

Edited Transcript of the February 28, 2003 HIPAA Implementation Roundtable focusing on
Security and Electronic Transactions and Code Sets

CENTERS FOR MEDICARE AND MEDICAID SERVICES

Moderator: Bernice Catherine Harper
February 28, 2003
1:00 pm CT

Operator: Good afternoon. My names is (Dashandra), and I will be your conference facilitator. At this time I would like to welcome everyone to the Seventh National HIPAA Implementations 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 Star then the Number 2 on your telephone keypad. Thank you.

I will now turn the call over to Dr. Bernice Catherine Harper. You may begin your conference.

Bernice Catherine Harper: Thank you, Ms. (McKullup).

I guess I should say good afternoon to some and good morning to others. I think you should know also in Washington, D.C. and Baltimore we're snowed in, but the government is not shut down. And we're delighted about this. And we were debating last night what we would do if we could not make it to our offices. We were planning to have this call from our various homes. But

we're just delighted to be able to be in Baltimore and can have the call from this facility.

As you know, this is the Centers for Medicare and Medicaid Services, or better known as CMS, which is part of the Department of Health and Human Services. Our subject today is Health Insurance Portability and Accountability Act of 1996 or HIPAA and specifically the Administrative Simplification provision.

There are four Administrative Simplification provisions; and these are 1, unique identifier, 2, privacy, 3, electronic transactions and code sets, 4, security. Our call today will focus on the last two, electronic transactions and code sets and security.

We regret that today we will not be able to answer any questions relative to privacy. But we're going to be scheduling a session in March, which we'll give you the date later, and this session in March will deal specifically with the privacy question.

So now it's my pleasure to call on Karen Trudel. After she gives some opening remarks, this will be followed by questions and answers.

Karen?

Karen Trudel: Good afternoon. Thank you very much, Dr. Harper.

We're very glad to be here with you for the seventh annual roundtable. And we are very relieved not to be doing this from our various kitchens.

We were very happy to be able to do presentations for you today on two recently published Final Rules, one on HIPAA security standards and the other on modifications to the transaction and code set standards. Both of these regulations were published in the Federal Register on February 20.

And we have a presentation on security first that I will provide. Then we'll have a presentation on the modification that Gladys Wheeler will present. We'll then open up to questions not only relating to these two regulations but any issues that you have to do with transactions and code sets.

As Dr. Harper says, we do not have a privacy expert from the Office of Civil Rights on the phone today. We did not do that because we do have some fairly voluminous presentations, and we wanted to be able to get in all of your questions about these two new regulations, which were long awaited. And we will be doing a one and a half hour privacy only roundtable towards the end of March. And there will be a fair amount of publicity on that when we have the specifics set up.

So let me get to the first presentation, which has to do with HIPAA security standards. We did publish a final regulation in the Federal Register on February 20th. If you're interested in the specifics of that, paper versions of the federal register are available from most public libraries. And you need to give them the date and the fact that you're looking for Volume 68, Number 34.

The effective date of the regulation will be April 21st of this year. That is to account for a 60-day congressional review period because it's considered a major rule. That makes the compliance date – because remember, the clock starts ticking at that point – the compliance date will be April 21, 2005 except for small health plans, which will have an extra year, until April 21, 2006.

And again, documents can be located either at the library, at the Government Printing Office Website, or there are documents at our own Website at www.cms.hhs.gov/hipaa.

The purpose of the security standard is to ensure the integrity, the confidentiality, and the availability of electronic protected health information. And electronic protected health information is a concept that I think many of you are aware of because it was established in the course of the privacy standards.

So we're talking about essentially the same kinds of information, information that is identifiable to a certain person that includes health information. And we're talking about ensuring not just the confidentiality of that data but the integrity and the availability of it too – integrity meaning that the data has been inappropriately modified or corrupted, and availability meaning that it's there when you need it.

Now security is always a balance. The very best security of electronic data is when you lock it in a room and you never let anybody see it. Unfortunately with respect to health information, health information we need to share with certain people. Physicians need to be able see information that relates to their patients. They need to be able to send it to health insurance plans so that their patients' bills can be paid. So there's always a balancing act of how much security, how much you let people see data, and how much you can keep it safe.

So what we're trying to do here is to protect against reasonably anticipated threats or hazards and improper use or disclosure. And again, we're talking about reasonably anticipated. I think everyone knows because of the publicity

that surrounds viruses and that kind of malicious software on the Internet that it's not really possible to have completely secure data and systems. So we're always talking about a tradeoff between what's feasible and what you can reasonably anticipate and take action for.

The scope of the security standards applies to all electronic protected health information. It includes data that is in motion and data that is at rest. And security standards must be met by all covered entities.

Let me explain that a little bit because there's some misunderstanding there. A provider that is a covered entity is one that conducts electronic transactions. That means that, if you are a covered entity, if you are a provider, all of the electronic data in your possession whether it relates to a transaction, whether it's in motion, whether it's at rest, all of it is covered. So you do not need to just safeguard data when you transmit it. You need to safeguard data when it is stored electronically in your facility as well.

Alternatively, a covered entity could have – a provider – could have electronic information stored on their facility that they never send anywhere in connection with a transaction. That provider is not a covered entity because they do not conduct transactions electronically. And the security standards do not apply to them.

Let's talk about the linkage between security and privacy for a moment. They are definitely closely linked. Security is what enables privacy. What do I mean by that? Once you have decided what the appropriate disclosures of data are, security is the sum total of the mechanisms that you use to make sure that that data is not shared in any other way.

The security scope in one way is larger than privacy. Privacy just talks about the confidentiality of information. And security also contains standards that protect the integrity and the availability, as I said before. Is the data being inappropriately changed – we hope not – and is it available when we need it?

The privacy scope is larger in that it addresses both paper and oral protected health information in addition to electronic. You will not see in these security standards any standards for the protection of paper data. The reason for that was that, when the security regulation was initially published, we had made a decision that we would limit the scope to electronic data. And when the privacy rules subsequently included paper, we made a determination that we would not change the security standards to include paper requirements. We would adopt paper requirements later, if it became necessary.

The security standards in general are based on three concepts. And I want to emphasize here that we are talking about an extremely common sense approach to security. We tried to make sure that our standards were flexible and scalable, which means that they permitted the standards to be interpreted and implemented appropriately from the smallest provider to the large health plan. What works for a small dentist's office does not work for the Medicare program. We acknowledge that.

They need to be comprehensive. They need to cover all aspects of security, behavioral as well as technical.

And what do I mean by that? You'll see, as we talk, that many of the standards really do not have a technological component at all. They really are people oriented. They are process oriented. And the example that I like best is that you can have a really wonderful computer system that requires all of the users to log on and to change their passwords periodically. And that's

really great. But if your staff is not trained to know that it's not okay to write your password on a little yellow sticky note and stick it on the monitor, the technological solutions will not work. So we're trying to cover all of the aspects of security.

The third general concept is that they're technology neutral. That means that we can utilize any future technology advances in this fast changing field without having to go back and realign the standards.

In the public comment period on the proposed regulation we basically got widespread support for these general concepts. And people said we needed to provide even more flexibility and that in some cases we had imposed too many hard and fast requirements.

So the changes that we made from the proposed rule consolidated and tightened some of the requirements. It added some flexibility in the guise of the concept of addressability that I'll talk about later. And it coordinated very closely with privacy.

One example of that is that in the proposed rule we had a concept called the chain of trust agreement that handled how you assure security as you pass data from one person to another. And we now handle this via the business associate agreement that's already a common concept in privacy.

So we have adopted both standards and implementation specifications. The standards are general requirements. There are 18 administrative physical and technical standards. There are four organizational standards that only need to be met in certain circumstances because they relate to hybrid entities, group health plans, et cetera. And there are two overarching standards that require policies and procedures and documentation.

The implementation specifications are specific measures that pertain to a standard. They explain things that you need to do or should do in order to be able to accomplish what the standard is. There are 36 implementation specifications. Most of them are addressable. And I'll talk about that in a moment.

These specifications can be either required or addressable. And if you look in the regulation, you will find a really nifty two-paged matrix that explains exactly what all of the standards are, all of the implementation specifications, states whether they are required or addressable, and then sends you to the right section of the document to go and read more about it. It's a very helpful tool.

If I could suggest something to you in terms of looking at this very voluminous document in a very fast way, I would suggest first reading that matrix and looking at the regulation text itself and then going from there.

Required implementation specifications must be implemented. They are things that you have to do. And if you don't do it, you can't successfully implement whatever the standard is.

The addressable ones must be considered and implemented, if appropriate. And if not appropriate, you need to document the reason why and what you did do in its place.

Standards can have either no separate implementation specification; they can have one or more specifications that are all required, one or more that are all addressable, or a combination of the two. But the bottom line is that all the standards must be implemented using a combination of either the required and addressable specifications or other security measures. It's important to

documents those choices. And this allows covered entities to make their own judgments regarding the risks and the most effective mechanisms to reduce the risks.

Two examples – there is one requirement called assigned security responsibility. And what it means is that you have to find someone in your organization and tell them that they're in charge of security. That kind of didn't seem to need any more explanation from our perspective. And as a result, there's no implementation specification.

There is another requirement called security management process. It requires a risk analysis, risk management, sanction policy, and information system activity review. All of those things we felt were needed in order to be able to set up a workable security management process.

And there's another requirement standard for security awareness and training. The specific topics to be discussed are addressable. They include things like log in monitoring and protection from malicious software. But even if none of those topics were relevant the covered entity still has to conduct training. And they can decide how they're going to provide it. Are they going to do it by computer based training, formal classroom training, reminders at staff meetings, whatever? So where all the specifications are addressable, these standards still must be met.

Other changes that we made in the final regulation over the proposed rules are encryption over an open network is now an addressable specification instead of being required. And we did that in order to not cause problems with Internet communications, e-mail communications between physicians for example.

And we also originally had a requirement for certification that required covered entities to either internally or externally certify that they had met all the security requirements. At this point the requirement is now for evaluation and is a much less rigorous requirement in terms of not having to go out and hire a consultant, et cetera.

In terms of outreach we will be developing technical assistance materials. We're already working on a security video. And we are going to be targeting especially small providers who don't have information technology staff and may need to get up to speed with concepts like what's a risk analysis and what's a contingency plan and how does that apply to me.

Again I would stress, if there's something that you can take away, it's that these requirements are common sense. They are things that you can see if you walk around your facility – making sure that people's computers monitors are not turned in such a way that electronic protected health information can be seen by people who shouldn't see it; that computers are not left unattended with protected health information showing on the screen; that you do need to have passwords, the passwords need to be changed periodically; that your electronic facilities need to be appropriately guarded whether that's in terms of a large computer facility or a small server closet; and that you do need to make sure that you staff is trained to understand some of these things, that they know what is appropriate and what is not appropriate; that when you terminate staff you make sure that they cannot continue to get into your network; that there is someone who is in charge of responsibility; that any incident procedures, viruses, whatever, can be dealt with and reported, that there are procedures for that; that your business associates, just as you're modifying your contract for you privacy provisions with your business associates, you need to make sure that you modify them also to take account of security. You need to make sure that people understand what to do with

respect to storing electronic media, whether it's diskettes or tapes and that there are policies in place as to what you do to those media before you throw them out, before you reuse them, basically that your system is set up in such a way that people only have access to the data that they need to do their job.

This is the common sense approach. It is not one that is heavy on technology. If you look, the vast majority of standards are administrative. They have to do with staffing, with training, with making sure that people are aware of what's going on. And that is something that is very critical.

It's entirely possible that a covered entity would not need to make any additional technology purchases in order to meet these requirements. And it's very important to keep that in mind and to make sure that you do a risk analysis before beginning to look at whether you do need to purchase additional consultant services, technology products, whatever.

And I do suggest very strongly that you take a look at the regulation. We will be developing outreach materials as quickly as we possibly can. They will be posted on our Website, which again is www.cms.hhs.gov/hipaa.

And that's it for security. Now I'm going to turn it over to Gladys Wheeler, who's going to talk a little bit about the modifications to the transaction and code set.

Gladys?

Gladys Wheeler: Good afternoon, everyone. This is Gladys Wheeler from the Office of HIPAA Standards. I'd like to give you an overview of the transactions modifications Final Rule also known as the Addenda Final Rule.

First I want to alert you to the fact that the Federal Register document has some inaccuracies. And the Federal Register will be publishing a correction. The PDF version on the CMS Website at www.cms.hhs.gov/hipaa is correct.

This Final Rule combines the two notices of proposed rule making published May 31, 2002. The adopted modifications are the responses to the problems in implementation of the transactions and code sets that were adopted by the August 2000 Final Rule.

Change requests to correct these problems were submitted during the designated standard maintenance organization change request process. They were presented to the National Committee on Vital and Health Statistics. And they were proposed by the Secretary in the two notices of proposed rule making. We received public comments on the two notices and consulted with the DSMOs on those comments before adopting the Final Addenda.

Some of the major provisions are the Final Rule adopts National Council for Prescription Drug Programs – that's NCPDP – the Batch Standard Batch Implementation Guide Version 1, Release 1 for retail pharmacy drug claims, eligibility, and coordination of benefits transactions. This replaces the earlier version from August 2000 that adopted Version 1, Release 0.

It adopts the NCPDP Batch Standard Batch Implementation Guide Version 1, Release 1 and the Telecommunications Standard Implementation Guide Version 5, Release 1 for the referral, certification, and authorization transactions. This replaces the ASC X12N 278 – Health Care Services Review Standard that was adopted by the August 2000 Final Rule.

It adopts the ASC X12N 835 – Health Care Claim for payment and remittance advice for retail pharmacy, healthcare payment and remittance advice

transactions. This replaces the NCPDP Batch Standard Batch Implementation Version 1.0 and Telecommunication Version 5.1 that was adopted in the August 2000 rule.

In addition to those modifications we also made some modifications to the actual standards implementations guides that were adopted. This Final Rule retracts the adoption of National Drug Code for reporting drugs and biologics on non-retail pharmacy standard transactions. It does not adopt a replacement standard at this time.

And we realize that the fact that the Final Rule does not adopt any standard for reporting drugs on non-retail pharmacy transactions is inconsistent with the Implementation Guide. And we will be working with the DSMOs and the industry to make the necessary adjustments to the Implementation Guide.

It adopts certain modifications that were considered maintenance, which are minor changes to correct errors or to clarify some of the standards. Some of these examples for some of the more substantive changes involved – we modified the requirements to report HCPCS codes on all outpatient hospital services, which was previously required. That requirement has been changed to only reporting the HCPCS codes when there is one for that particular service.

We modified the required usage of the healthcare provider taxonomy codes at the line level and the claim level for institutional claims to situational uses at the billing or pay to provider level for institutional claims. We modified the required usage of a healthcare provider taxonomy code on professional claims to situational usage.

We maintain the original specification for reporting anesthesia time in units and minutes. A provision of the proposed agenda was to report anesthesia services in minutes. And the Final Addenda permits anesthesia services to be reported in minutes and units.

This Final Rule also adopts the addenda for the 834 Enrollment and Disenrollment in a health plan and the 837 coordinates the no benefits transactions, which were not in the May 2000 proposed rules. We did adopt the addenda in this Final Rule.

The compliance date for the Final Rule is October 16, 2003. And I think that's it for the major provisions. I would ask you to please take a look at the Final Rule. For now use the version that is on our Website because that is the correct version.

Thank you.

Karen Trudel: Okay, this is Karen again. I want to just kind of wrap up with Gladys just presented in terms of the changes being in three basic groups.

The first group, where Gladys mentioned we were adopting one standard instead of another, those issues only apply to you if you are a retail pharmacy.

The second major change applies to you if you are not a retail pharmacy. And that has to do with the fact that you will no longer be required to use the National Drug Code. You can continue to use the HCPCS codes or whatever you're using right now. And you need to talk to your health plan trading partners to find out how that's going to work.

And then the third is the fact that we have adopted changes to the Implementation Guide. In some publications you will hear them referred to as Addenda. And the really important thing for you to take away from this discussion is that now you have another question to begin to ask your vendor and your health plan trading partners. And that is when are you going to be ready with a version of these standards that includes the changes in the addenda. And the other shorthand way to refer to this is the addenda are called 4010a. So you would want to ask your vendor when are you going to be able to deliver to me software that is compliant with the HIPAA standard in 4010a. So those are kind of three takeaway points.

I think we've pretty much carried out all of the presentation. And rather than talk at you anymore I think we're just about at a time where we want to begin to entertain some questions. So perhaps the operator wants to begin to look at the question poll.

Operator: At this time I would like to remind everyone in order to ask a question please press Star then the Number 1 on your telephone keypad now. We'll pause for just a moment to compile the Q&A roster.

Your first question comes from (David Pate).

(David Pate): Yeah, this is (David Pate). I had a question regarding electronic claims transmission.

If claims are received electronically – well anyway we're a PPO – if claims are received electronically and converted to paper to be transferred to a third-party administrator who does not receive claims electronically, does that make the PPO a clearinghouse or covered entity?

Stanley Nachimson: Hello. This is Stanley Nachimson. In this situation the PPO is serving as a representative of individual providers. And the organization is taking electronic transmissions from those providers, turning them into paper claims, and then sending them to the third-party administrator for processing?

(David Pate): Yes.

Stanley Nachimson: Yeah, in that situation the initial provider would then not become a covered entity because they are engaging in paper transactions. However, I think it's important to realize that the TPA is obligated under the HIPAA regulations to be able to accept electronic transactions. They cannot require provider organizations to only send them paper. So it's certainly the choice of the provider organization to send paper or electronic transactions to a health plan, which in this case is represented by the TPA. But if that provider organization wants to send electronic transactions as their means of submitting claims, for example, the third-party administrator is absolutely obligated to accept those in the standard format.

(David Pate): If they have no claims that are over the \$5 million limitation, you know, for the year until that type of thing, does that change the situation?

Stanley Nachimson: I believe you're talking about on a small health plan if they have less than \$5 million in receipts?

(David Pate): Yes.

Stanley Nachimson: That would normally change the situation; however, the deadline for all health plans is now October 16, 2003. So, as a small health plan, they're obligated by October 16, 2003 to be able to accept the standard electronic transactions.

(David Pate): Okay, thank you.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from (Ken Fabric).

(Ken Fabric): Yeah, hi. This is (Ken). You mentioned in the first part of the meeting about encryption of e-mail. Could you go over that again or just the need to not encrypting e-mail?

Karen Trudel: Yes, I can answer that. Initially the proposed rule required that all transmissions over an open network be encrypted. We have since decided that – and the Final Rule reflects this – that it is not required to encrypt transmissions over an open network. It is something that the covered entity needs to assess to determine whether that is appropriate for them and under what circumstances. For instance, Medicare does not even accept transmissions over the Internet at all. So that is something that each covered entity needs to think about.

What I said about encrypting e-mail was that one of the considerations that we had was that especially for small health care providers who are communicating among each other via e-mail to discuss patient care, requiring that those transmissions be encrypted could have a chilling effect on patient care. And therefore, that was one of the considerations that caused us to make this an addressable implementation specification. Therefore, the general rule is encryption over an open network is addressable. The covered entity needs to look at whether they need to do it, make a decision as to whether it's right for them or wrong, and then either implement or document what else they're

going to do to keep communications over an open network like the Internet safe and secure.

And one thing – someone who’s a provider told me that what they do, when they do Internet e-mail communication with their patients is that they tell the patient ahead of time, if you’re going to e-mail me, you must understand that the Internet is inherently an insecure medium. And if you’re going to use it, you need to accept that risk. And essentially that is one of the other things that they’ve put in place to increase the awareness on the part of the patient as to whether they want to accept that risk or not.

(Ken Fabric): Okay. Yeah, I understand.

Bernice Catherine Harper: Thank you very much. Next question please.

Operator: Your next question comes from (Pat Mackinenny). (Pat), your line is open.

(Pat Mackinenny): Hello?

Karen Trudel: Yes?

(Pat Mackinenny): Okay, sorry. I was wondering if you could clarify the electronic data that’s covered by security – I got a little confused when you said it’s only if it’s transmitted or if there was an organization that was not going to ever transmit it, then security doesn’t apply to them. Can you clarify that again?

Stanley Nachimson: Sure. And that’s really in two parts. The regulation requires that covered entities follow the requirements of the security standards. A covered entity is a health plan, a healthcare clearinghouse, or a provider that transmits

information electronically. So the first step is decide if you're a covered entity.

(Pat Mackinenny): Yes.

Stanley Nachimson: If you're a health plan at a clearinghouse, you have to follow those security rules. If you're a provider and you transmit information electronically, you then become a covered entity and then must follow the requirements of the security rules.

The security rules require that all electronic protected health information is protected according to the rules. And electronic protected health information is information that's in electronic form and it's either stored, received, or transmitted by a covered entity.

So you're really got the two tests here. First determine if you're a covered entity. And then again, if you're a provider, if you transmit the information, you become a covered entity. And then you have to protect information that's both stored. And that's all electronic protected health information either stored or transmitted.

(Pat Mackinenny): That was really my question. I don't have to worry about – I have to worry about all my data, not just the data I might transmit.

Stanley Nachimson: That's correct, if you're a covered entity.

Bernice Catherine Harper: Thank you. Next question please.

Operator: Your next question comes from (Ken Rivar).

(Ken Rivar): Good afternoon. A question I have is specific to the 4010a release, the version. Has CMS published a timeline yet as to when they are going to be able to provide test files for their trading partners in the 4010a format?

Janis Nero-Phillips: As far as the Medicare program is concerned – this is Janis Nero-Phillips at CMS – as far as Medicare is concerned, we're looking at implementation of 4010a by April 1st at the Medicare contractors. So we're hoping to open up testing and to allow providers to work with the EDI department at the contractors soon after April 1, 2003.

(Ken Rivar): We're on the payer side of that. So when would the payers for the COB format be able to get test files?

Janis Nero-Phillips: Probably shortly thereafter, probably towards May 1, 2003 – we're planning to go full steam ahead with the 4010a implementation for the 837 inbound and outbound and the 835. And then the other transactions will follow.

(Ken Rivar): So that sort of says that the direction's been set, and really there is no more effort being put on the 4010. Is that correct?

Janis Nero-Phillips: Partly. Providers can test on 4010 right now with contractors, so we are continuing our effort with testing and bringing providers into production on 4010. And for payers like yourself, you can test the COB on 4010 now.

(Ken Rivar): Okay. I have one last question. Has any memorandum or anything been published by Medicare regarding what Medicare would expect to receive back from a payer who received electronic 837 4010a crossover and in terms of 997s, et cetera?

Janis Nero-Phillips: No, we don't have that documentation for the functional acknowledgement. We have not published that.

(Ken Rivar): When will you publish that?

Janis Nero-Phillips: I don't think we're ever planning to do that. That's really on a case-by-case basis.

(Ken Rivar): Doesn't that leave a large whole though? Because one of the primary concerns we have is that today of course taking in NSF's we have a way to balance the file that we receive, question anything that our trading partner agreement would not have required to be sent, and, therefore, resolve any billing problems and so forth. Without something, you know, in place of that it seems like we have a large whole there that doesn't have any, you know, solution to address administrative billing issues.

Janis Nero-Phillips: Well I would suggest that you contact the specific contractor and see if you can work something out with their EDI department to get that type of information because we have not formally said that that's a requirement for the contractors to send back that information on the 997.

(Ken Rivar): Okay, thank you.

Janis Nero-Phillips: You're welcome.

Karen Trudel: Thank you.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from (Becky Anderson). Ms. (Anderson), your line is open.

Shay Vaughan: Hi. We're calling from ISIS Healthcare Systems. We're a software vendor and a clearinghouse. We have a question regarding the drug information requirement, the drug pricing information that's in the 2410. We're trying to figure out, since the NDC is no longer required for non-pharmacy, is the other information in that loop still required for non-pharmacy, such as unit price, quantity, unit of measure?

Janis Nero-Phillips: We haven't made a determination on that. We're trying to put out our final change request for the contractors for the NCPDP transaction. And that's something that we can get back to you about. So I'd like to take the information from your question and then get back to you.

Shay Vaughan: Okay. And I'm sorry. Who is this that I'm speaking with?

Janis Nero-Phillips: Oh hi. This is Janis Nero-Phillips again.

Shay Vaughan: Okay.

Stanley Nachimson: And that question was specific to Medicare, right – whether Medicare will be requiring the information in that loop?

Shay Vaughan: I guess we can start with Medicare. It's really for all (ANSI). But let's start with Medicare, yes.

Stanley Nachimson: The implementation guide should be specific as to whether the information is required or situational. And that's the guide that should be

followed. Now it may be that each health plan will be looking at the situations to determine whether or not that information will be required.

Karen Trudel: I guess what we'd like to do is, if you don't mind, share your name and phone number. Although in the interest of privacy protections I have to warn you that there are several thousand people listening. If you're willing to give us your name and phone number, we can go find an Implementation Guide, take a look at it, and see what we can work out after we've put our heads together, and give you a call back.

Shay Vaughan: Sure, I'm bold. And my name is Shay, S-H-A-Y, Vaughan, V-A-U-G-H-A-N.

Karen Trudel: Thank you, Shay.

Bernice Catherine Harper: Thank you very much. Next question please.

Operator: Your next question comes from (Patrick) (sic) (Fowler).

(Patrice Fowler): Hi, this is (Patrice). Our party intermediary has some information out on the Website about the part of the eligibility transaction. And I've also seen some program memorandums talking about a MCN Network. Can you tell us what the strategy is to support the eligibility 270/271 from a CMS perspective for Medicare?

And Number 2, I appreciate these calls. I think you guys get out a lot of information. But if there's thousands of us on here, I know that we're not all getting our questions answered. So I'm wondering if you can give us some info on when the FAQ support could start up again, because that's a very, very

helpful tool out there? And I think the last time we saw an update was in 2001. Thanks, Stanley.

Stanley Nachimson: You're welcome.

(Patrice Fowler): And Karen, and everybody there.

Karen Trudel: Thank you. Actually I'll answer the second part of that question first. This is Karen. And then I'll turn the first part over to Janis.

There are two different Websites where there are frequently asked questions included. And one of those is an HHS Website. The frequently asked questions are no longer being posted on that Website. We do have frequently asked questions on our own Website, which again is www.cms.hhs.gov/hipaa. And there are updated frequently asked questions there. We're handling them as quickly as we can. And when we receive e-mail questions, when we do find that we're getting the same question from a number of people, we do turn it into a FAQ. So...

(Patrice Fowler): What kind of turnaround could we see on that? I sent one in on the (EIN) probably a month and a half ago.

Karen Trudel: It really depends. Some of the questions that are – the more complicated the question and the more research it requires and if it needs to go to our legal department or if we need to consult with one of the standards developing organizations, it can take definitely weeks and maybe months. We're turning around some of the I need materials, I want a copy of the video, I need to know if I'm a covered entity, can you tell me where I can find information, those we turn around sometimes within a day or so. So it really just kind of

depends. And the more complex ones do take a lot longer. And we do beg your patience. There's nothing easy about some of this stuff.

We do have frequently asked questions posted already on security and on these modifications, at least the ones we thought would be frequently asked. So we suggest you might want to go there if you have questions on those topics.

And now Janis will answer the question on eligibility.

Janis Nero-Phillips: Yes. Okay. Hi, this is Janis again. And your question was about the 270/271 transaction and how your intermediary is implementing – was that your question?

(Patrice Fowler): Yeah, you know, it sounds sort of confusing, but we're getting through to them on a local network right now. Then I've read things that we have to go to IVANS. And then I've read other things that talk about this future move to MCN. So for long-term strategy we want to know what's the way we should be trying to go.

Janis Nero-Phillips: Certainly. We're in the process of completing the final (PN) that will give instructions to the contractors for implementation of this transaction. That should be going out within the next few weeks. And we're looking towards a July implementation of this transaction of the contractor site.

You're correct. There are several ways that a provider can set up to become connected to the CWF through their data center. And for the intermediaries the LU6.2 is a methodology that could be used, if you've set that up already. And then the other alternative is to use IVANS, which is a

telecommunications resaler for CMS, to get linked into the AT&T network. And your transaction will go through the data center straight to the CWF.

So the details behind this are coming out very soon. I suggest that you either contact your intermediary in a few weeks to ask more questions about this. And they will also be getting out to the providers to give them information as far as provider education on how to send in this transaction.

We are doing the 270 in a real-time mode. That has been decided.

(Patrice Fowler): That's great. Thank you.

Janis Nero-Phillips: You're welcome.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from Dr. (Peter Kanaris).

(Peter Kanaris): Yes, hi. This question really has to do with again determining whether or not I would be a HIPAA entity. And I think it may have been addressed earlier, so forgive me if it's redundant.

But in the process of sending out a paper fax that unbeknownst to me could be received by a computer modem, would that make me a HIPAA entity, if in all other ways I am not currently a HIPAA entity, or by merely sending paper does that keep me safe in this regard?

Stanley Nachimson: Yeah, and that's an excellent question. If you are sending a paper fax, again only using a plain paper fax machine, you would not be considered a

covered entity. We're not considering transmissions from regular fax machines to be electronic transmissions.

However, if you're using your computer to create the fax and do that, that is considered an electronic transaction. So that would make you a covered entity.

But whether or not the entity at the other end receives it via computer modem or some other way that does not make you a covered entity, if you're using the plain paper fax.

I just also want to let folks know that we have on the CMS HIPAA Website that's been mentioned a couple of times a tool that anyone can use to determine whether or not they're a covered entity. Questions like this could possibly be answered by the tool. We're certainly welcome to take them here. But it's available for anyone to use to help determine whether or not they're a covered entity under HIPAA.

Karen Trudel: And when you look at our Website, that's called the I believe covered entity decision tool.

(Peter Kanaris): May I ask a second brief question? Just a point of clarification – I believe it was earlier stated that the compliance date for the security rule was April 21st '05. Is that correct?

Karen Trudel: Yes, that's correct.

(Peter Kanaris): Okay. So that means we don't need to have a plan in place necessarily until that date?

Karen Trudel: That's correct. However, a number of people have said that they need to think about security at the same time that they're thinking about privacy. So there is some connection between the two. And indeed, as you're looking at setting up privacy training, there's always the consideration of whether you want to at some point in the future add security training to it or whether you want your privacy officer or coordinator to be the security person also. So there are some considerations we recommend you start thinking about sooner.

(Peter Kanaris): Thank you very much.

Karen Trudel: You're welcome.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from (Brian Ross). Mr. (Ross)?

(Brian Ross): Yeah, sorry about that. A question back on – to continue the discussion around the 997, I'm trying to understand if there's a standard way that we're going to be looking for these intermediaries to respond to us. It seems like there's a lot of possibilities in the absence of a standard. So what is CMS's approach with these intermediaries? Are you putting some guidance that in this circumstance kind of 997; in another circumstances, you know, send a 277? And again, in the absence of those HIPAA compliance components, what is the instruction, as they're being given?

Janis Nero-Phillips: Hi. This is Janis Nero-Phillips again. From a contractor perspective we've asked the contractors EDI departments to send back error reports. So when a submitter or provider sends in a healthcare claim, let's say for example, they will receive an error report back from the EDI department noting what was wrong with the transaction.

We have also created companion documents for the 837s and the 835, which you can obtain from your respective contractor also. The companion document for the 837I should be out in a few weeks. But the one for the 837 professional and the 835 are already ready. So I would suggest that you get in contact with your specific EDI department at your intermediaries. And they can tell you exactly what they can provide to you to let you know about the disposition of errors on transactions that you may send in.

Bernice Catherine Harper: Thank you. Next question please.

Operator: Your next question comes from (Christina Hobbs).

(Christina Hobbs): Yes, good afternoon. You mentioned the matrix for the security rule. And I wondered if that could be accessed online. If so, how?

Stanley Nachimson: The matrix that you're referring to are basically included in the last several pages of the regulation. That can be accessed in a couple of places, both the CMS Website that we've mentioned before and the Website at the Office of the Federal Register, if you look for the regulation that was published on February 20th. It's in the last two or three pages of the regulation. So it is both an excellent tool and actually an official part of the regulation.

(Christina Hobbs): Okay. Thank you very much.

Stanley Nachimson: You're welcome.

Karen Trudel: I think I'm kind of getting a sense that it might be helpful for us to post just the matrix on our Website as its own small document. And we're all making notes to go ahead and do that after this.

(Christina Hobbs):Great.

Bernice Catherine Harper: Thank you very much. Next question please.

Operator: Your next question comes from Cherylinn Smyrski.

Cherylinn Smyrski: Yes, hi. My question is regarding re-billings for dates of service prior to 10/16/03. I've had previous communications, and I just need some further clarification. I had asked a question, and I received an answer from CMS indicating that you have to make reasonable effort to obtain newly required fields if you're transmitting after 10/16/03.

Actually I have two questions to that. How do you quantify reasonable due diligence? That's number one.

And number two, other payers are not going to accept due diligence because the Implementation Guides stipulate that you have to have these data content fields. And if you don't have them after 10/16/03, they're going to deny the claim, which impacts revenue greatly.

Stanley Nachimson: So you've got a couple questions. Have we actually specified what a reasonable effort or due diligence is? And no, we have not made any specific guidelines to that.

In regards to what other payers are doing, there's not too much that we can do to control them. But certainly we would need to make sure that they are not violating any of the requirements of the Implementation Guide going beyond what's actually required.

Secondly, I think you need to make a reasonable effort to meet what the requirements of the implementation guide are in terms of not only content but format. And my guess is that in working with your payers you may be able to come to some agreement that, if you put things that match the format and are a reasonable approximations of the content, they probably will be able to accept that.

Cherylann Smyrski: Well, the format is not the issue. It's the content. And the concern is for my re-bills because we can re-bill Medicare up to 18 months. And the issue with that is the revenue, if I am sending it in the proper format, however, it will get rejected because I don't have the newly required fields because the patient was here prior to the 10/16/03 date, and they could have deceased or we just can't get that information in order to resubmit the claim. And it's not really the format that I'm concerned with. I can put it in the proper format; however, I'm going to have blanks in those newly required fields because our data systems just didn't capture that information because there was no field to capture that information prior to 10/16/03.

Stanley Nachimson: And we've got someone that at least can provide some information from the Medicare perspective.

Janis Nero-Phillips: Hi. This is Janis Nero-Phillips again. And in this case I think that you can gap fill those required fields for the data content. But this is another thing that I'd like to check on and give you a call back to make sure we're giving you the accurate information.

Cherylann Smyrski: I'm sorry. When you say gap fill, what are you gap filling it with, just the...?

Janis Nero-Phillips: You would be gap filling it with different numeric descriptions based on what the contractor, your intermediary or your carrier, would specify. And I'm really just talking from a Medicare perspective, not if you're billing another payer outside the Medicare program.

Are you speaking about Medicare specifically?

Cherylinn Smyrski: I'm speaking for Medicare and other payers because I belong to the Greater New York Hospital Association. I attend the HIPAA meetings there. And this issue was brought up. And the payers that were in the room all were going to handle the situation a different way.

Janis Nero-Phillips: Exactly. And it's their prerogative to do that based on the way they want to interpret the Implementation Guide. So for Medicare I'd like to take your name and number and get back to you to make sure we're giving you the correct information today.

Cherylinn Smyrski: Okay.

Stanley Nachimson: And this is Stanley. I'd also like to add that certainly we're aware of the issue, and it is being discussed. And we intend to discuss it with some of the national organizations like WITI to see if there's at least some sort of an industry wide response that could be agreed upon and some industry wide guidelines that could be presented.

Cherylinn Smyrski: Right, because that's the only way that we're going to have payers try to handle the claims in the same manner.

Okay. My name is Cherylinn. My last name is Smyrski.

Bernice Catherine Harper: Thank you very much.

Cherylann Smyrski: Thank you so much for taking my call.

Bernice Catherine Harper: You're welcome. Next question please.

Operator: Your next question comes from (Grace Guthrie).

(Grace Guthrie): Yes, my question is that you mentioned that an addenda for anesthesiologists there's going to be you could use units or minutes. Can you tell me what segment and data element that is or loop?

Gladys Wheeler: You know, I'm sorry. Offhand I don't have the Implementation Guide here with me. And I don't have that information in front of me. But I'll be glad to call you with it.

(Grace Guthrie): Okay. My name is (Grace Guthrie).

Karen Trudel: Thank you.

Gladys Wheeler: Thank you, (Grace). I will call you with that information.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from (Bruce Rodman).

(Bruce Rodman): Thank you. I have two questions. The first one is that, CMS did recognize in the preamble the requirement for drug coding on the X12 claim side for non-retail pharmacies, the current Implementation Guides require either HCPCS code or NDC code to be used. And Gladys, you had addressed what's also in

the preamble about going back to the X12 organization to open that up to other possibilities in some way.

A concern that providers would have would be to open up the possibility so that payers could, in fact, specify custom codes that are good only for the payer to be used for coding of drugs on the X12 claims. And my question is where is CMS really headed on this area in terms of how they would be approaching X12? And then I have another one that I'll ask in a minute.

Bernice Catherine Harper: We're having consultation regarding who will answer.

Karen Trudel: Sorry. This is Karen. I'll answer the – you've asked kind of a high level philosophical question. And I'll answer that one. I don't know enough to be anything more than dangerous at a detail level.

What we found when we looked at the comments that we received back on the proposed rule was that we had a really pretty big split within the industry among people who said HCPCS is what we need for non-pharmacy transactions and people saying no NCPDP is really what we need – or the NDC is really what we need for pharmacy transactions.

It became apparent that for some business purposes many reimbursement mechanisms the HCPCS was working pretty well and that going to the level of the National Drug Code, which includes the manufacturer, the product, and the package size, was way too much detail for the benefit it might provide.

Other people, especially those who were working with drug rebate systems where they needed to know who the manufacturer was, said don't take away the National Drug Code. We need it.

It seems that there really were two different sets of requirement and no one code set that met everything. What we decided was to leave the status quo, no standard, so that people could continue to use whatever drug code set they are using now. And that leaves us with a point where industry can begin to talk about and perhaps develop and get some consensus around some other drug coding schema that would meet a wider spectrum of needs. And we're aware, for instance, that the FDA and the HHS's National Library of Medicine are already doing some work in this respect.

So what we wanted to do was to leave the door open for some innovation, but innovation in a productive way that would lead to a code set that could be a consensus standard in the future. What we didn't intend was for everyone to take that as a carte blanche to go off and make up their own code. And there was obviously a lot of thought that went into that. And I hope at least that that's kind of given you a high level perspective.

(Bruce Rodman): And it doesn't, in fact – with the X12 implementation guides, you cannot make up customer codes. And I did see something in the preamble about not making up local codes in the HCPCS for that. So that was very good. So I think what you're telling us is you wouldn't be going to the X12 group to ask to open it up to just anything mutually defined. It would be something else that would be done in some other way.

Stanley Nachimson: I think we'll go to X12 and the rest of the industry to determine what the best way would be to modify the implementation guides along the lines of the regulation. And that's again I think dependent on industry consultation, not dependent on what CMS wants to do.

(Bruce Rodman): Okay. But I know that providers would be very, very concerned if it was opened up to mutually defined because the end result of that is that carriers

would be able to define the codes that would be used by drugs, and it would be all different.

Karen Trudel: We hear your concern.

(Bruce Rodman): An editorial comment.

Karen Trudel: Thank you.

(Bruce Rodman): My other question is really kind of a two-part, but it's really the same thing. The TCS Rule was first published in August 2000. Then, as I recall, you did a technical correction several months later that year. And now you've done a third update to it. And in the regulation portion of the final rule itself, each time that's issued it's kind of like where it said this change it to this and where it said this change it to this. Is there someplace that you're going to put together so that we can all get at what the final Final Rule is without having to merge them all in together?

And then I really have the same question, which is I've been seeing some lesser discussion on one of the list servers about the 4010a being merged in with the 4010 for a single document on the X12 standards.

Stanley Nachimson: I think we will leave the actual production of the X12 documents up to X12. I can only tell you that the official adopted standards are the original implementation guides with the addenda's. So it would be up to folks to take both those documents and have them on hand and recognize that's what the standard is.

Karen Trudel: As far as your first question, which was a composite view of the regulation, interestingly this is not the first time I've heard this in the last couple days.

And the Office for Civil Rights did a composite of the privacy rule. Now that the security rule has been published there is some information in the privacy rule that has moved.

What I'm considering doing is talking to the Office for Civil Rights and putting our heads together to do a complete composite HIPAA rule, which would be security, privacy, and transactions and code sets as modified to date. I can't promise that, but that's where we're going to try to go.

Stanley Nachimson: But the Office of the Federal Register – actually the Code of Federal Regulations is republished every October in an official document that combines and keeps the rules up to date. So I don't know exactly when that comes out, but the version will be as of October 1, 2003. So if we can't do it on our own, we'll certainly I think take the document from the Federal Register and attempt to extract the relevant portions of that and put it up on our Website so that there is a consolidated rule that people can access. And that will be actually an official document.

(Bruce Rodman): Thank you very much for the answers.

Stanley Nachimson: That's a very good suggestion.

Bernice Catherine Harper: Next question please.

Operator: Your next question comes from (Aria Sanchez).

(Aria Sanchez): Yes hello?

Karen Trudel: Yes?

(Aria Sanchez): Yes, just so that I have this clear, the covered entity is a covered entity if it transmits electronically any data. But if it has data in storing the media in say a hard drive or a diskette but does not transmit it, it is not a covered entity.

Karen Trudel: That's right.

Stanley Nachimson: If it's a provider.

Karen Trudel: If it's a provider.

(Aria Sanchez): Okay. If it is a provider and it is not transmitting but it stores the information in a computer, it still is not a covered entity.

Karen Trudel: Not a covered entity.

(Aria Sanchez): Okay, thank you.

Karen Trudel: You're welcome.

Bernice Catherine Harper: Thank you, Ms. (Sanchez). Next question please.

Operator: Your next question comes from (Watson Joseph).

(Watson Joseph): Hello?

Karen Trudel: Yes?

(Watson Joseph): Yeah, my name is (Watson Joseph) from SUNCOM Industries. And we are vocational rehab for the disabled in Central Pennsylvania.

HIPAA we realize has a lot of requirements. And we were wondering if there was anything more specific to suit our agency as far as interpreting HIPAA than to look at the whole big picture?

Stanley Nachimson: That's an excellent question. We certainly have a number of documents on the CMS Website, sort of introductory HIPAA documents and videos. That's number one. Number two, I would also urge you to talk to any provider organizations that you happen to be a member of. Generally individual provider organizations are creating information that's specific to their particular members. Thirdly, there are often local organizations – and I believe in Pennsylvania there's something called the e-Pennsylvania Alliance – that also has been formed to assist local providers and health plans in interpreting the requirements of HIPAA. So there are a number of resources available to you that can assist you in these types of interpretations rather than you having to read the regulations yourself.

(Watson Joseph): Yeah. Well we're not really a health plan. I guess we'd be like a social service agency. We have a shelter workshop daily, and we have individual that come in here and, you know, they're transported daily. We're trying to interpret it to suit our agency, and it's pretty much amongst us.

Stanley Nachimson: I think the first step would be for you to determine, using the covered entity tool that we mentioned at the CMS Website, whether or not you're a covered entity and if these regulations apply to you. And once you determine – if you would determine that you are a covered entity, then you do need to get into a deeper understanding of the regulations using some of the resources that we've mentioned.

(Watson Joseph): Thank you very much.

Stanley Nachimson: You're welcome.

Bernice Catherine Harper: Next question please.

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

(Steve Haney): Hi. This is (Steve Haney) from Idaho. We had two quick questions. The first one I'm going to turn over to (Kate). She has a question about security and e-mail.

(Kate): CMS currently has a requirement, it's my understand, that, if you're e-mailing regarding Medicare information, it has to be encrypted. Will that change since the HIPAA Security Rule won't require that?

Karen Trudel: I'm going to refer that question to Bill Schooler, who is one of our HIPAA security experts. Bill, do you want to take that question please?

Bill Schooler: Certainly. No, that will not change. There's no interconnection between the two regulations.

(Kate): So if I understand this correctly, if a provider wants to e-mail our Medicare Plus Choice plan and we want to send back the message, it has to be encrypted, and it's going to stay that way.

Bill Schooler: It is not required to be encrypted by the HIPAA Security Regulation.

(Kate): But by CMS.

Bill Schooler: Then that would stand unchanged.

(Kate): Okay, thank you.

(Steve Haney): Okay. The second question – and we’re going to go back and revisit this anesthesia units versus minutes question that came up a little bit ago – we are in Loop 2400 in SV1 in Segment 3 where you have a qualifier per minute and unit and following that in SV1 Segment 4 you have the actual value. My question to you is this. The statement I heard from Gladys was anesthesia could be billed with minutes and units. I’m scratching my head. I have one set of fields or do I get both?

Karen Trudel: No, that’s minutes or units.

(Steve Haney): Minutes or units – if you use units, is there a standard base, in other words 15 minutes is one unit, or is that something that the payer must negotiate with their provider community?

Gladys Wheeler: No, there is no standard definition for anesthesia time per unit.

(Steve Haney): So if you have modifiers that add additional units to the service, you’d have to then bill in units and negotiate that?

Gladys Wheeler: Yes. Usually that’s determined in your training partner agreement. That’s a business decision.

(Steve Haney): But there is no way to send both minutes and units on the same line?

Gladys Wheeler: No.

(Steve Haney): Wonderful. That was my interpretation. I just was a little perplexed because (unintelligible)...

Karen Trudel: Okay. And I would add to that that this is not a change. That's the way business is happening today.

(Steve Haney): Correct. Well, except that the national standards format allows for both minutes and units to be billed on a single line.

Karen Trudel: No, I meant 4010.

(Steve Haney): And then 4010 you're right. It is one field, and you have to bill one side or the other. Okay, thank you.

Bernice Catherine Harper: Ms. (McKullup), we have time for two more questions please.

Operator: Your next question comes from (Chris Owen).

(Chris Owen): Yes, we're a large hospital provider. And we are looking at contracting with a vendor who will take the print image of our UV92 and emulate keystrokes to direct enter it into the CMS system. What is CMS's position on this? Is this compliant under the direct data entry exception?

Stanley Nachimson: Actually we're currently looking at that question. There's a major discussion being held next week to talk about direct data entry and some other – direct data entry. And this is really one of the items that we're discussing with the industry, whether something like that will be considered a direct data entry transaction or something that needs to be done using regular EDI. So I can't give you a specific answer on that today. We hope to have that resolved some time in the next several months.

Karen Trudel: And we will put a frequently asked question on the Website on that because that's something that many people are asking about.

(Chris Owen): And you say you think you'll have that resolved in the next couple of months?

Stanley Nachimson: I would estimate that we could have it resolved in the next several months. I certainly don't want to promise anything sooner than that.

(Chris Owen): Okay. That kind of leaves us hanging. We hate to start new business without knowing.

Stanley Nachimson: Yeah, I cannot guarantee that that will or will not be considered a direct data entry transaction. So that's something that you might need to consider in your plan.

Karen Trudel: We understand that that's the case. This whole area of direct data entry is one that has turned out to be amazing in its complexity. And the variety of products on the market tend to make it more difficult to deal with. So we're trying to do this in a way that we get a reasonable business solution that will work for people and is not unfairly advantaging various technologies and products.

(Chris Owen): Thank you very much.

Bernice Catherine Harper: Ms. (McKullup), this is our last call.

Operator: Your last question comes from (Joy Salatto).

Karen Trudel: Thank you.

(Joy Salatto): Hello?

Karen Trudel: Yes?

(Joy Salatto): This is (Joy).

Karen Trudel: Hi.

(Joy Salatto): I have a question that involves the two changes in the modification to Final Rule having to do with the HCPCS codes. And there's also one in the Federal Register copy that I have that refers to deleting the requirement for the principle diagnosis in some situations.

I know that that wasn't addressed. I'm assuming that's still true.

Stanley Nachimson: You mean it wasn't addressed in the conversations that we've had here?

(Joy Salatto): Right.

Stanley Nachimson: Yes. Yeah, we did not cover every change that's made in the Addenda. But you're correct in that the requirement for the principle diagnosis is not now on every claim. But there are certain claim types that it's no longer required. That's one of the Addenda changes.

(Joy Salatto): Okay. My question is, as a payer, would we with these changes then expect to receive claims where those data elements are blank in the transactions?

Stanley Nachimson: If the – are you talking about in the diagnosis code are, would you expect blanks there?

(Joy Salatto): Right. And also for HCPCS – if there was no HCPCS code for that particular service, would we expect to receive that, for instance, at the service line level with all of the data there, a charge and so forth, but just no code?

Stanley Nachimson: If that's the way that the implementation guide is set up, that's absolutely correct. My understanding is that for X12 blanks they're not sent. But the data element is just not there. There's no characters there.

(Joy Salatto): Right. So we won't get that data. So instead of being able to look at that claim and say it's noncompliant because the data is not there, we would then have to accept that in and review that claim to determine whether it met the criteria as outlined in the Addenda.

Stanley Nachimson: Although your translator should be set up to do that, yes.

(Joy Salatto): Okay.

Bernice Catherine Harper: Thank you very much. It is getting close to 3:30 Eastern Standard Time. And I'm going to ask Ms. (Brown) to give the announcement regarding the Encore feature.

Ms. (Brown): Arrangements have been made for an Encore feature service. The service will provide you with a recorded playback of the entire session. Because of the upcoming weekend, this feature will begin on Monday, March 3, 2003 and will be available for up to 72 hours. The toll free number is 1-800-642-1687. There will be an operator there to ask you to key in the identification number, which is 8096358. You will then be able to hear the conference call in its entirety.

Bernice Catherine Harper: Thank you, Ms. (Brown).

Now the next roundtable conference will be held on March the 26th at 2:00 p.m. Eastern Standard Time. And it will be addressing the issues of privacy. This will be the sole discussion on that roundtable meeting on the 26th of March.

Also I wanted to let you know that we're going to do a posting of the transcript on the Web. And it will be available I think within the next two or three days.

Also if you want information regarding the conference call on the 26th of March, you can go to the Website www.cms.hhs.gov/hipaa/hipaa2.

And I want to thank the members of our staff that participated with us today. We want to thank all of you who came online.

And, Ms. (McKullup), will you tell us the number of people that were online today please?

Operator: I'm showing there were 1939 participants.

Bernice Catherine Harper: Thank you very much. The conference is now concluded.

Operator: Thank you for participating in today's conference call. You may now disconnect.

END