hopefully the only person getting on that machine is that individual user. And therefore those are the only people that have access or are authenticated for that individual program. That's one example of controlling that.

So a front end password authentication procedure for the machine guarantees that that authentication is for that individual program. It's just an example.

(Dennis Lockhorn): A lot of times some of these you can use, you know, if they are network based you could use, you know, the network level login as entity authentication. That doesn't always work in all areas either because of work flows, you know, and the one that comes up commonly is the surgery area actually take their gloves off and touch a machine.

Brad Peska: Right and this is Brad Peska.

I also want to make sure that we continue to clarify that there are, you know, of course business decisions that also need to be made here. Stanley and I have mentioned based on the risk analysis and organizational factors that may allow you to make certain determinations on how to handle these situations.

At this point we are not providing specifics on implementation of these standards.

We will however continue to try and clarify some of these issues in the future and we will definitely take this into consideration.

(Dennis Lockhorn): Okay, you just went back to the original statement though. You said you do this risk based and yet they are required standards.

So it's kind of a circular argument that we keep hearing.

Brad Peska: This is Brad Peska again.

We are looking for covered entities to make reasonable and appropriate decisions to comply with the security rule.

And your scenario it sounds like there are potential options some desirable, some not desirable for your specific entity.

And we do require that you take into consideration those factors when you're making your implementation decision.

But inaction is not an element of the security rule.

Harper: Thank you very much.

Mr. (Paris) we have time for one more question, please.

Operator: Your final question comes from (Greg Lyman).

(Greg Lyman): Hello and thank you all for your time today.

I would like to ask a question on whether you will be distributing some content or guidance for the response to a complaint from a covered entity so that we as covered entity may be able to prepare in advance materials and documentation that would be.

Brad Peska: Thank you. This is Brad Peska. Thank you very much for your question.

You know our preference of course would be that we would never have to involve any covered entities in the complaint process.

But being that it does exist and we are here to enforce the rule, the Federal Register Notice that I identified earlier and referred to does identify the responses both to the initial notification from our office to a covered entity the acceptable responses as well as any potential circumstances where the covered entity disagrees the content that we are looking for them to provide us in writing as to the disagreement.

So there are - there is a framework. Within those procedures, there is no additional, you know, standard reply response because we do anticipate the covered entities will respond to our initial notification and subsequent requests for information as part of the investigation process in different ways.

So even though, you know, we do provide the guidelines in that notice.

But we do not have a format or structure for replying back to us.

Stanley Nachimson: And this is Stanley.

And I think we would anticipate that for security complaints for example, the documentation requirements within the security rule are things that we would be looking for.

So I don't know if we would look for additional types of documentation beyond that what is already required by the security rule.

Harper: Thank you very much. I want to thank the attendees today for the conference and your being on line with us. I'd like to thank the staff members for their presence here today.

And I have a little more information I'd like to give you just to remind you that you can go to our website which is located at www.cms.hhs.gov/hipaa/hipaa2.

We will be posting a transcript of this call on the website as well as future announcements of conference calls.

And just as a reminder I'm sure you know it, that the deadline for the compliance with the HIPAA Security Rule is April the 20th, 2005, and it's right around the corner.

And April the 20th, 2006 for small health plans.

If you have additional questions, please email us at your - at our electronic mailbox at askhipaa@cms.hhs.gov or call the HIPAA hotline at 1-866-282-0659. I'm going to repeat that telephone number, 1-866-282-0659.

Now Mr. (Paris), can you tell us how many persons we had on line today, please?

Operator: Today's teleconference had 1,400 participants and more.

Harper: Thank you very much. The conference is over.

Operator: This concludes today's conference.

You may now disconnect.

Harper: Thank you.

Man: Thank you very much Dr. Harper.

END